# Which? How to spot a scam

Ask yourself the following questions. If you answer yes to any of them, there's a good chance it's a scam.


- Have you been contacted out of the blue?

  Cold calls or unexpected emails or messages should raise suspicion, especially if you're asked to give personal or payment details. It's very unusual for legitimate organisations to contact you and ask for sensitive information if you're not expecting them to. If you're not 100% convinced about the identity of the caller, hang up and contact the company directly.

- Have you been asked to share personal details?

  Never share your personal details with anyone if you can't confirm they are who they say they are. Scammers will often try and get valuable personal data from you, and they can use this to steal your money, or even to steal your identity. You should also be wary of anyone who asks you to pay in an unusual way, such as through Western Union or by using Cryptocurrency.

- Are the contact details vague?

Scam websites often have vague contact details. Remember that legitimate companies will have a place of business, phone number or email address to contact them on. Sometimes scammers also use premium rate numbers (starting ‘09’) to squeeze every penny they can out of you.

- Are you being asked to keep it secret?

It's important you can discuss any agreements with your friends, family or advisors as outside perspectives can provide valuable voices of reason. Fraudsters use grooming techniques including isolating you so that you don't tell anyone about the situation you're in and fall deeper into the scam. Asking you to keep quiet is a way to keep you away from the advice and support you need in making a decision.

- Is the offer too good to be true?

Scams will often promise high returns for very little financial commitment. They may even say that a deal is too good to miss. Use your common sense, if a deal seems too good to be true, it inevitably is.

- Are you being pressured to make a decision?

Fraudsters often try to hurry your decision making. Don’t let anyone make you feel under pressure - it’s OK to take a break and think things through if you’re not sure. It's also a common technique for scammers to use a countdown timer on scam websites to pile on further pressure. Genuine companies should always give you time and space to make an informed decision - anyone who tries to rush you should not be trusted.

- Are there spelling and grammar mistakes?

Emails or messages littered with spelling and grammar mistakes are a scam giveaway. Legitimate organisations will rarely, if ever, make spelling

or grammatical mistakes in their emails to you because they've been put together by professionals and checked before they're sent.

# How to spot a fake, fraudulent or scam website

## Don't lose your money to online con artists. Follow our tips to identify and avoid fake, fraudulent or scam websites.

Which?**Editorial team**

---

### In this article



---

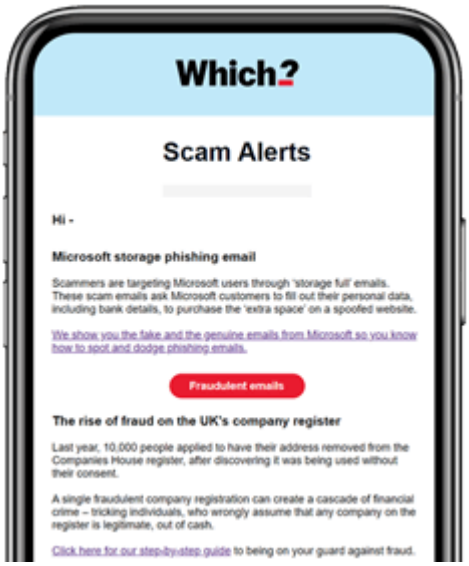
It can be difficult to spot a fake, fraudulent or scam website. Fraudsters can be extremely cunning and use their expertise to create convincing websites.

We're here to help - follow our eight simple tips below to test whether a website is legitimate or not.

# Sign up for scam alerts

Our emails will alert you to scams doing the rounds, and provide practical advice to keep you one step ahead of fraudsters.

**Sign up for scam alerts**




# 1. Double-check the domain name

Many fraudulent websites use a domain name that references a well-known brand or product name.

For example, website domains such as www.ipadoffers.net or www.discountnikeclothes.com should raise alarm bells.

You should also be cautious of domains that end in .net or .org. These are rarely used for online shopping so may have been acquired by questionable people or organisations.

## 2. Is the offer too good to be true?

If prices seem too good to be true then, sadly, they probably are.

Scam websites use low prices to lure bargain-hungry shoppers in order to quickly sell fake, counterfeit or non-existent items.

Sometimes, scammers also use pushy language or a countdown timer to pile on the pressure to buy something while the offer lasts, so be alert to this.

You can use our tips for spotting a scam to help you identify if something is actually a good deal or simply a con.

## 3. Never pay by bank transfer

If you are asked to pay for something online via a bank transfer, don't do it.

If you buy an item that turns out to be fake or non-existent with a credit or debit card, you do have some rights to get your money back.

But if you pay by bank transfer, there's very little you can do to get your cash back.

## 4. Browse the website

Take a couple of minutes to double-check the site. Visit the homepage or the ‘About us’ pages and read the information.

Watch out for poor English, such as spelling and grammar mistakes, or phrases that don’t sound quite right.

It could mean the site isn’t genuine and was put together by someone abroad looking to make a quick profit.

Keep an eye out for pixelated images or graphics, and out-of-date logos or branding. These could indicate that scammers are attempting to imitate a legitimate brand or don't have the resources to create a professional website.

## Contact information

You should also check that the website lists contact information. Legitmate companies will always list how to get in touch with them; if the website doesn’t have a ‘Contact us’ page, it could well be fraudulent.

If the site does have ‘Contact us’ page but only offers a form to fill out, be wary as this could also be an indication of a dubious website.

Any company offering goods or services should list a place of business, as well as a phone number or email address through which to contact it.

If none of this information is available, you should treat the website as highly suspicious.

# 5. Check the returns policy

If the company is selling a product online, it should have a shipping and returns policy listed on its website.

If it’s a real company, it should tell you how and where to return a faulty item.

The website should also have terms and conditions, and a privacy policy that tells you exactly what it plans to do with any data you share and any extra contractual rights you may have.

# 6. Read online reviews

Look at reviews across a number of sources, such as Trustpilot, Feefo or Sitejabber, which aggregate customer reviews.

Don’t look at just one review website – make sure you check several.

You should also check the company’s social media pages for recent activity and to see what other people are posting on their social channels.

CAUTION

## Spot a fake review

Use our top tips to spot a fake review:

**1. Are there lots of oddly similar reviews?**

Similar reviews across several websites may be a red flag.

Reading through reviews, you might notice a whole set that use very similar word groupings and writing styles.

This often means the reviewers are copying information or that the reviews were all written by the same person.

**2. Are the reviewers all very new?**

Watch out for reviews from new accounts. Some of the reviews should be from long-standing members of the site.

You might find the person has reviewed hundreds of websites, which gives them more credibility than someone who's only reviewed one site.

**3. Is the review non-factual or overly factual?**

Facts are important in a review; don't trust a review if facts or actionable information is light on the ground.

Similarly, a review that gives no personal opinion at all may well be a fake – and in any case, it's not a great deal of help.

**4. Can you only find very few reviews?**

In this case, it's probably best to give any suspicious website a miss.

# 7. Can you trust a trust mark?

Research carried out by ANEC, a European consumer organisation, found that seven in ten people say they're more likely to use a website with a trust-mark label or logo.

But with more than 50 different trust-mark labels and logos in use across Europe, and many countries also not using them at all, they are not always a sound way of judging whether a website is trustworthy.

Also, just because a website appears to carry the logo of a reputable trade organisation, it still doesn't necessarily mean the website is genuine.

If you're in doubt, you could always contact the trust-mark company to check.

# 8. Look for a padlock

A padlock next to a website's URL means the site is encrypted, so what you do on on it – such as browse or make payments – can't be intercepted.

Most websites now have this feature, so if you notice a site doesn't have one it could be a red flag.

But equally, scammers are able to forge or buy these padlocks, so seeing one doesn't always mean a website is safe.

Looking for a padlock should always be combined with the other checks we've recommended.

## Seen or been affected by a scam? Help us protect others

Sharing details of the scam helps us to protect others as well as inform our scams content, research and policy work. We will collect information relating to your experience of a scam, but we won't be able to identify your responses unless you choose to provide your contact details.

**Share scam details**

# Phone scams

## Commonly known as 'vishing' scams, these involve fraudsters trying to trick you over the phone. Stay one step ahead with our tips


Which? Team

---

### In this article

---

# What is a phone scam?

Phone scams involve fraudsters attempting to obtain your personal or financial information over the phone.

These scams are often referred to as 'vishing' scams - a combination of 'voice' and 'phishing'.

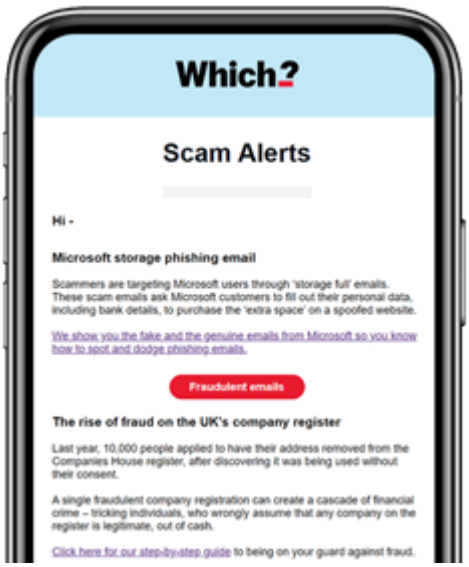
It's not always easy to spot a phone scam. For example, fraudsters can spoof phone numbers so it appears that you're genuinely being called by your bank or a government department. Additionally, they may already have some of your information from a previous data breach, which might make you think the call is genuine.

Read on to learn more about the most common types of phone scams and how to avoid them.

# Sign up for scam alerts

Our emails will alert you to scams doing the rounds, and provide practical advice to keep you one step ahead of fraudsters.

**Sign up for scam alerts**




# Common types of phone scam

- **Impersonation scams:** Someone calls you out of the blue claiming to be from your bank's fraud department. They inform you that your account has been compromised and encourage you to transfer your money into a 'safe' account, before disappearing with your cash. Scammers have also been known to impersonate the police, utility providers and government departments.
- **Remote access scams:** Similar to the above, the fraudster claims your account has been compromised and informs you that you'll need to download software onto your device so that they can access the account. The software is from a legitimate company but is used by the scammer to steal your money. If you're encouraged to download software, end the call, disconnect from your wi-fi and delete anything you've downloaded.
- **Tech support scams:** These scams also involve remote access software. The fraudster impersonates a tech company such as Microsoft and informs you that your device has been infected with malware. To fix the issue, they will either ask you to download remote access software to give them control over your device or trick you into installing malware.

- **HMRC scams:** A scammer calls you claiming to be from HMRC, telling you that you have underpaid your tax. Some scammers leave automated voicemails which state that you're being taken to court and ask you to press a number that then puts you through to a fraudster. Other HMRC scams begin with an email or text message asking you to call a dodgy number to secure your account or claim a tax refund. You can report scam calls to HMRC online (you'll be asked to sign in using your Government Gateway user ID or your email address).
- **Investment and financial scams:** A scammer calls you out of the blue about a phoney investment opportunity, promising huge returns. Pension cold calls are banned, and the government is consulting on extending this to all financial products. If the changes come into force, you'll know that any unsolicited financial call trying to sell you a product is a scam.
- **Prize draw scams:** A fraudster calls you claiming that you've won a prize or the lottery. They'll invent a story to make up for the fact that you don't remember entering a competition. You'll usually be asked for your personal or financial information to receive the prize or money.

KEY INFORMATION

## Watch out for number spoofing

This is when a scammer has been able to spoof a company's legitimate phone number to appear genuine.

If you receive an unexpected call from a company, it's always best to hang up and call back yourself.

# How to stay safe from phone scams

Follow these tips to stay safe from scammers who target you over the phone:

1. Never disclose your financial information over the phone. If you're at all suspicious about the caller, end the call immediately.
2. Register with the Telephone Preference Service (TPS). This will stop legitimate companies from making unsolicited sales and marketing calls to your phone number, so when you receive a call, you'll know a scammer is on the other end of the line.
3. Consider installing a call blocker for nuisance calls.
4. Be aware that scammers may be able to keep your phone line open even after you've hung up, so if you hang up on a dodgy call, use a different phone to call the company back on a trusted number or wait for at least 10 to 15 minutes.Call 159
5. Call 159 if you receive a call claiming to be from your bank. When you call, you'll be put through to your bank's genuine customer service line. The banks involved in the scheme include Barclays, Bank of Scotland, Co-operative, First Direct, Halifax, HSBC, Lloyds, Metro Bank, Nationwide, NatWest, Royal Bank of Scotland, Santander, Starling Bank, Tide, TSB and Ulster Bank.

# How to report phone scams

If you receive a spam call on your iPhone, you can report it to your provider by texting the word 'call' followed by the phone number to 7726.

If you have an Android phone, text the word 'call' to 7726. You'll then receive a message asking you for the scam number.

For scam calls received on WhatsApp, open the WhatsApp chat with the dodgy phone number and tap 'block.' You can report the contact by tapping 'report contact' and 'block'.

You can also report scam calls to Action Fraud or call the police on 101 if you're in Scotland.

# Premium-rate number scams

Fraudsters also look to trick victims via premium-rate number scams.

We've previously reported on 'call connecting' companies buying up ads on search engines that appear when you search for a government department or utility provider.

These 'click to dial' ads allow you to click on the phone number and be put straight through to the company. You will be sent through to the company's genuine phone line, but via a premium-rate number, meaning a call that should be free could cost you upwards of £100.

Premium numbers to look out for typically start with 084, 087, 090, 091 or 098. To avoid these scams, don't click on sponsored results when looking up companies or government departments. Instead, ensure you're navigating to their official website.

If you've been unexpectedly charged a premium rate for a call and believe this wasn't made clear, you can report this to the Phone-paid Services Authority.

Finally, it's also worth being on your guard against 'missed call' scams. This is when a scammer calls you from a premium number but ends the call before you can answer it, in the hope you'll phone back and run up a big bill.

## Seen or been affected by a scam? Help us protect others

Sharing details of the scam helps us to protect others as well as inform our scams content, research and policy work. We will collect information relating to your experience of a scam, but we won't be able to identify your responses unless you choose to provide your contact details.

**Share scam details**

# How to spot an email scam

Follow our top tips to avoid email scams and safeguard yourself from fraudsters trying to steal your personal information and bank details.

W

Which?**Editorial team**

# What is an email scam?

Email scams, also known as 'phishing' scams, have become increasingly common as fraudsters come up with new ways to try and steal your personal information and bank details.

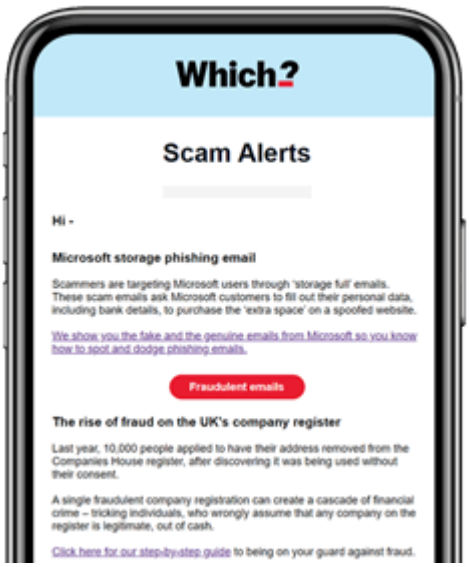
These scams often involve a fraudster sending you an email purporting to be from a well-known brand or retailer. When you click on a link in the email, you'll be sent to a spoofed website where you're asked to enter your personal information. If you do this, you'll be handing your details to the scammer.

In some instances, scam emails contain malicious software which can infect your computer, tablet or mobile phone with a virus. If you suspect an email might be from a scammer, don't click on any links or download any attachments. Stay security-savvy and ensure your antivirus software is always up to date, as this will provide an extra layer of protection.

# Sign up for scam alerts

Our emails will alert you to scams doing the rounds, and provide practical advice to keep you one step ahead of fraudsters.

**Sign up for scam alerts**




# How to spot an email scam

Email scams can be incredibly tricky to spot.

See the example below of an email scam impersonating HMRC. The scammer uses HMRC branding, and is convincing enough to catch people out.

## HMRC scam emails

HM Revenue
& Customs

# Self Assessment


**Dear customer,**

Our record indicates your Self Assessment Online profile is not up to date.

Please note that your HMRC account profile security is about to expire, For it to remain active, please activate your account.

We've recently been reviewing all our tax payers accounts for the year.

Follow the reference below to update your Self Assessment online profile now.:

**Update Now**

Yours faithfully

- 

Dear Customer

We are writing to let you know that your HMRC Self Assessment password is about to expire.

To keep your account active, Follow the reference link below to update your Self Assessment online profile now:

**https://www.tax.service.gov.uk/profileupdate**

You need to complete this process within 48 hours to avoid account inactive.

Yours faithfully

Geoff Greensmith
Head of Digital Engagement and Communication Services

Twitter Visit GOV.UK YouTube HMRC Forum

**Stay safe online**
For more information, please search 'avoid and report internet scams and phishing' on GOV.UK

**HMRC's help and support email service**

- A scam email impersonating HMRC

HM Revenue
& Customs

# Self Assessment


**Dear customer,**

Our record indicates your Self Assessment Online profile is not up to date.

Please note that your HMRC account profile security is about to expire, For it to remain active, please activate your account.

We've recently been reviewing all our tax payers accounts for the year.

Follow the reference below to update your Self Assessment online profile now.:

**Update Now**

Yours faithfully

Dear Customer

We are writing to let you know that your HMRC Self Assessment password is about to expire.

To keep your account active, Follow the reference link below to update your Self Assessment online profile now:

**https://www.tax.service.gov.uk/profileupdate**

You need to complete this process within 48 hours to avoid account inactive.

Yours faithfully

Geoff Greensmith
Head of Digital Engagement and Communication Services


But there are clues to spotting this scam:

- The greeting isn't personalised - it addresses the recipient as a 'customer'
- There are some basic grammatical errors, such as random capitalised words and full stops
- Investigating the links in the emails show that the website address differs to that of the official HMRC

Follow our top tips to spot and avoid falling for an email scam.

## 1. Check the sender's email address

A scam email will usually come from an unrecognisable email address. This may consist of random numbers, letters or words that have nothing to do with the organisation the scammer is impersonating.

To find out if there’s a fraudster behind what appears to be a genuine email, hover your cursor over or right-click on the sender's name and you should be able to view the email address behind it.

## 2. Is the greeting impersonal?

Some email scams include your name in the first line of the message. However, not all do.

Sometimes scam emails will just say “Hi” and not include a name, or your email address will be used after “Hi”. This impersonal approach is a sign that it’s likely to be a scammer behind the email.

## 3. Check contact information and dates

Hover your cursor over anywhere you'd usually expect there to be a link in the email.

For example, check the bottom of the email for 'contact us' buttons or links to terms and conditions.

By hovering your cursor over any links, you can see the URL they'll send you to without clicking on them.

It's also worth checking whether any dates in the email are correct. Often scammers will forget this detail.

## 4. Check the branding

Take a look at the quality of of any logos in the email. For example, if the images are pixelated, this can strongly indicate that the email is a scam.

Compare the branding in the email to the company's genuine website or any genuine emails you've received from the company in the past.

## 5. Check if the linked website is legitimate

If you've clicked through to a website from an email thinking it is genuine, double-check the authenticity of the website before entering any details.

The domain information checker Who.is will show you when the website was created. If the site was created recently, it's likely to be dodgy.

If it’s a big brand or company being impersonated, open a new tab and visit its genuine website to compare the URLs.

If you haven't yet clicked a link but are being asked to do so you can access a message on your account, avoid the temptation to act quickly.

Instead, navigate to the company's website to log in to your account. If no message or alert is present, you'll know the email is dodgy.

## 6. Is the email asking for personal information or bank details?

If an email asks you to update or re-enter your personal information or bank details out of the blue, it is likely to be a scam.

Most companies will never ask for personal information via email.

## 7. Does it have poor spelling, grammar and presentation?

Scammers are getting better at presenting phishing emails that are more or less free of poor spelling and grammar - but you should still watch out for these tell-tale signs.

You might also notice a lack of consistency with the presentation of the email, which may include several different font styles and sizes and a mishmash of logos.

## 8. Is it trying hard to be 'official'?

Scammers often try hard to make a dodgy email sound official. They will do this in a number of ways, including by using the word ‘official’.

You are unlikely to see the messaging in a truly official email shouting about how official it is.

Scam emails may also contain information such as account numbers and IDs designed to trick you into thinking the email is genuine. Check any of these against your records to see if they match.

## 9. Is it trying to rush you?

Fraudsters will try to pressure you with time-sensitive offers, encouraging you to act now or miss out on ‘exclusive’ deals.

Take your time to make all the checks you need. If the message regards an account you have with the company, organisation or retailer, you should log in separately to your account in a new tab or window

It’s better to miss out on a genuine deal than risk compromising your personal details.

## 10. Check with company, brand or department

If you’re still unsure whether a scammer is behind the email you received, get in touch with the brand or company featured in your email directly via social media or its 'contact us' page.

Check the brand or company's help and customer services pages. Big companies are sometimes aware of scams and publish advice for customers on what to watch out for.

# Reporting email scams

You can report email scams by forwarding the email to report@phishing.gov.uk

You can also report emails to your email provider - select the ‘Report Spam’ on Gmail, the ‘Report phishing’ button on Hotmail and send scam emails to abuse@yahoo.com if you use a Yahoo account.

### Seen or been affected by a scam? Help us protect others

Sharing details of the scam helps us to protect others as well as inform our scams content, research and policy work. We will collect information relating to your experience of a scam, but we won't be able to identify your responses unless you choose to provide your contact details.

**Share scam details**

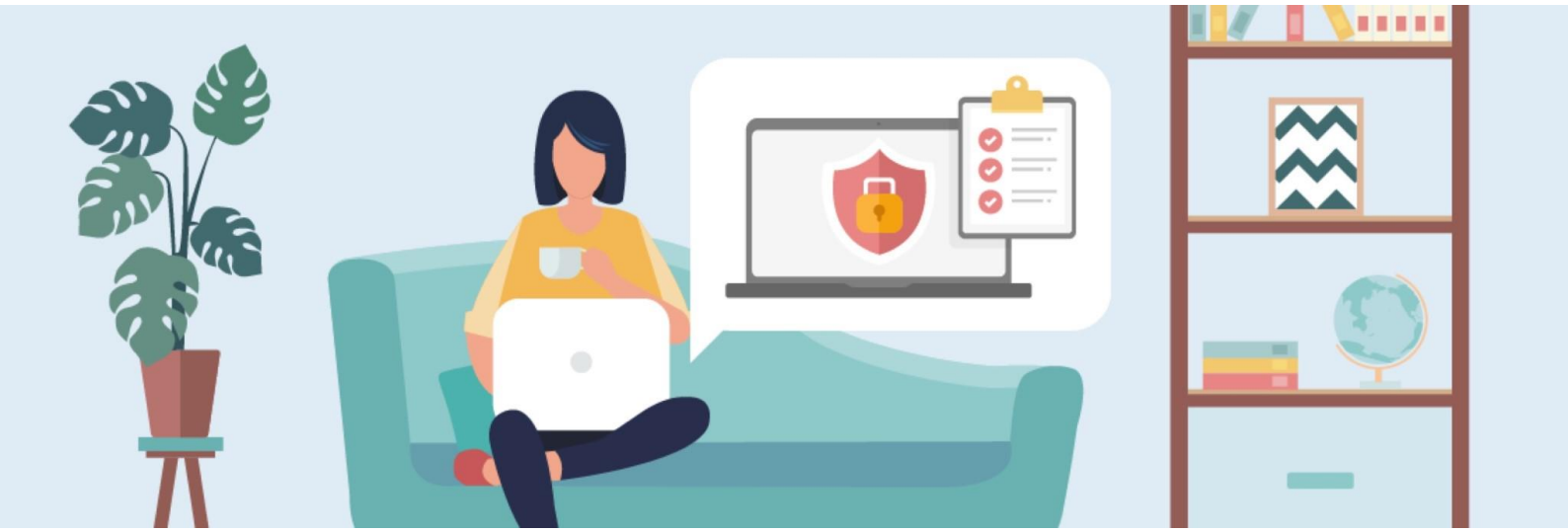
# Scams Protection Checklist

Scammers have become more sophisticated in their bid to part us from our cash.

Protect yourself from being scammed by following our tips.

# Scams Protection Checklist

Scammers have become more sophisticated in their bid to part us from our cash. Protect yourself from being scammed by following our tips.



- [ ] Whether it's an email scam, text scam or phone scam, our guide explains how and where to report a scam . We also have advice on how to get your money back if you've lost out to a scam

- [ ] Always set strong passwords , and have a unique one for every single website. Re-using passwords can make you vulnerable to a credential-stuffing attack . Using easy-to-remember passwords and reusing the same passwords across lots of websites is not secure. If you'd like to securely store all of your passwords for different accounts we recommend using a password manager. For more on password managers and to help you choose, check out our password manager reviews

- [ ] 2FA is when you add a second step to the log-in process for your online accounts. So rather than just typing in your password, you have to complete a second step, too. Examples of this could be typing in a code sent to you by SMS, generated by an app on your phone or it can be confirming that it's you with a fingerprint or a scan of your face. Read more advice on two-factor authentication.

☐ Find out if your details have been compromised in a data breach. If your account has been compromised then the company should let you know, but you can find out yourself by visiting haveibeenpwned.com . This is a service run by Troy Hunt, one of the most respected names in online security. It is safe to enter your password to check if it's been revealed in a data breach the site doesn't store passwords you enter. Try not to worry too much about a data breach, just make sure you change the password for that account and ensure you've not used that password anywhere else.

☐ Checking your credit report is an important part of maintaining your financial health. It'll allow you to pick up on any mistakes - or even fraudulent applications. Read our advice on how to check your credit file for free . You could also join Cifas Protection Registration which notifies banks to make extra checks if your details are used to open a new account.

☐ Avoid putting your phone number and full date of birth on social media scammers trawl through profiles looking through this information. Update your privacy settings so your profile and the things you post are only visible to your friends and family. You can choose settings that will stop strangers from sending you messages or friend requests. Ignore friend or connection requests from people you don't know in real life.

☐ Call blockers stop unsolicited calls, by registering for the free Telephone Register Service companies shouldn't call you. There are also ways you can block nuisance calls on your landline and mobile device.

☐ Sadly, if you've been scammed once, you're more likely to be targeted again. It might be worth changing your number and/or email address if you're being bombarded by cold calls and spam.

☐ We will send you emails with the latest scams and practical advice on how to stay one step ahead of fraudsters. Sign up online .

☐ For £5/month the Which? Tech support helpline can give you one to one guidance and support with your online security questions. Sign up online .

# Check if something might be a scam

This advice applies to England. See advice for See advice forNorthern Ireland, See advice forScotland, See advice forWales

Scams can be difficult to recognise, but there are things you can look out for.

## If you've seen something online or in an email or text

You can use our online tool to get advice. Our tool will ask you questions and use your answers to give you advice on:

- how to check whether something is a scam
- what to do if you've been scammed

Start the online tool

## Recognising a scam

It might be a scam if:

- it seems too good to be true – for example, a holiday that's much cheaper than you'd expect
- someone you don't know contacts you unexpectedly
- you suspect you're not dealing with a real company – for example, if there's no postal address
- you've been asked to transfer money quickly
- you've been asked to pay in an unusual way – for example, by iTunes vouchers or through a transfer service like MoneyGram or Western Union
- you've been asked to give away personal information like passwords or PINs
- you haven't had written confirmation of what's been agreed

If you think you've paid too much for something

Paying more for something than you think it's worth isn't the same as being scammed. Usually, a scam will involve theft or fraud.

You have other rights if you think you've overpaid.

## If you think you've spotted a scam

If you've given away money or information because of a scam, there are things you should do. Check what to do if you've been scammed.

If you haven’t been scammed but you’ve seen something you think is a scam, you should report it. Find out how to report a scam.

If you think someone is calling to trick you into giving them money or your personal details, hang up and call 159. This is a secure service that connects you directly with your bank.

Calls to 159 are usually charged at the national rate - it depends on your provider.

Check if your bank uses 159 on the Stop Scams UK website.

## Protecting yourself online

There are things you can do to protect yourself from being scammed online.

### Check the signs of fake online shops

You can search for a company's details on GOV.UK. This will tell you if they're a registered company or not.

If you’re buying something on a site you haven't used before, spend a few minutes checking it – start by finding its terms and conditions. The company’s address should have a street name, not just a post office box.

Check to see what people have said about the company. It’s worth looking for reviews on different websites – don’t rely on reviews the company has put on its own website.

Also, don’t rely on seeing a padlock in the address bar of your browser - this doesn’t guarantee you’re buying from a real company.

### Don’t click on or download anything you don’t trust

Don’t click on or download anything you don’t trust - for example, if you get an email from a company with a strange email address. Doing this could infect your computer with a virus.

Make sure your antivirus software is up to date to give you more protection.

### Be careful about giving personal information away

Some scammers try to get your personal information – for example, the name of your primary school or your National Insurance number. They can use this information to hack your accounts. If you come across sites that ask for this type of information without an obvious reason, check they’re legitimate.

Check if your details have been shared online

Sometimes your log-in details can be made publicly available when a website is hacked. This means that someone could use your details in a scam. Check whether your accounts have been put at risk on Have I Been Pwned.

Make your online accounts secure

Make sure you have a strong password for your email accounts that you don't use anywhere else. If you're worried about remembering lots of different passwords, you can use a password manager.

Some websites let you add a second step when you log in to your account – this is known as 'two-factor authentication'. This makes it harder for scammers to access your accounts.

Find out how to set up two-factor authentication across services like Gmail, Facebook, Twitter, LinkedIn, Outlook and iTunes on the on the National Cyber Security Centre website.

Pay by debit or credit card

Pay by card to get extra protection if things go wrong. Read our advice on getting your money back after you've been scammed.

Know how your bank operates

Check your bank's website to see how your bank will and won't communicate with you. For example, find out what type of security questions they'll ask if they phone you.

## Find out about recent scams

To find out about scams across the country, you can sign up to the Trading Standards email alert on their website. Trading Standards can investigate and take court action against scammers.

If you want to know about scams in your local area, sign up for email alerts on Action Fraud's website.

You can also find out about common financial scams on the Financial Conduct Authority's website.

## Help us improve our website

Take 3 minutes to tell us if you found what you needed on our website. Your feedback will help us give millions of people the information they need.

# Where to go for help

- How to spot a scam - Which?
- Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK
- Phone scams – dealing with cold and nuisance calls | Age UK
- Check if something might be a scam - Citizens Advice

# 8 tips to stay safe online and spot fake websites: Your ultimate guide

**Synopsis**

**To protect personal and financial information from cybercriminals who use fake websites, observe internet safety etiquette. Use secure connections, verify URLs, don't rely solely on Google to find websites, watch out for spelling mistakes and poor grammar, check for contact information and SSL certificates, and review ratings before using a website**.

ReutersCybercriminals are constantly on the prowl, and they can use a variety of methods to steal your personal and financial information. One of the most common ways they do this is by creating fake websites that mimic legitimate ones

The internet has become an integral part of our lives, and with it comes the need to stay safe online. Cybercriminals are constantly on the prowl, and they can use a variety of methods to steal your personal and financial information. One of the most common ways they do this is by creating fake websites that mimic legitimate ones.

Recently, several Indian investors trading on cryptocurrency platforms lost crores of rupees and falling prey to fraudsters who promised high returns and goade .

**Here is how to stay safe online and spot fake websites.**

**Use a Secure Connection:** Always use a secure connection when browsing the internet. Look for the padlock icon in the address bar, which indicates that the website is using a secure connection. A secure connection ensures that your information is encrypted and cannot be intercepted by hackers.

**Verify the URL:** Before entering any personal or financial information on a website, verify the URL. Check to see if it matches the website you intend to visit. Cybercriminals often create fake websites with URLs that are similar to legitimate ones, hoping to trick users into entering their information.

**Don't always use google to find a website:** People often use Google to find website links. But you should carefully check the link and authenticity before trusting the site to conduct any online transaction. Fraudster often manipulate google search to throw their website up higher in google ranking.

**Check for Misspellings and Grammar Errors:** Fake websites often have misspellings and grammar errors. Legitimate websites are usually professionally designed and will not have these types of errors. If you notice any spelling or grammar mistakes on a website, it's a red flag that it may be fake.

**Look for Contact Information:** Legitimate websites will always have contact information, such as an email address, phone number, or physical address. If you cannot find any contact information on a website, it's a red flag that it may be fake.

**Don't Click on Suspicious Links:** If you receive an email or message with a link that you were not expecting, do not click on it. Cybercriminals often use phishing scams to trick users into clicking on links that lead to fake websites. Always verify the sender and the content of the message before clicking on any links.

**Check the Website's SSL Certificate:** An SSL certificate is a security protocol that ensures that your information is encrypted when you enter it on a website. Legitimate websites will always have an SSL certificate. You can check for the SSL certificate by looking for the padlock icon in the address bar.

**Look for Reviews and Ratings:** If you are unsure whether a website is legitimate or not, look for reviews and ratings from other users. Sites like Trustpilot and Yelp allow users to rate and review websites. If a website has a lot of negative reviews or no reviews at all, it's a red flag that it may be fake.

Staying safe online and spotting fake websites is essential to protect your personal and financial information. Always use a secure connection, verify the URL, check for misspellings and grammar errors, look for contact information, don't click on suspicious links, check the website's SSL certificate, and look for reviews and ratings. By following these tips, you can avoid falling victim to cybercriminals and keep your information safe online.

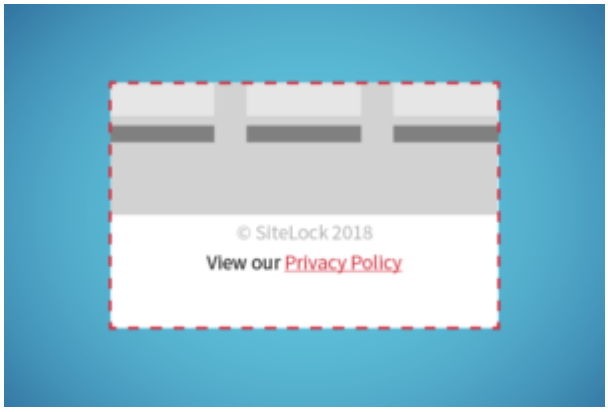
# How Can I Tell If a Website Is Safe? Look For These 5 Signs

**AUGUST 24, 2018** in **Cyber Attacks**

Every website owner should take responsibility for ensuring the safety of its visitors, but unfortunately, some websites just aren't secure. An unsafe website can spread malware, steal your information, send spam, and more. To protect yourself and your personal information, it's important to know that a website takes your safety seriously – but how can you tell? Look for these five signs that a website is safe:


## 1. Look for the "S" in HTTPS

If HTTPS sounds familiar, it should – many URLs begin with "https" instead of just "http" to indicate that they are encrypted. This security is provided by an SSL certificate, which protects sensitive information entered into that site as it travels from the site to a server. Without an SSL certificate, that information is exposed and easily accessible by cybercriminals. It's important to note that HTTPS isn't the only thing a website can – or should do – to protect its visitors, but it's a good sign that the website owner cares about your safety. Whether you're logging in, making a payment, or just entering your email address, check that the URL starts with "https."




2. Check for a website privacy policy

A website's privacy policy should clearly communicate how your data is collected, used, and protected by the website. Nearly all websites will have one, as they are required by data privacy laws in countries like Australia and Canada, and even stricter rules have been introduced in the EU. A privacy policy indicates that the website owner cares about complying with these laws and ensuring that their website is safe. Be sure to look for one, and read it over, before giving your information to a website.

## 3. Find their contact information

If finding a website's contact information makes that site seem more trustworthy to you, you're not alone. A survey of website visitors found that 44 percent of respondents will leave a website that lacks a phone number or other contact information. Ideally, a safe website will clearly display an email address, a phone number, a physical address if they have one, return policy if applicable, and social media accounts. These won't necessarily provide protection, but they indicate that there's likely someone you can reach out to if you need assistance.


4. Verify their trust seal

If you see an icon with the words "Secure" or "Verified," it's likely a trust seal. A trust seal indicates that the website works with a security partner. These seals are often an indicator that a site has HTTPS security, but they can also indicate other safety features, like the date since the site's last malware scan.

Although 79 percent of online shoppers expect to see a trust seal, the presence of the seal isn't enough. It's also important to verify that the badge is legitimate. Fortunately, it's easy to do – simply click the badge and see if it takes you to a verification page. This confirms that the site is working with that particular security firm. It doesn't hurt to do your own research on the company supplying the badge, too!


*If a trust seal is legitimate, clicking on it will take you to a page that verifies the authenticity of that seal. As an example, SiteLock's verification page looks like this.*


5. Know the signs of website malware

Even if a website has an SSL certificate, a privacy policy, contact information, and a trust badge, it may still not be safe if it is infected with malware. But how do you know if a website is infected with malware? Look for the signs of these common attacks:

- **Defacements.** This attack is easily spotted: cybercriminals replace a site's content with their name, logo, and/or ideological imagery.
- **Suspicious pop ups.** Be cautious of pop ups that make outlandish claims – they are likely trying to entice you to click and accidentally download malware.
- **Malvertising.** Some malicious ads are easy to catch. They typically appear unprofessional, contain spelling/grammar errors, promote "miracle" cures or celebrity scandals, or feature products that don't match your browsing history. It's important to note that legitimate ads can also be injected with malware, so exercise caution when clicking.
- **Phishing kits.** Phishing kits are websites that imitate commonly visited sites, like banking websites, in order to trick users into handing over sensitive information. They may appear legitimate, but spelling and grammar errors will give them away.
  Malicious redirects. If you type in a URL and are redirected to another site – especially one that looks suspicious – you have been affected by a malicious redirect. They are often used in conjunction with phishing kits.
- **SEO spam.** The appearance of unusual links on a site, often in the comments section, is a sure sign of SEO spam.

- **Search engine warnings.** Some popular search engines will scan websites for malware, and place a warning on that site if it is definitely infected with malware.

It's unfortunate that not every website is trustworthy and secure, but don't let that keep you from going online – just do it safely! Simply being able to recognize a safe

website can go a long way to help protect your personal data. A legitimate trust seal, “https,” a privacy policy, and contact information are all good signs that a website is safe! For more on protecting your information online, check out our blog on safe online shopping.

Has your site's security been breached? See how SiteLock can help fix your hacked website immediately.

# How to spot a fake, fraudulent or scam website

Don’t lose your money to online con artists. Follow our tips to identify and avoid fake, fraudulent or scam websites.

W

Which?**Editorial team**


---

**In this article**



---

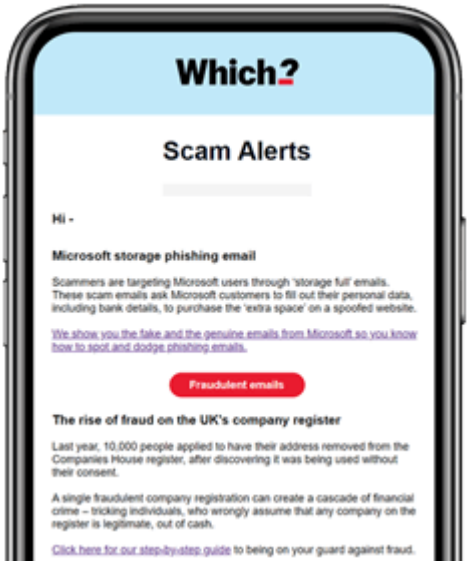
It can be difficult to spot a fake, fraudulent or scam website. Fraudsters can be extremely cunning and use their expertise to create convincing websites.

We're here to help - follow our eight simple tips below to test whether a website is legitimate or not.

# Sign up for scam alerts

Our emails will alert you to scams doing the rounds, and provide practical advice to keep you one step ahead of fraudsters.

**Sign up for scam alerts**




# 1. Double-check the domain name

Many fraudulent websites use a domain name that references a well-known brand or product name.

For example, website domains such as www.ipadoffers.net or www.discountnikeclothes.com should raise alarm bells.

You should also be cautious of domains that end in .net or .org. These are rarely used for online shopping so may have been acquired by questionable people or organisations.

## 2. Is the offer too good to be true?

If prices seem too good to be true then, sadly, they probably are.

Scam websites use low prices to lure bargain-hungry shoppers in order to quickly sell fake, counterfeit or non-existent items.

Sometimes, scammers also use pushy language or a countdown timer to pile on the pressure to buy something while the offer lasts, so be alert to this.

You can use our tips for spotting a scam to help you identify if something is actually a good deal or simply a con.

## 3. Never pay by bank transfer

If you are asked to pay for something online via a bank transfer, don't do it.

If you buy an item that turns out to be fake or non-existent with a credit or debit card, you do have some rights to get your money back.

But if you pay by bank transfer, there's very little you can do to get your cash back.

## 4. Browse the website

Take a couple of minutes to double-check the site. Visit the homepage or the 'About us' pages and read the information.

Watch out for poor English, such as spelling and grammar mistakes, or phrases that don't sound quite right.

It could mean the site isn’t genuine and was put together by someone abroad looking to make a quick profit.

Keep an eye out for pixelated images or graphics, and out-of-date logos or branding. These could indicate that scammers are attempting to imitate a legitimate brand or don't have the resources to create a professional website.

## Contact information

You should also check that the website lists contact information. Legitmate companies will always list how to get in touch with them; if the website doesn’t have a ‘Contact us’ page, it could well be fraudulent.

If the site does have ‘Contact us’ page but only offers a form to fill out, be wary as this could also be an indication of a dubious website.

Any company offering goods or services should list a place of business, as well as a phone number or email address through which to contact it.

If none of this information is available, you should treat the website as highly suspicious.

# 5. Check the returns policy

If the company is selling a product online, it should have a shipping and returns policy listed on its website.

If it’s a real company, it should tell you how and where to return a faulty item.

The website should also have terms and conditions, and a privacy policy that tells you exactly what it plans to do with any data you share and any extra contractual rights you may have.

# 6. Read online reviews

Look at reviews across a number of sources, such as Trustpilot, Feefo or Sitejabber, which aggregate customer reviews.

Don’t look at just one review website – make sure you check several.

You should also check the company’s social media pages for recent activity and to see what other people are posting on their social channels.

CAUTION

## Spot a fake review

Use our top tips to spot a fake review:

**1. Are there lots of oddly similar reviews?**

Similar reviews across several websites may be a red flag.

Reading through reviews, you might notice a whole set that use very similar word groupings and writing styles.

This often means the reviewers are copying information or that the reviews were all written by the same person.

**2. Are the reviewers all very new?**

Watch out for reviews from new accounts. Some of the reviews should be from long-standing members of the site.

You might find the person has reviewed hundreds of websites, which gives them more credibility than someone who's only reviewed one site.

**3. Is the review non-factual or overly factual?**

Facts are important in a review; don't trust a review if facts or actionable information is light on the ground.

Similarly, a review that gives no personal opinion at all may well be a fake – and in any case, it's not a great deal of help.

**4. Can you only find very few reviews?**

In this case, it's probably best to give any suspicious website a miss.

# 7. Can you trust a trust mark?

Research carried out by ANEC, a European consumer organisation, found that seven in ten people say they're more likely to use a website with a trust-mark label or logo.

But with more than 50 different trust-mark labels and logos in use across Europe, and many countries also not using them at all, they are not always a sound way of judging whether a website is trustworthy.

Also, just because a website appears to carry the logo of a reputable trade organisation, it still doesn't necessarily mean the website is genuine.

If you're in doubt, you could always contact the trust-mark company to check.

# 8. Look for a padlock

A padlock next to a website's URL means the site is encrypted, so what you do on it – such as browse or make payments – can't be intercepted.

Most websites now have this feature, so if you notice a site doesn't have one it could be a red flag.

But equally, scammers are able to forge or buy these padlocks, so seeing one doesn't always mean a website is safe.

Looking for a padlock should always be combined with the other checks we've recommended.

## Seen or been affected by a scam? Help us protect others

Sharing details of the scam helps us to protect others as well as inform our scams content, research and policy work. We will collect information relating to your experience of a scam, but we won't be able to identify your responses unless you choose to provide your contact details.

Share scam details

# 5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam – 2018

## There are many ways to determine if a website is fake—here's what we recommend.

The internet is full of websites that are either fake, fraudulent or a scam. It's a sad fact of life. You see, the evolution of the internet has brought with it a number of extremely convenient advances in the way we shop, bank, and interact with the world around us. At the same time, that evolution has also given way to new risks—new avenues for criminals to rip off the unsuspecting. In 2018 Cybercrime will be a $1.5 trillion industry.

Really, what it all boils down to is fraud. These hackers and cyber criminals are little more than new age con men. And the con game is as old as time itself—people have literally been tricking one another since the beginning of time. And in the same vein as ancient mystics and old-fashioned snake oil salesmen, these con-men are after one thing: your money.

Nowadays their tactics tend to involve phishing. Lots and lots of phishing.

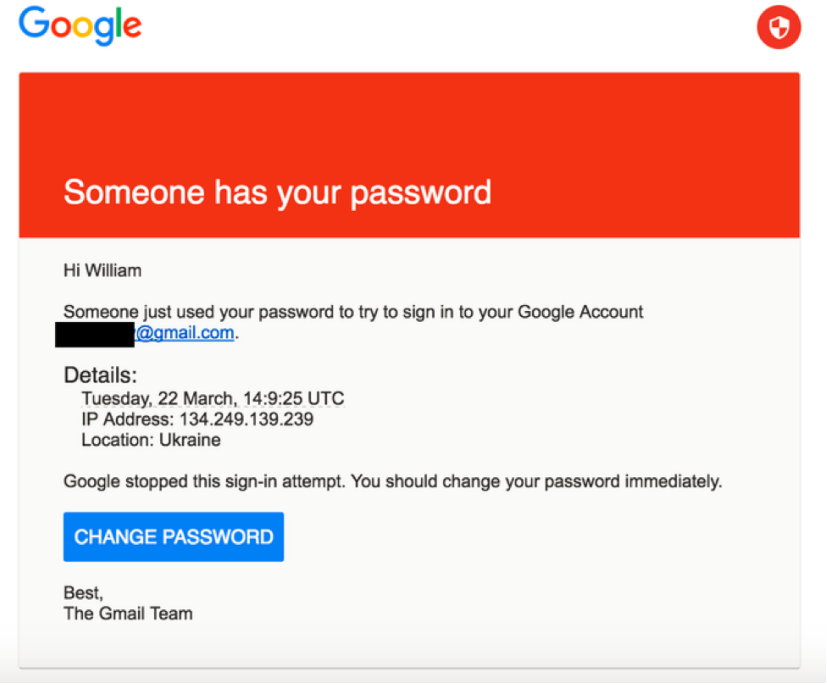
## What is Phishing?

Phishing is a type of online fraud that involves getting an individual or organization to disclose sensitive, sometimes compromising information, under false pretenses that have been expertly manufactured by the attackers. Tailoring your phishing attack to your target is sometimes called spearphishing, it's a form of social engineering. These attacks take several forms, often elaborately combining multiple mediums to create the impression of legitimacy.

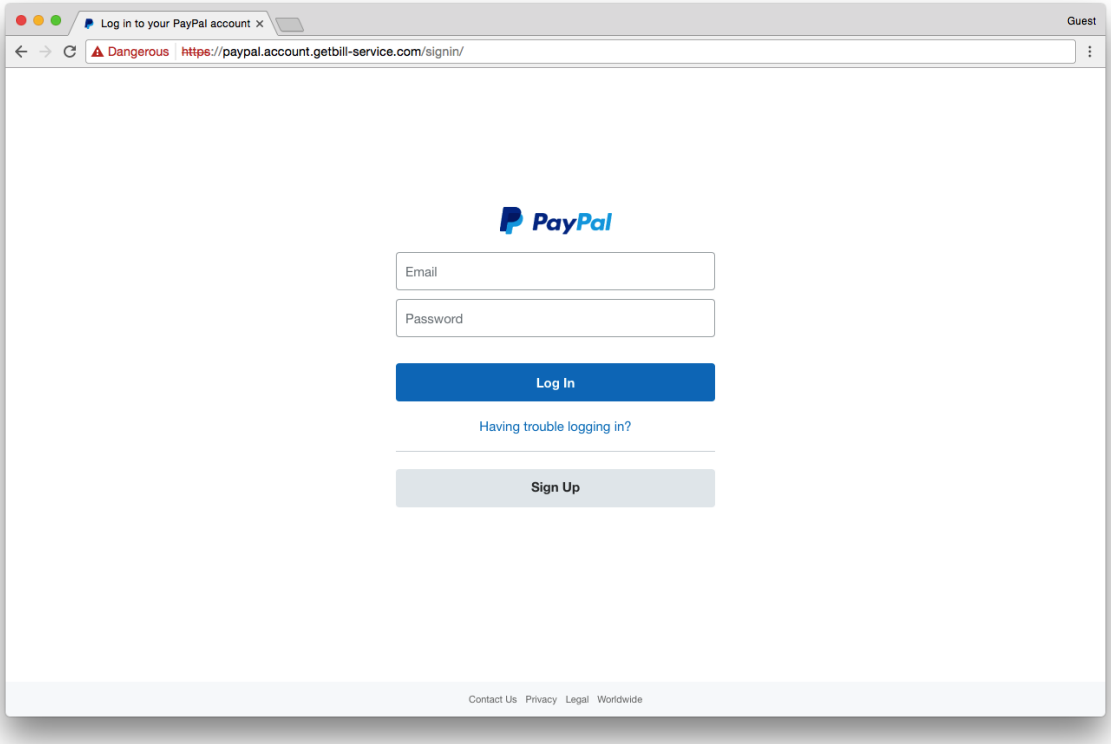
What does that mean?

Well, let's look at an example. An attacker may start by sending you a formal looking email from an address that resembles an official account. It may say something like, "an attempt to login to your account has been made from another country, please update your password."

In fact, that's exactly how John Podesta, the chairman of Hillary's Clinton's presidential campaign, had his email account compromised.




That email included a link to a specially designed page that is a perfect replication of the Google login page. To the untrained eye, it's almost impossible to tell the fake site from the real one. You can see how similar tactics could be used to steal financial information or medical data. Here's an example of a fake PayPal login screen:




And with the advent of free SSL services and recent changes to browser indicators, it's becoming easier than ever to disguise phishing sites as legitimate.

UPDATE: Google has now changed its browser UI to be less misleading.

## Other Types of Cyber Attacks to Be Aware Of

Phishing is amongst the most prevalent, but not the only type of attack that you need to be wary of on the internet. Here are some examples of other types of internet malfeasance:

- **Third-Party Content Injection** – The most common example of this is over public WiFi hotspots. Have you ever noticed an abundance of extra ads or pop-ups (on websites that don't normally contain them) when you're at the mall or the airport? This is an example of third-party content injection. Because the website lacks SSL, the ISP can inject its own content onto the site. This means you're not seeing the site as it's intended. And if the third-party has negative intentions, it can inject harmful content.
- **Eavesdropping** – Similar to phishing, if an attacker knows how, they can eavesdrop on a connection and steal any information being transmitted. This underscores the need for connection security—without it, everything you send online can be intercepted and stolen by anyone who wants it.
- **Good Old-Fashioned Fraud** – Ever seen a 20-dollar iPad? Neither have we. Now, that doesn't mean you won't see websites advertise them—they just almost never exist. In all likelihood you're about to wire money to an account in the Philippines. Staring longingly at that low-res image on the pop-up ad is the closest you'll ever get to actually owning the tablet.

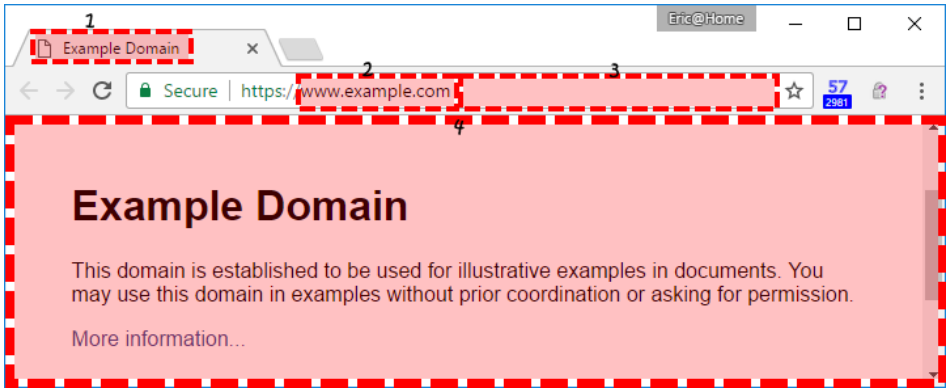
## 5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam

Here are 5 ways to determine if a website is fake – plus some additional tips to stay safe online.

## 1. Pay Close Attention to the URL

You would be absolutely shocked how many people pay little to no attention to the address bar of their browser. This is a huge mistake. The address bar contains a ton of vital information about where you are and how secure you are there. So get into the habit of occasionally glancing up there whenever you visit a new page.

In fact, most of the browsers abide a concept called the Line of Death. The idea is that a user should never trust anything below a certain point on the browser, the so-called line of death. An attacker can control everything below the line (and even some things above it) so you have to know where to look for reliable information.




The areas that an attacker can control are highlighted in red and numbered. Let's go over them really quickly:

1. The Favicon – Websites can put whatever icon they want in the tab.
2. Domain Name – This is part of the URL and it's trustworthy, as long as you know what you're looking for (more on that in a second).
3. File path/Director – Ditto.
4. Web content area – This can be whatever the attacker wants it to be, including a very convincing spoof of a legitimate website.

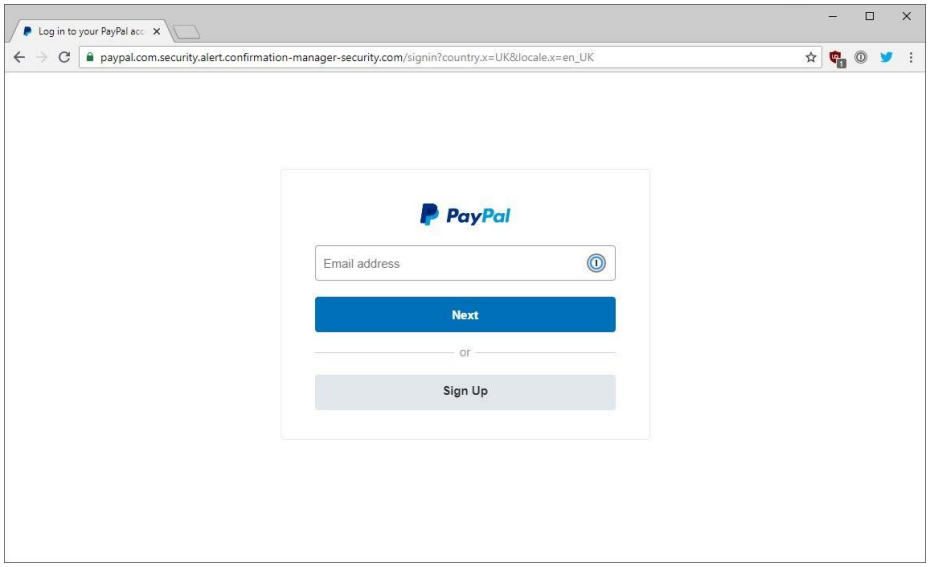
One of the chief tactics in phishing is to create a website that is almost indistinguishable from the real thing. In order to do this, hackers and cybercriminals have gotten very ingenious in the ways they copy URLs. Between the ability to create sub-domains that mimic real domains and how browsers can confusingly shorten URLs, it's easy to get duped.

**Related**: *What is Unicode Phishing?*

In order to know what to look for when examining the URL, you need to know how a URL is constructed.


**Related**: *Secure Your Domain & Sub-Domains with a RapidSSL Wildcard Certificate.*

Now, armed with that knowledge, always make sure that you know what the actual domain you're on is. Sub-domains can be misleading. Here's an example of a first- and second-level sub-domain that intentionally mimic a domain and TLD:




This URL is designed to look like it's PayPal.com, but if you look closer you'll notice that those are sub-domains, the name of the actual domain is "confirmation-manager-security." Remember, the real domain name appears right before the TLD (e.g. .com/). This is not really PayPal. This is a phishing site. Notice how it still displays the little green padlock thanks to the use of an SSL certificate?

That's why you always have to check the URL.

## 2. Check Connection Security Indicators

Back to the address bar. If the last point didn't underscore the importance of this browser feature—this one should drive the point home. Within the address bar are several connection indicators that let you know whether your connection with this website is private. As we mentioned earlier, it's possible to eavesdrop on connections on the internet.


The internet was built on HTTP, or the hypertext transfer protocol. When HTTP was first defined the internet was not used for commercial activity. In fact, commercial activity on the internet was actually illegal at the time. The internet was primarily supposed to be a platform for the free exchange of information between academia and the government. Any communication done via HTTP is sent in plaintext and can be intercepted, manipulated, stolen—you name it.

In order to remedy this, SSL or Secure Sockets Layer was developed. SSL was later succeeded by TLS or Transport Layer Security. Today, we colloquially refer to both as SSL.

At any rate, HTTP + TLS = HTTPS, which is a secure version of HTTP that prevents communication from being intercepted and read by anyone but you and the website you are connected to. That's a lot of information, but what you really need to know is this:

HTTP = Bad
HTTPS = Good

Never trust an HTTP website with your personal information.

Now, let's get to connection security indicators. You want to look for one of the two following indicators:

**The Padlock Icon**

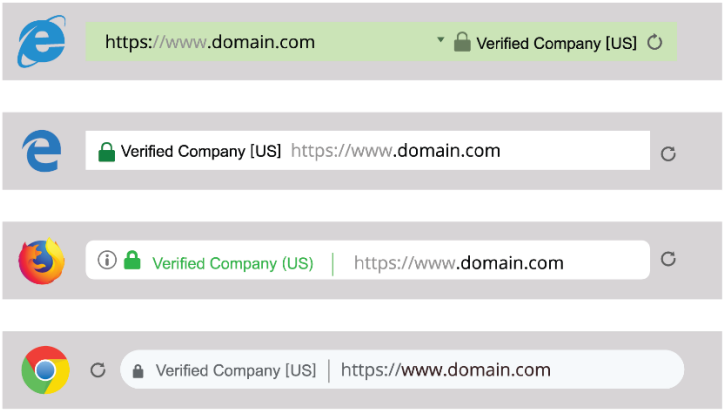

**Or, the EV Name Badge/Green Address Bar**


Both of these icons indicate that the website is using HTTPS and that you have a secure connection. If you see either of these, your connection is secure and you are communicating privately with the website listed in the URL.

Remember, most secure connections will have the padlock icon, but some may *also* have the Green Address Bar. Or rather, it used to be uniformly green. Nowadays, different browsers display the EV Name Badge in different ways.

The Green Address Bar/EV Name Badge is only shown when a website is using a specific type of SSL certificate known as an Extended Validation (EV) SSL Certificate. This certificate allows a website to assert its identity and prove it is operated by a real-world, legally incorporated company. Browsers give websites with EV SSL certificates preferential treatment by displaying the company name to the left of the URL. When you see an EV Name Badge, you can relax—you're secure. The green address bar cannot be faked, it is un-impugnable proof of identity—and by extension trustworthiness.

The exact appearance of EV name badge varies by browser. Sometimes the name is written in green, sometimes it is inside a green rectangle and sometimes it's not green at all. Here are a few examples of how EV certificates look in popular browsers:




It's possible for a URL to have HTTPS in it but for the padlock icon not to appear correctly, too. This indicates that there is some security issue with the connection – usually mixed content, when a site is still loading some assets that are HTTP – and represents a cause for concern. If this is the case, it's best to assume you do not have a secure connection.


You will now see the "Not Secure" warning on all websites that are being served via HTTP as of July of 2018, too. This will give you an immediate visual indication that your connection is not secure.


Now, one more thing: A secure connection doesn't necessarily equate to a safe website. Lots of fake websites use free SSL certificates. Think of it like this:

- You should only visit sites that use HTTPS
- Just because a site has HTTPS, doesn't mean you can automatically trust it.

Just because the connection is secure (which should be mandatory), you don't necessarily know who is on the other end of that connection. Outside of Extended Validation SSL and the EV Name Badge, which can be trusted on site, you'll need to do a little more sleuthing to make sure the site is legitimate. To verify a website's HTTPS connection, you can also try this SSL checker tool.

## 3. View Certificate Details

This one is a bit more advanced because it involves diving a bit deeper into your browser's menu and that can be misleading if you don't have a proper understanding of SSL.

If a website doesn't have the green address bar, the most that you can tell from the presence of security connection indicators is that your connection is secure. That means no third party can eavesdrop and steal information. But as we just discussed, it doesn't mean you're safe, though.

That's because you don't know who is on the other end of the connection, yet.

Fortunately, that information might be available. Here's how to find it:

Most browsers (like Safari and Firefox) allow you to view the certificate by clicking the padlock icon in the address bar.

**For Firefox:**

- Click the Padlock icon
- Click "More Information"
- Click "View Certificate"

**For Safari:**

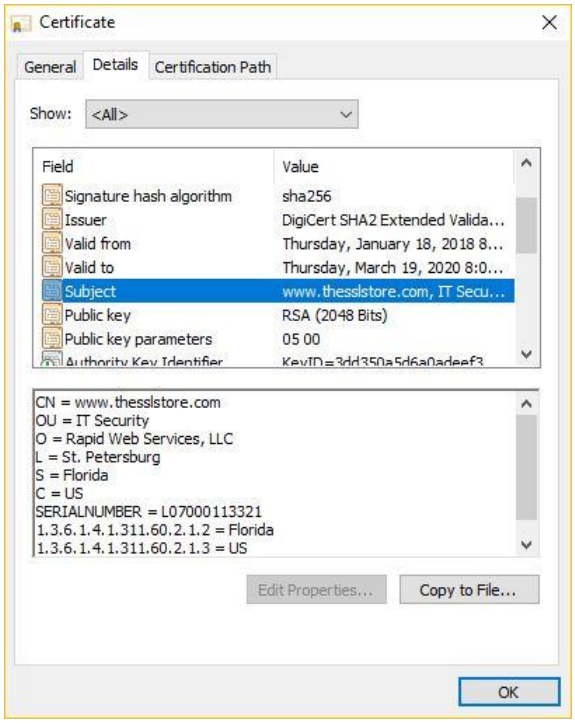
- Click the Padlock icon
- Click "View Certificate"

**For Chrome:**

- Click the Three Dots icon to bring up the menu
- Under "More Tools" select "Developer Tools."
- Click on the Security tab
- Click "View Certificate."
  -or-
- Click the Padlock icon
- Click "View Certificate" (Google returned to making certificate details available by clicking the padlock last year)

When you click on the certificate information, you will get all of the information the CA verified before it issued the certificate.

Once you have the certificate details open you want to look for the following field: Subject.




The Subject is the website or organization that the certificate is representing. Depending on the type of certificate (DV, OV, or EV) you will see different amounts of information in the Subject.

A DV certificate will just have a domain name. An OV certificate will include limited company information (a name, a state/province and country). An EV will have detailed company information, such as an exact street address. You can recognize an EV certificate if the browser is displaying the EV Name Badge. Extended Validation offers the most information—that's why it has a special visual indicator.

If an organization has an OV SSL certificate – which is recommended as a baseline for e-commerce businesses, financial institutions, etc. – then you will be able to see verified business details in the certificate information. Provided the website is registered to the right company, you're fine. You can probably trust this site.

If it doesn't, then you need to be careful.

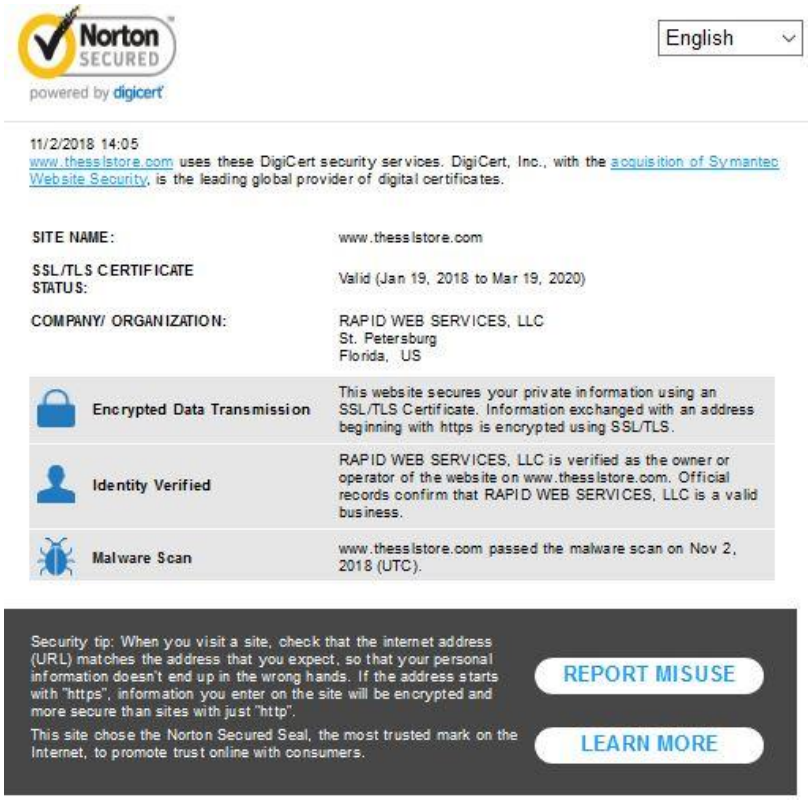
There's also the possibility that this information isn't supplied at all. If that's the case then the website only has a Domain Validated SSL certificate. This doesn't mean you should automatically distrust the website, but it does mean you need to continue to be skeptical until the site can prove its legitimacy.

## 4. Look for Trust Seals

When a company or organization makes a substantial investment in their customers' security, they typically want a little bit of credit for it. That's one of several reasons that trust seals exist. You've probably seen more than a few trust seals in your time on the internet. They look like this:


Trust seals are commonly placed on homepages, login pages, and checkout pages. They're immediately recognizable and they remind visitors that they are secure on this page. It's not unlike putting a sign in your yard or a sticker in your window that advertises your security system. People know what they mean as soon as they see them.

**But did you know you can click on them too?**




That's right, most SSL certificates come with trust seals that will display verified information when clicked on. This is important because it lets you know that the SSL certificate is in good standing and might also inform you of additional security mechanisms in place like malware scans or vulnerability assessments. SSL/TLS certificates aren't the only products that comes with site seals, either.

But, just seeing the site seal isn't enough, it is essential that you click on it to verify it's legitimate.

## 5. Consult the Google Safe Browsing Transparency Report

This is the last resort, but it serves as a nice final safeguard: Google it. Literally. The Google Safe Browsing Transparency Report allows you to copy and paste the URL into a field and it gives you a report on whether or not you can trust that website. It's not especially fancy, nor does it boast impressive aesthetics, but it certainly is an effective way to determine whether or not a site is unsafe.

Granted, this isn't the end-all, be-all. Google does occasionally miss stuff. But not for long. When you're as ubiquitous as Google, nothing escapes your view for long. Google's Safe Browsing service is amongst the best on the internet when it comes to keeping users safe. If you're ever in doubt, Google it.

## Bonus! You can learn a lot from a Privacy Policy

Right now, in 2018, people are as attuned to their privacy and data security as they have ever been. A big part of that stems from the litany of new privacy regulations that have being instituted the world over– regulations like GDPR. These efforts to legally require companies to safeguard our data and be more transparent have provided an additional, unforeseen benefit, too: it's now a lot easier to tell a legitimate company or organization from a fraudster.

It starts with the Privacy Policy, no matter where you are — what jurisdiction — organizations are required to provide certain information in their privacy policies. The nice part about this information is you can check it, verify it and make sure that you are dealing with real people and a real website.

Let's start with a simple binary: is this a passable Privacy Policy? You may not be a connoisseur of privacy pages but chances are you have seen enough of them to be able to tell a real one from something more dubious. The easiest way to check is to look for actual specific information: names of officers or employees, addresses, ways to get in contact and participation in specific programs.

A good example of this would be the EU-US and Swiss-US Privacy Shield program run by the US Department of Commerce, the Department of Transportation and the FTC. US companies that have partners in Europe are oftentimes required to certify themselves in order to comply with the EU's General Data Protection Regulation. The Privacy Shield has an official list that you can check to verify an organization's participation, too. Check that list. If you see the company there, you're set.


If they claim to be certified and they're not, they're breaking the law by misrepresenting themselves, which should give you pause. Even if this is a legitimate website, is this the kind of outfit you want to give your business to?

# 8 More Internet Tips to Help you Spot Fake or Fraudulent Websites

This next section might as well be called our common sense section. That being said, you'd be genuinely surprised how many people ignore this stuff on a regular basis. Here are eight more tips to help keep you safe online.

## Trust Your Browser

The browsers are our portal to the internet. We can only go where they take us, and sometimes they don't want to take us certain places. Do yourself a favor and listen to them when they suggest you not go to a website. Whether it's Chrome or Firefox or even Edge or Safari – they all let you know when you're about to stray to somewhere unsavory. And this isn't just guesswork, either. This is based on data and user reports that clearly indicate a threat. So take that threat seriously: listen to your browser.

Bonus Tip: Despite bad advice from plenty of other articles, NEVER disable your antivirus or drop your firewall. Ever.

## Look for Bad English

Good websites take pride in themselves. That means the graphics look sharp, the spelling and grammar is on point and the entire experience feels streamlined and polished. If you're on a website that feels like it was written by someone with a third-grade education – or by someone who doesn't speak English as a first language – you may want to be a little bit wary. Especially if those mistakes appear on important pages.

Everyone makes the occasional mistakes—even big companies. But at the point the mistakes become egregious you need to beware.

## Look at the Contact Us Section

Another telltale sign when it comes to whether or not a website is fake or not can be found on its "Contact Us" section. How much information is there? Is an address supplied? What about a phone number? Does that line actually connect to the company? The more information that is supplied, the more confident you should feel—provided it's actually good information. If all they're giving you is an email address or, worse, there's no contact information whatsoever—run.

And remember to verify the information. Google the address, maybe even check out street view. See if any employee that's listed has a LinkedIn profile. Do a little homework.

## Is there an Over-Abundance of Ads?

Ads are a fact of life. No matter where you go, you're going to run into ads. But if you're on a website that is more ads than content, tread carefully. If you have to click several links to get through intrusive pop-ups and redirects to reach the intended page—you're

on a website that is probably fake or at least scamming. There's a fine line between UX and selling ads. When it's clear that a website has no regard for that line, you need to be wary.

## Check the Who.Is

This is another tip for advanced users.

If you really want to know who is running a website there is a database called Who.Is that can tell you what email address it's registered to. There are a number of free sites that allow you to check a website's official WHO.IS registration, though GDPR concerns have complicated access lately.

A WHO.IS registration can tell you the owner of a website and if it's an individual or a company. If it's a company there will be an "Organization" listed along with an address and phone number. For an individual, there will be a "Name" listed along with an address.

This can be an invaluable tool, especially when you're dealing with brands. If you're at a website that claims to be owned by a large company but is registered to some address in another country, there's a good chance you're on a fake website.

## Check the Shipping and Return Policy

Any legitimate e-commerce company is going to have a shipping and return policy, it's considered a best practice. So any website that purports to be selling something but lacks this documentation is automatically suspect. Likewise, if you click the link and the policy looks flimsy or has been copy-and-pasted directly from another website, that's also suspect. Look, we're not telling you to read the whole thing – nor are we naïve enough to believe you would – but a quick look should tell you all you need to know.

## What forms of payment do they accept?

This is another tip that is more for e-commerce, but what forms of payment does the website offer to accept? Most legitimate companies will take major credit cards and typically have a couple of non-payment card options, too. If a website is asking you to send money to a random PayPal address, wire it by Western Union, pay in iTunes gift cards or only deals in cryptocurrency, that should send up a red flag. The majority of the time, those methods are done to avoid scrutiny and ensure that a transaction can't be reversed. Remember, a legitimate website would have nothing to hide and likely wouldn't participate in this kind of suspicious business practice.

## Check for a Digital Footprint

The beautiful thing about the internet is that nothing exists in a vacuum. Chances are other people have had experiences with this company and – good or bad – they have shared those experiences somewhere. With just a tiny bit of digging, you can probably figure out if a website is fake based on reviews alone. Google the name of the site along with "+ reviews." Check with the Better Business Bureau, or one of the myriad scam

sites that exist to protect consumers. Just look a little. The internet may not be the best at telling you whether something is good, but it can definitely tell you when something is bad. And all it takes to find out is about three minutes and Google.

## Where to Report Fake or Fraudulent Websites

We encourage you to report fake websites. It's good for the internet, it's good for your inner chi and if you're petty—it gives you that good tingly feeling. Here's where to report malicious websites:

- Google – Safe Browsing
- Mozilla – Protect the Fox

Microsoft gives its users an opportunity to report malicious sites within its browsers. To do this go to the Tools/Safety menu, select Phishing Filter/SmartScreen Filter and click "Report Unsafe Website."

## A Final Word

It's possible that after reading this guide you're feeling a little uneasy. That's not the point we were trying to make. The internet is an amazing place and you can use it for a countless number of worthwhile activities. But, much like anything else in life, there are some dangers. Don't let that dissuade you, as long as you stay vigilant you're not likely to run into many problems.

Just stay on the beaten path, trust websites that have made an investment in authentication and be careful if you ever get the sense that something might be off.

# Internet

By Britannica

## What is the Internet?

The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection.

## Who invented the Internet?

The Internet consists of technologies developed by different individuals and organizations. Important figures include Robert W. Taylor, who led the development of the ARPANET (an early prototype of the Internet), and Vinton Cerf and Robert Kahn, who developed the Transmission Control Protocol/Internet Protocol (TCP/IP) technologies.

## How does the Internet work?

The Internet works through a series of networks that connect devices around the world through telephone lines. Users are provided access to the Internet by Internet service providers. The widespread use of mobile broadband and Wi-Fi in the 21st century has allowed this connection to be wireless.

## Is the Internet dangerous?

The advent of the Internet has brought into existence new forms of exploitation, such as spam e-mail and malware, and harmful social behaviour, such as cyberbullying and doxxing. Many companies collect extensive information from users, which some deem a violation of privacy.

## What is the Dark Web?

The Dark Web refers to a series of Web sites that require special decryption and configuration tools to access. It is most commonly used for purposes that require strict anonymity, including illegal sales (e.g., of weapons and drugs), political dissent in countries with heavy censorship, and whistleblowing.

## Who controls the Internet?

While the Internet is theoretically decentralized and thus controlled by no single entity, many argue that tech companies such as Amazon, Facebook, and Google represent a small concentration of organizations that have unprecedented influence over the information and money on the Internet. In some countries, certain parts of the Internet are blocked via censorship.

## Is the Internet “making us stupid”?

Whether the Internet is "making us stupid" is widely debated. Some argue the Internet is reprogramming our brains for the worse, as seen by diminishing IQ scores, and that new technologies and platforms like the Internet are harming attention spams, the ability to concentrate, and perform simple tasks. Others argue that virtually all new technologies throughout history have been initially feared, that the Internet gives voice to diverse

populations and equal access to information for the benefit of social advancement, and that changing how the brain works and how we access and process information is not necessarily bad. For more on the debate about whether the Internet is "making us stupid," visit ProCon.org.

### Is cancel culture (or “callout culture”) good for society?

Whether cancel culture is good for society is widely debated. Some argue it allows the public and marginalized people to seek accountability in their leaders, gives a voice to disenfranchised or less powerful people, and is simply a new form of boycott. Others see cancel culture as a dangerous form of bullying, a suppression of free speech, and a form of intolerance that harms democratic societies by excluding and ostracizing anyone with contrary views. For more on the cancel culture debate, visit ProCon.org.

**Internet**, a system architecture that has revolutionized mass communication, mass media, and commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a “network of networks,” the Internet emerged in the United States in the 1970s but did not become visible to the general public until the early 1990s. By 2020, approximately 4.5 billion people, or more than half of the world’s population, were estimated to have access to the Internet. And that number is growing, largely due to the prevalence of “smart” technology and the "Internet of Things," where computer-like devices connect with the Internet or interact via wireless networks. These “things” include smartphones, appliances, thermostats, lighting systems, irrigation systems, security cameras. vehicles, even cities.

The Internet provides a capability so powerful and general that it can be used for almost any purpose that depends on information, and it is accessible by every individual who connects to one of its constituent networks. It supports human communication via social media, electronic mail (e-mail), “chat rooms,” newsgroups, and audio and video transmission and allows people to work collaboratively at many different locations. It supports access to digital information by many applications, including the World Wide Web. The Internet has proved to be a spawning ground for a large and growing number of “e-businesses” (including subsidiaries of traditional “brick-and-mortar” companies) that carry out most of their sales and services over the Internet. (*See* electronic commerce.)

# Origin and development


## Early networks

How does the Internet really work?

See all videos for this article

The first computer networks were dedicated special-purpose systems such as SABRE (an airline reservation system) and AUTODIN I (a defense command-and-control system), both designed and implemented in the late 1950s

and early 1960s. By the early 1960s computer manufacturers had begun to use semiconductor technology in commercial products, and both conventional batch-processing and time-sharing systems were in place in many large, technologically advanced companies. Time-sharing systems allowed a computer's resources to be shared in rapid succession with multiple users, cycling through the queue of users so quickly that the computer appeared dedicated to each user's tasks despite the existence of many others accessing the system "simultaneously." This led to the notion of sharing computer resources (called host computers or simply hosts) over an entire network. Host-to-host interactions were envisioned, along with access to specialized resources (such as supercomputers and mass storage systems) and interactive access by remote users to the computational powers of time-sharing systems located elsewhere. These ideas were first realized in ARPANET, which established the first host-to-host network connection on October 29, 1969. It was created by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. ARPANET was one of the first general-purpose computer networks. It connected time-sharing computers at government-supported research sites, principally universities in the United States, and it soon became a critical piece of infrastructure for the computer science research community in the United States. Tools and applications—such as the simple mail transfer protocol (SMTP, commonly referred to as e-mail), for sending short messages, and the file transfer protocol (FTP), for longer transmissions—quickly emerged. In order to achieve cost-effective interactive communications between computers, which typically communicate in short bursts of data, ARPANET employed the new technology of packet switching. Packet switching takes large messages (or chunks of computer data) and breaks them into smaller, manageable pieces (known as packets) that can travel independently over any available circuit to the target destination, where the pieces are reassembled. Thus, unlike traditional voice communications, packet switching does not require a single dedicated circuit between each pair of users.

Commercial packet networks were introduced in the 1970s, but these were designed principally to provide efficient access to remote computers by dedicated terminals. Briefly, they replaced long-distance modem connections by less-expensive "virtual" circuits over packet networks. In the United States, Telenet and Tymnet were two such packet networks. Neither supported host-to-host communications; in the 1970s this was still the province of the research networks, and it would remain so for many years.




DARPA (Defense Advanced Research Projects Agency; formerly ARPA) supported initiatives for ground-based and satellite-based packet networks. The ground-based packet radio system provided mobile access to computing resources, while the packet satellite network connected the United States with several European countries and enabled connections with widely dispersed and remote regions. With the introduction of packet radio, connecting a mobile terminal to a computer network became feasible. However, time-sharing systems were then still too large,

unwieldy, and costly to be mobile or even to exist outside a climate-controlled computing environment. A strong motivation thus existed to connect the packet radio network to ARPANET in order to allow mobile users with simple terminals to access the time-sharing systems for which they had authorization. Similarly, the packet satellite network was used by DARPA to link the United States with satellite terminals serving the United Kingdom, Norway, Germany, and Italy. These terminals, however, had to be connected to other networks in European countries in order to reach the end users. Thus arose the need to connect the packet satellite net, as well as the packet radio net, with other networks.

## Foundation of the Internet

The Internet resulted from the effort to connect various research networks in the United States and Europe. First, DARPA established a program to investigate the interconnection of "heterogeneous networks." This program, called Internetting, was based on the newly introduced concept of open architecture networking, in which networks with defined standard interfaces would be interconnected by "gateways." A working demonstration of the concept was planned. In order for the concept to work, a new protocol had to be designed and developed; indeed, a system architecture was also required.

In 1974 Vinton Cerf, then at Stanford University in California, and this author, then at DARPA, collaborated on a paper that first described such a protocol and system architecture—namely, the transmission control protocol (TCP), which enabled different types of machines on networks all over the world to route and assemble data packets. TCP, which originally included the Internet protocol (IP), a global addressing mechanism that allowed routers to get data packets to their ultimate destination, formed the TCP/IP standard, which was adopted by the U.S. Department of Defense in 1980. By the early 1980s the "open architecture" of the TCP/IP approach was adopted and endorsed by many other researchers and eventually by technologists and businessmen around the world.

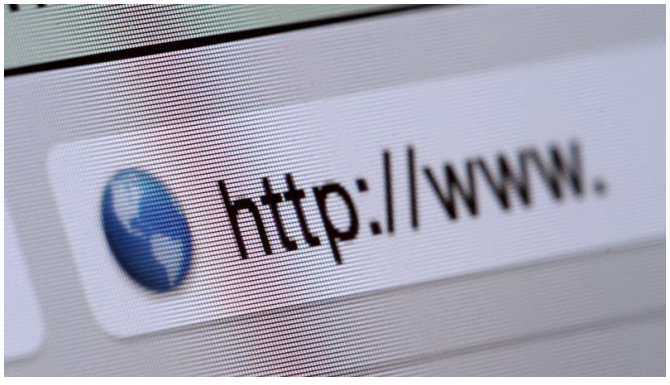
By the 1980s other U.S. governmental bodies were heavily involved with networking, including the National Science Foundation (NSF), the Department of Energy, and the National Aeronautics and Space Administration (NASA). While DARPA had played a seminal role in creating a small-scale version of the Internet among its researchers, NSF worked with DARPA to expand access to the entire scientific and academic community and to make TCP/IP the standard in all federally supported research networks. In 1985–86 NSF funded the first five supercomputing centres—at Princeton University, the University of Pittsburgh, the University of California, San Diego, the University of Illinois, and Cornell University. In the 1980s NSF also funded the development and operation of the NSFNET, a national "backbone" network to connect these centres. By the late 1980s the network was operating at millions of bits per second. NSF also funded various nonprofit local and regional networks to connect other users to the NSFNET. A few commercial networks also began in the late 1980s; these were soon joined by others, and the Commercial Internet Exchange (CIX) was formed to allow transit traffic between commercial networks that otherwise would not have been allowed on the NSFNET backbone. In 1995, after extensive review of the situation, NSF decided that support of the NSFNET infrastructure was no longer required, since many commercial providers were now willing and able to meet the needs of the research community,

and its support was withdrawn. Meanwhile, NSF had fostered a competitive collection of commercial Internet backbones connected to one another through so-called network access points (NAPs).

From the Internet's origin in the early 1970s, control of it steadily devolved from government stewardship to private-sector participation and finally to private custody with government oversight and forbearance. Today a loosely structured group of several thousand interested individuals known as the Internet Engineering Task Force participates in a grassroots development process for Internet standards. Internet standards are maintained by the nonprofit Internet Society, an international body with headquarters in Reston, Virginia. The Internet Corporation for Assigned Names and Numbers (ICANN), another nonprofit, private organization, oversees various aspects of policy regarding Internet domain names and numbers.

## Commercial expansion

The rise of commercial Internet services and applications helped to fuel a rapid commercialization of the Internet. This phenomenon was the result of several other factors as well. One important factor was the introduction of the personal computer and the workstation in the early 1980s—a development that in turn was fueled by unprecedented progress in integrated circuit technology and an attendant rapid decline in computer prices. Another factor, which took on increasing importance, was the emergence of Ethernet and other "local area networks" to link personal computers. But other forces were at work too. Following the restructuring of AT&T in 1984, NSF took advantage of various new options for national-level digital backbone services for the NSFNET. In 1988 the Corporation for National Research Initiatives received approval to conduct an experiment linking a commercial e-mail service (MCI Mail) to the Internet. This application was the first Internet connection to a commercial provider that was not also part of the research community. Approval quickly followed to allow other e-mail providers access, and the Internet began its first explosion in traffic.




How was the Internet invented?

See all videos for this article

In 1993 federal legislation allowed NSF to open the NSFNET backbone to commercial users. Prior to that time, use of the backbone was subject to an "acceptable use" policy, established and administered by NSF, under which commercial use was limited to those applications that served the research community. NSF recognized that commercially supplied network services, now that they were available, would ultimately be far less expensive than continued funding of special-purpose network services.

Also in 1993 the University of Illinois made widely available Mosaic, a new type of computer program, known as a browser, that ran on most types of computers and,

through its “point-and-click” interface, simplified access, retrieval, and display of files through the Internet. Mosaic incorporated a set of access protocols and display standards originally developed at the European Organization for Nuclear Research (CERN) by Tim Berners-Lee for a new Internet application called the World Wide Web (WWW). In 1994 Netscape Communications Corporation (originally called Mosaic Communications Corporation) was formed to further develop the Mosaic browser and server software for commercial use. Shortly thereafter, the software giant Microsoft Corporation became interested in supporting Internet applications on personal computers (PCs) and developed its Internet Explorer Web browser (based initially on Mosaic) and other programs. These new commercial capabilities accelerated the growth of the Internet, which as early as 1988 had already been growing at the rate of 100 percent per year.

By the late 1990s there were approximately 10,000 Internet service providers (ISPs) around the world, more than half located in the United States. However, most of these ISPs provided only local service and relied on access to regional and national ISPs for wider connectivity. Consolidation began at the end of the decade, with many small to medium-size providers merging or being acquired by larger ISPs. Among these larger providers were groups such as America Online, Inc. (AOL), which started as a dial-up information service with no Internet connectivity but made a transition in the late 1990s to become the leading provider of Internet services in the world—with more than 25 million subscribers by 2000 and with branches in Australia, Europe, South America, and Asia. Widely used Internet “portals” such as AOL, Yahoo!, Excite, and others were able to command advertising fees owing to the number of “eyeballs” that visited their sites. Indeed, during the late 1990s advertising revenue became the main quest of many Internet sites, some of which began to speculate by offering free or low-cost services of various kinds that were visually augmented with advertisements. By 2001 this speculative bubble had burst.

## The 21st century and future directions

What is net neutrality?

See all videos for this article

After the collapse of the Internet bubble came the emergence of what was called “Web 2.0,” an Internet with emphasis on social networking and content generated by users, and cloud computing. Social media services such as Facebook, Twitter, and Instagram became some of the most popular Internet sites through allowing users to share their own content with their friends and the wider world. Mobile phones became able to access the Web, and, with the introduction of smartphones like Apple’s iPhone (introduced in 2007), the number of Internet users worldwide exploded from about one sixth of the world population in 2005 to more than half in 2020.

The increased availability of wireless access enabled applications that were previously uneconomical. For example, global positioning systems (GPS) combined with wireless Internet access help mobile users to locate alternate routes, generate precise accident reports and initiate recovery services, and improve traffic management and congestion control. In addition to smartphones, wireless laptop computers, and personal digital assistants (PDAs), wearable devices with voice input and special display glasses were developed.

While the precise structure of the future Internet is not yet clear, many directions of growth seem apparent. One is toward higher backbone and network access speeds. Backbone data rates of 100 billion bits (100 gigabits) per second are readily available today, but data rates of 1 trillion bits (1 terabit) per second or higher will eventually become commercially feasible. If the development of computer hardware, software, applications, and local access keeps pace, it may be possible for users to access networks at speeds of 100 gigabits per second. At such data rates, high-resolution video—indeed, multiple video streams—would occupy only a small fraction of available bandwidth. Remaining bandwidth could be used to transmit auxiliary information about the data being sent, which in turn would enable rapid customization of displays and prompt resolution of certain local queries. Much research, both public and private, has gone into integrated broadband systems that can simultaneously carry multiple signals—data, voice, and video. In particular, the U.S. government has funded research to create new high-speed network capabilities dedicated to the scientific-research community.

It is clear that communications connectivity will be an important function of a future Internet as more machines and devices are interconnected. In 1998, after four years of study, the Internet Engineering Task Force published a new 128-bit IP address standard intended to replace the conventional 32-bit standard. By allowing a vast increase in the number of available addresses ($2^{128}$, as opposed to $2^{32}$), this standard makes it possible to assign unique addresses to almost every electronic device imaginable. Thus, through the "Internet of things," in which all machines and devices could be connected to the Internet, the expressions "wired" office, home, and car may all take on new meanings, even if the access is really wireless.

The dissemination of digitized text, pictures, and audio and video recordings over the Internet, primarily available today through the World Wide Web, has resulted in an information explosion. Clearly, powerful tools are needed to manage network-based information. Information available on the Internet today may not be available tomorrow without careful attention's being paid to preservation and archiving techniques. The key to making information persistently available is infrastructure and the management of that infrastructure. Repositories of information, stored as digital objects, will soon populate the Internet. At first these repositories may be dominated by digital objects specifically created and formatted for the World Wide Web, but in time they will contain objects of all kinds in formats that will be dynamically resolvable by users' computers in real time. Movement of digital objects from one repository to another will still leave them available to users who are authorized to access them, while replicated instances of objects in multiple repositories will provide alternatives to users who are better able to interact with certain parts of the Internet than with others. Information will have its own identity and, indeed, become a "first-class citizen" on the Internet.

*Robert Kahn*

## Society and the Internet

What began as a largely technical and limited universe of designers and users became one of the most important mediums of the late 20th and early 21st centuries. As the Pew Charitable Trust observed in 2004, it took 46 years to wire 30 percent of the United States for electricity; it took only 7 years for the Internet to reach that same level of connection to American homes. By 2005, 68 percent of American adults and 90 percent of American teenagers had used the Internet. Europe and Asia were at least as well connected as the United States. Nearly half of the citizens of the European Union are online, and even higher rates are found in the Scandinavian countries. There is a wide variance in Asian countries; for example, by 2005 Taiwan, Hong Kong, and Japan had at least half of their populations online, whereas India, Pakistan, and Vietnam had less than 10 percent. South Korea was the world leader in connecting its population to the Internet through high-speed broadband connections.

Such statistics can chart the Internet's growth, but they offer few insights into the changes wrought as users—individuals, groups, corporations, and governments—have embedded the technology into everyday life. The Internet is now as much a lived experience as a tool for performing particular tasks, offering the possibility of creating an environment or virtual reality in which individuals might work, socially interact with others, and perhaps even live out their lives.

# History, community, and communications

# Two agendas

The Internet has evolved from the integration of two very different technological agendas—the Cold War networking of the U.S. military and the personal computer (PC) revolution. The first agenda can be dated to 1973, when the Defense Advanced Research Projects Agency (DARPA) sought to create a communications network that would support the transfer of large data files between government and government-sponsored academic-research laboratories. The result was the ARPANET, a robust decentralized network that supported a vast array of computer hardware. Initially, ARPANET was the preserve of academics and corporate researchers with access to time-sharing mainframe computer systems. Computers were large and expensive; most computer professionals could not imagine anyone needing, let alone owning, his own "personal" computer. And yet Joseph Licklider, one of the driving forces at DARPA for computer networking, stated that online communication would "change the nature and value of communication even more profoundly than did the printing press and the picture tube."

The second agenda began to emerge in 1977 with the introduction of the Apple II, the first affordable computer for individuals and small businesses. Created by Apple Computer, Inc. (now Apple Inc.), the Apple II was popular in schools by 1979, but in the corporate market it was stigmatized as a game machine. The task of cracking the business market fell to IBM. In 1981 the IBM PC was released and immediately standardized the PC's basic hardware and operating system—so much so that first *PC-compatible* and then simply *PC* came to mean any personal computer built

along the lines of the IBM PC. A major centre of the PC revolution was the San Francisco Bay area, where several major research institutions funded by DARPA—Stanford University, the University of California, Berkeley, and Xerox PARC—provided much of the technical foundation for Silicon Valley. It was no small coincidence that Apple's two young founders—Steven Jobs and Stephen Wozniak—worked as interns in the Stanford University Artificial Intelligence Laboratory and at the nearby Hewlett-Packard Company. The Bay Area's counterculture also figured prominently in the PC's history. Electronic hobbyists saw themselves in open revolt against the "priesthood" of the mainframe computer and worked together in computer-enthusiast groups to spread computing to the masses.


**Britannica Quiz**

What Do You Actually Know About the Internet?

## The WELL

Why does this matter? The military played an essential role in shaping the Internet's architecture, but it was through the counterculture that many of the practices of contemporary online life emerged. A telling example is the early electronic bulletin board system (BBS), such as the WELL (Whole Earth 'Lectronic Link). Established in 1985 by American publisher Stewart Brand, who viewed the BBS as an extension of his *Whole Earth Catalog*, the WELL was one of the first electronic communities organized around forums dedicated to particular subjects such as parenting and Grateful Dead concerts. The latter were an especially popular topic of online conversation, but it was in the parenting forum where a profound sense of community and belonging initially appeared. For example, when one participant's child was diagnosed with leukemia, members of the forum went out of their way either to find health resources or to comfort the distressed parents. In this one instance, several features still prevalent in the online world can be seen. First, geography was irrelevant. WELL members in California and New York could bring their knowledge together within the confines of a forum—and could do so collectively, often exceeding the experience available to any local physician or medical centre. This marshaling of shared resources persists to this day as many individuals use the Internet to learn more about their ailments, find others who suffer from the same disease, and learn about drugs, physicians, and alternative therapies.

Another feature that distinguished the WELL forums was the use of moderators who could interrupt and focus discussion while also disciplining users who broke the rather loose rules. "Flame wars" (crass, offensive, or insulting exchanges) were possible, but anyone dissatisfied in one forum was free to organize another. In addition, the WELL was intensely democratic. WELL forums were the original chat rooms—online spaces where individuals possessing similar interests might congregate, converse, and even share their physical locations to facilitate meeting in person. Finally, the WELL served as a template for other online communities

dedicated to subjects as diverse as Roman Catholicism, liberal politics, gardening, and automobile modification.

## Instant broadcast communication

For the individual, the Internet opened up new communication possibilities. E-mail led to a substantial decline in traditional "snail mail." Instant messaging (IM), or text messaging, expanded, especially among youth, with the convergence of the Internet and cellular telephone access to the Web. Indeed, IM became a particular problem in classrooms, with students often surreptitiously exchanging notes via wireless communication devices. More than 50 million American adults, including 11 million at work, use IM.

From mailing lists to "buddy lists," e-mail and IM have been used to create "smart mobs" that converge in the physical world. Examples include protest organizing, spontaneous performance art, and shopping. Obviously, people congregated before the Internet existed, but the change wrought by mass e-mailings was in the speed of assembling such events. In February 1999, for example, activists began planning protests against the November 1999 World Trade Organization (WTO) meetings in Seattle, Washington. Using the Internet, organizers mobilized more than 50,000 individuals from around the world to engage in demonstrations—at times violent—that effectively altered the WTO's agenda.

More than a decade later, in June 2010 Egyptian computer engineer Wael Ghonim anonymously created a page titled "We Are All Khaled Said" on the social media site Facebook to publicize the death of a 28-year-old Egyptian man beaten to death by police. The page garnered hundreds of thousands of members, becoming an online forum for the discussion of police brutality in Egypt. After a popular uprising in Tunisia in January 2011, Ghonim and several other Internet democracy activists posted messages to their sites calling for similar action in Egypt. Their social media campaign helped spur mass demonstrations that forced Egyptian Pres. Hosni Mubarak from power.

(The convergence of mobs is not without some techno-silliness. "Flash mobs"—groups of strangers who are mobilized on short notice via websites, online discussion groups, or e-mail distribution lists—often take part in bizarre though usually harmless activities in public places, such as engaging in mass free-for-alls around the world on Pillow Fight Day.)

In the wake of catastrophic disasters, citizens have used the Internet to donate to charities in an unprecedented fashion. Others have used the Internet to reunite family members or to match lost pets with their owners. The role of the Internet in responding to disasters, both natural and deliberate, remains the topic of much discussion, as it is unclear whether the Internet actually can function in a disaster area when much of the infrastructure is destroyed. Certainly during the September 11, 2001, attacks, people found it easier to communicate with loved ones in New York City via e-mail than through the overwhelmed telephone network.

Following the earthquake that struck Haiti in January 2010, electronic media emerged as a useful mode for connecting those separated by the quake and for

coordinating relief efforts. Survivors who were able to access the Internet—and friends and relatives abroad—took to social networking sites such as Facebook in search of information on those missing in the wake of the catastrophe. Feeds from those sites also assisted aid organizations in constructing maps of the areas affected and in determining where to channel resources. The many Haitians lacking Internet access were able to contribute updates via text messaging on mobile phones.

## Social gaming and social networking

One-to-one or even one-to-many communication is only the most elementary form of Internet social life. The very nature of the Internet makes spatial distances largely irrelevant for social interactions. Online gaming moved from simply playing a game with friends to a rather complex form of social life in which the game's virtual reality spills over into the physical world. The case of *World of Warcraft*, a popular electronic game with several million players, is one example. Property acquired in the game can be sold online, although such secondary economies are discouraged by Blizzard Entertainment, the publisher of *World of Warcraft*, as a violation of the game's terms of service. In any case, what does it mean that one can own virtual property and that someone is willing to pay for this property with real money? Economists have begun studying such virtual economies, some of which now exceed the gross national product of countries in Africa and Asia. In fact, virtual economies have given economists a means of running controlled experiments.

Millions of people have created online game characters for entertainment purposes. Gaming creates an online community, but it also allows for a blurring of the boundaries between the real world and the virtual one. In Shanghai one gamer stabbed and killed another one in the real world over a virtual sword used in *Legend of Mir 3*. Although attempts were made to involve the authorities in the original dispute, the police found themselves at a loss prior to the murder because the law did not acknowledge the existence of virtual property. In South Korea violence surrounding online gaming happens often enough that police refer to such murders as "off-line PK," a reference to player killing (PK), or player-versus-player lethal contests, which are allowed or encouraged in some games. By 2001 crime related to *Lineage* had forced South Korean police to create special cybercrime units to patrol both within the game and off-line. Potential problems from such games are not limited to crime. Virtual life can be addictive. Reports of players neglecting family, school, work, and even their health to the point of death have become more common.

Social networking sites (SNSs) emerged as a significant online phenomenon since the bursting of the "Internet bubble" in the early 2000s. SNSs use software to facilitate online communities where members with shared interests swap files, photographs, videos, and music, send messages and chat, set up blogs (Web diaries) and discussion groups, and share opinions. Early social networking services included Classmates.com, which connected former schoolmates, and Yahoo! 360° and SixDegrees, which built networks of connections via friends of friends. In the postbubble era the leading social networking services were Myspace, Facebook, Friendster, Orkut, and LinkedIn. LinkedIn became an effective tool for business staff recruiting. Businesses have begun to exploit these networks, drawing on social networking research and theory, which suggests that finding key "influential"

members of existing networks of individuals can give those businesses access to and credibility with the whole network.

## Love and sex

By the start of the 21st century, approximately 20 percent of the Internet population had used it at some time to meet others, with Internet dating services collecting nearly half a billion dollars per year in matchmaking fees. Dating sites capture an important aspect of the Web economy—the ability to appeal to particular niche groups. Of the myriads of dating websites, many cater to individuals of particular ethnic or national identities and thereby preselect people along some well-defined axes of interest. Because of the low costs involved in setting up a website, the possibilities for "nichification" are nearly endless.

More From Britannica

computer: The Internet

Pornography is another domain in which nichification is prevalent. By the 21st century there were some four million websites devoted to pornography, containing more than a quarter of a billion pages—in other words, more than 10 percent of the Web. Forty million American adults regularly visit pornographic sites, which generate billions of dollars in yearly revenues. All of society's vices, as well as its virtues, have manifested themselves on the Internet.

### Advertising and e-commerce

Nichification allows for consumers to find what they want, but it also provides opportunities for advertisers to find consumers. For example, most search engines generate revenue by matching ads to an individual's particular search query. Among the greatest challenges facing the Internet's continued development is the task of reconciling advertising and commercial needs with the right of Internet users not to be bombarded by "pop-up" Web pages and spam (unsolicited e-mail).

Nichification also opens up important e-commerce opportunities. A bookstore can carry only so much inventory on its shelves, which thereby limits its collection to books with broad appeal. An online bookstore can "display" nearly everything ever published. Although traditional bookstores often have a special-order department, consumers have taken to searching and ordering from online stores from the convenience of their homes and offices.

Although books can be made into purely digital artifacts, "e-books" have not sold nearly as well as digital music. In part, this disparity is due to the need for an e-book reader to have a large, bright screen, which adds to the display's cost and weight and leads to more-frequent battery replacement. Also, it is difficult to match the handy design and low cost of an old-fashioned paperback book. Interestingly, it turns out that listeners download from online music vendors as many obscure songs as big record company hits. Just a few people interested in some obscure song are enough to make it worthwhile for a vendor to store it electronically for sale over the Internet.

What makes the Internet special here is not only its ability to match buyers and sellers quickly and relatively inexpensively but also that the Internet and the digital economy in general allow for a flowering of multiple tastes—in games, people, and music.

## Information and copyright

## Education

Commerce and industry are certainly arenas in which the Internet has had a profound effect, but what of the foundational institutions of any society—namely, those related to education and the production of knowledge? Here the Internet has had a variety of effects, some of which are quite disturbing. There are more computers in the classroom than ever before, but there is scant evidence that they enhance the learning of basic skills in reading, writing, and arithmetic. And while access to vast amounts of digital information is convenient, it has also become apparent that most students now see libraries as antiquated institutions better used for their computer terminals than for their book collections. As teachers at all education levels can attest, students typically prefer to research their papers by reading online rather than wandering through a library's stacks.

More From Britannica

What's the Difference Between the Deep Web and the Dark Web?

In a related effect the Internet has brought plagiarism into the computer era in two distinct senses. First, electronic texts have made it simple for students to "cut and paste" published sources (e.g., encyclopaedia articles) into their own papers. Second, although students could always get someone to write their papers for them, it is now much easier to find and purchase anonymous papers at websites and to even commission original term papers for a fixed fee. Ironically, what the Internet gives, it also takes away. Teachers now have access to databases of electronically submitted papers and can easily compare their own students' papers against a vast archive of sources. Even a simple online search can sometimes find where one particularly well-turned phrase originally appeared.

## File sharing

College students have been at the leading edge of the growing awareness of the centrality of intellectual property in a digital age. When American college student Shawn Fanning invented Napster in 1999, he set in motion an ongoing legal battle over digital rights. Napster was a file-sharing system that allowed users to share electronic copies of music online. The problem was obvious: recording companies were losing revenues as one legal copy of a song was shared among many people. Although the record companies succeeded in shutting down Napster, they found themselves having to contend with a new form of file sharing, P2P ("person-to-person"). In P2P there is no central administrator to shut down as there had been

with Napster. Initially, the recording industry sued the makers of P2P software and a few of the most prolific users—often students located on university campuses with access to high-speed connections for serving music and, later, movie files—in an attempt to discourage the millions of people who regularly used the software. Still, even while some P2P software makers have been held liable for losses that the copyright owners have incurred, more-devious schemes for circumventing apprehension have been invented.

The inability to prevent file sharing has led the recording and movie industries to devise sophisticated copy protection on their CDs and DVDs. In a particularly controversial incident, Sony Corporation introduced CDs into the market in 2005 with copy protection that involved a special viruslike code that hid on a user's computer. This code, however, also was open to being exploited by virus writers to gain control of users' machines.

## Electronic publishing

The Internet has become an invaluable and discipline-transforming environment for scientists and scholars. In 2004 Google began digitizing public-domain and out-of-print materials from several cooperating libraries in North America and Europe, such as the University of Michigan library, which made some seven million volumes available. Although some authors and publishers challenged the project for fear of losing control of copyrighted material, similar digitization projects were launched by Microsoft Corporation and the online book vendor Amazon.com, although the latter company proposed that each electronic page would be retrieved for a small fee shared with the copyright holders.

The majority of academic journals are now online and searchable. This has created a revolution in scholarly publishing, especially in the sciences and engineering. For example, arXiv.org has transformed the rate at which scientists publish and react to new theories and experimental data. Begun in 1991, arXiv.org is an online archive in which physicists, mathematicians, computer scientists, and computational biologists upload research papers long before they will appear in a print journal. The articles are then open to the scrutiny of the entire scientific community, rather than to one or two referees selected by a journal editor. In this way scientists around the world can receive an abstract of a paper as soon as it has been uploaded into the depository. If the abstract piques a reader's interest, the entire paper can be downloaded for study. Cornell University in Ithaca, New York, and the U.S. National Science Foundation support arXiv.org as an international resource.

While arXiv.org deals with articles that might ultimately appear in print, it is also part of a larger shift in the nature of scientific publishing. In the print world a handful of companies control the publication of the most scientific journals, and the price of institutional subscriptions is frequently exorbitant. This has led to a growing movement to create online-only journals that are accessible for free to the entire public—a public that often supports the original research with its taxes. For example, the Public Library of Science publishes online journals of biology and medicine that compete with traditional print journals. There is no difference in how their articles are vetted for publication; the difference is that the material is made available for free. Unlike other creators of content, academics are not paid for what they publish in scholarly journals, nor are those who review the articles. Journal publishers, on

the other hand, have long received subsidies from the scientific community, even while charging that community high prices for its own work. Although some commercial journals have reputations that can advance the careers of those who publish in them, the U.S. government has taken the side of the "open source" publishers and demanded that government-financed research be made available to taxpayers as soon as it has been published.

In addition to serving as a medium for the exchange of articles, the Internet can facilitate the discussion of scientific work long before it appears in print. Scientific blogs—online journals kept by individuals or groups of researchers—have flourished as a form of online salon for the discussion of ongoing research. There are pitfalls to such practices, though. Astronomers who in 2005 posted abstracts detailing the discovery of a potential 10th planet found that other researchers had used their abstracts to find the new astronomical body themselves. In order to claim priority of discovery, the original group rushed to hold a news conference rather than waiting to announce their work at an academic conference or in a peer-reviewed journal.

## Politics and culture

## Free speech

The Internet has broadened political participation by ordinary citizens, especially through the phenomenon of blogs. Many blogs are simply online diaries or journals, but others have become sources of information and opinion that challenge official government pronouncements or the mainstream news media. By 2005 there were approximately 15 million blogs, a number that was doubling roughly every six months. The United States dominates the blog universe, or "blogosphere," with English as the lingua franca, but blogs in other languages are proliferating. In one striking development, the Iranian national language, Farsi, has become the commonest Middle Eastern language in the blogosphere. Despite the Iranian government's attempts to limit access to the Internet, some 60,000 active Farsi blogs are hosted at a single service provider, PersianBlog.

The Internet poses a particular problem for autocratic regimes that restrict access to independent sources of information. The Chinese government has been particularly successful at policing the public's access to the Internet, beginning with its "Great Firewall of China" that automatically blocks access to undesirable websites. The state also actively monitors Chinese websites to ensure that they adhere to government limits on acceptable discourse and tolerable dissent. In 2000 the Chinese government banned nine types of information, including postings that might "harm the dignity and interests of the state" or "disturb social order." Users must enter their national identification number in order to access the Internet at cybercafés. Also, Internet service providers are responsible for the content on their servers. Hence, providers engage in a significant amount of self-censorship in order to avoid problems with the law, which may result in losing access to the Internet or even serving jail time. Finally, the authorities are willing to shut websites quickly and with no discussion. Of course, the state's efforts are not completely effective. Information can be smuggled into China on DVDs, and creative Chinese users can circumvent the national firewall with proxy servers—websites that allow users to

move through the firewall to an ostensibly acceptable website where they can connect to the rest of the Internet.

Others have taken advantage of the Internet's openness to spread a variety of political messages. The Ukrainian Orange Revolution of 2004 had a significant Internet component. More troubling is the use of the Internet by terrorist groups such as al-Qaeda to recruit members, pass along instructions to sleeper cells, and celebrate their own horrific activities. The Iraq War was fought not only on the ground but also online as al-Qaeda operatives used specific websites to call their followers to jihad. Al-Qaeda used password-protected chat rooms as key recruitment centres, as well as websites to test potential recruits before granting them access to the group's actual network. On the other hand, posting material online is also a potential vulnerability. Gaining access to the group's "Jihad Encyclopaedia" has enabled security analysts to learn about potential tactics, and Arabic-speaking investigators have learned to infiltrate chat rooms and gain access to otherwise hidden materials.

## Political campaigns and muckraking

During the 2004 U.S. presidential campaign, blogs became a locus for often heated exchanges about the candidates. In fact, the candidates themselves used blogs and websites for fund-raising and networking. One of the first innovators was Howard Dean, an early front-runner in the Democratic primaries, whose campaign used a website for fund-raising and organizing local meetings. In particular, Dean demonstrated that a modern presidential campaign could use the Internet to galvanize volunteer campaign workers and to raise significant sums from many small donations. In a particularly astute move, Dean's campaign set up a blog for comments from his supporters, and it generated immediate feedback on certain proposals such as refusing to accept public campaign funding. Both the George W. Bush and the John Kerry presidential campaigns, as well as the Democratic and Republican parties, came to copy the practices pioneered by Dean and his advisers. In addition, changes in U.S. campaign finance laws allowed for the creation of "527s," independent action groups such as Moveon.org that used the Internet to raise funds and rally support for particular issues and candidates.

By 2005 it was widely agreed that politicians would have to deal not only with the mainstream media (i.e., newspapers, magazines, radio, and television) but also with a new phenomenon—the blogosphere. Although blogs do not have editors or fact checkers, they have benefited from scandals in the mainstream media, which have made many readers more skeptical of all sources of information. Also, bloggers have forced mainstream media to confront topics they might otherwise ignore. Some pundits have gone so far as to predict that blogs and online news sources will replace the mainstream media, but it is far more likely that these diverse sources of information will complement each other. Indeed, falling subscription rates have led many newspaper publishers to branch into electronic editions and to incorporate editorial blogs and forums for reader feedback; thus, some of the distinctions between the media have already been blurred.

## Privacy and the Internet

Concerns about privacy in cyberspace are an issue of international debate. As reading and writing, health care and shopping, and sex and gossip increasingly take place in cyberspace, citizens around the world are concerned that the most intimate details of their daily lives are being monitored, searched, recorded, stored, and often misinterpreted when taken out of context. For many, the greatest threats to privacy come not from state agents but from the architecture of e-commerce itself, which is based, in unprecedented ways, on the recording and exchange of intimate personal information.

# "Getting over it"

The threats to privacy in the new Internet age were crystallized in 2000 by the case of DoubleClick, Inc. For a few years DoubleClick, the Internet's largest advertising company, had been compiling detailed information on the browsing habits of millions of World Wide Web users by placing "cookie" files on computer hard drives. Cookies are electronic footprints that allow websites and advertising networks to monitor people's online movements with telescopic precision—including the search terms people enter as well as the articles they skim and how long they spend skimming them. As long as users were confident that their virtual identities were not being linked to their actual identities, many were happy to accept DoubleClick cookies in exchange for the convenience of navigating the Web more efficiently. Then in November 1999 DoubleClick bought Abacus Direct, which held a database of names, addresses, and information about the off-line buying habits of 90 million households compiled from the largest direct-mail catalogs and retailers in the nation. Two months later DoubleClick began compiling profiles linking individuals' actual names and addresses to Abacus's detailed records of their online and off-line purchases. Suddenly, shopping that once seemed anonymous was being archived in personally identifiable dossiers.

Under pressure from privacy advocates and dot-com investors, DoubleClick announced in 2000 that it would postpone its profiling scheme until the U.S. government and the e-commerce industry had agreed on privacy standards. Two years later it settled consolidated class-action lawsuits from several states, agreeing to pay legal expenses of up to $1.8 million, to tell consumers about its data-collection activities in its online privacy policy, and to get permission before combining a consumer's personally identifiable data with his or her Web-surfing history. DoubleClick also agreed to pay hundreds of thousands of dollars to settle differences with attorneys general from 10 states who were investigating its information gathering.

The retreat of DoubleClick might have seemed like a victory for privacy, but it was only an early battle in a much larger war—one in which many observers still worry that privacy may be vanquished. "You already have zero privacy—get over it," Scott McNealy, the CEO of Sun Microsystems, memorably remarked in 1999 in response to a question at a product show at which Sun introduced a new interactive technology called Jini. Sun's cheerful website promised to usher in the "networked home" of the future, in which the company's "gateway" software would operate "like a congenial party host inside the home to help consumer appliances communicate intelligently with each other and with outside networks." In this chatty new world of

electronic networking, a household's refrigerator and coffeemaker could talk to a television, and all three could be monitored from the office computer. The incessant information exchanged by these gossiping appliances might, of course, generate detailed records of the most intimate details of their owners' daily lives.

New evidence seemed to emerge every day to support McNealy's grim verdict about the triumph of online surveillance technology over privacy. A survey of nearly a thousand large companies conducted by the American Management Association in 2000 found that more than half of the large American firms surveyed monitored the Internet connections of their employees. Two-thirds of the firms monitored e-mail messages, computer files, or telephone conversations, up from only one-third three years earlier. Some companies used Orwellian computer software with names like Spector, Assentor, or Investigator that could monitor and record every keystroke on the computer with video-like precision. These virtual snoops could also be programmed to screen all incoming and outgoing e-mail for forbidden words and phrases—such as those involving racism, body parts, or the name of the boss—and then forward suspicious messages to a supervisor for review.

## Issues in new media

Changes in the delivery of books, music, and television extended the technologies of surveillance beyond the office, blurring the boundaries between work and home. The same technologies that make it possible to download digitally stored books, songs, and movies directly onto computer hard drives or mobile devices could make it possible for publishers and entertainment companies to record and monitor each individual's browsing habits with unsettling specificity. Television too is being redesigned to create precise records of viewing habits. For instance, digital video recorders make it possible to store hours of television programs and enable viewers to skip commercials and to create their own program lineups. The data generated by such actions could create viewer profiles, which could then be used to make viewing suggestions and to record future shows.


website for Pegasus spyware


activist protesting the murder of Jamal Khashoggi

Privacy of cell phone communication also has become an issue, especially with the advent of nearly undetectable spyware and the professed need by national governments to monitor criminals who used wireless communications. The controversy over Pegasus spyware is a prime case in point. The Israeli cyber-intelligence firm NSO Group (founded in 2010) created the smartphone-attached spyware for eavesdropping on phones and harvesting their data (including calls, texts, photos, passwords, and locations). The company claims its product, which can steal private data without leaving an obvious trace of its actions, is sold exclusively to

government security and law enforcement agencies and only for the purpose of aiding rescue operations and battling criminals, such as money launderers, sex- and drug-traffickers, and terrorists. Yet, Pegasus has been used to track politicians, government leaders, human rights activists, dissidents, and journalists. The Saudi Arabian government used it to track Saudi journalist and U.S. resident Jamal Khashoggi. Months before Khashoggi's murder and dismemberment by Saudi agents in October 2018, Pegasus had been attached to the phone of Khashoggi's wife.

The United States is not immune to these controversies. In 2010 Pres. Barack Obama's administration said that in order to prevent terrorism and identify criminals, it wanted Congress to require that all Internet services be capable of complying with wiretap orders. The broad requirement would include Internet phone services, social networking services, and other types of Internet communication, and it would enable even encrypted messages to be decoded and read—something that required considerable time and effort. Critics complained that the monitoring proposal challenged the ideals of privacy and the lack of centralized authority for which the Internet had long been known.

Photos and videos also emerged as unexpected threats to personal privacy. "Geotags" are created when photos or videos are embedded with geographic location data from GPS chips inside cameras, including those in cell phones. When images are uploaded to the Internet, the geotags allow homes or other personal locations within the images to be precisely located by those who view the photos online. The security risk is not widely understood by the public, however, and in some cases disabling the geotag feature in certain models of digital cameras and camera-equipped smartphones is complicated.

Google's Street View photo-mapping service caused privacy concerns when the company disclosed that it had been recording locations and some data from unprotected household wireless networks as it took pictures. The company said that the data had been gathered inadvertently. German officials objected to Google's actions on the basis of Germany's strict privacy laws, and, although German courts decided against the objections, Google did not expand its Street View service in Germany beyond the handful of urban centres that it had already photo-mapped. The controversy led to other investigations of the Street View service by several U.S. states and the governments of several countries (including the Czech Republic, which eventually refused to grant Google permission to offer the Street View service there).

The social network Facebook has been a particular focus of privacy concerns on the Internet. Over the lifetime of the site, the default privacy settings for a Facebook user's information evolved from most content being accessible only to a user's friends or friends of friends to being accessible to everyone. In December 2009 Facebook rolled out a new privacy settings update that allowed users to exercise more "granular" control over what personal information was shared or displayed. However, the labyrinthine nature of the various privacy-control menus discouraged use of the new privacy settings. Users tended to fall back on Facebook's default settings, which, because of the expansion of Facebook's "opt-out" policy, were at the loosest level of security, forcing users to "opt-in" to make information private. Responding to criticism, Facebook revised its privacy policy again in May 2010, with a simplified system that consolidated privacy settings onto a single page.

Listen to a thirteen-year-old share her experience of cyberbullying and learn about its psychological effects and how to prevent it

See all videos for this article

Another privacy issue is cyberbullying—using the Internet to threaten or humiliate another person with words, photos, or videos. The problem received particular attention in 2010 when a male Rutgers University student committed suicide after two acquaintances reportedly streamed a video over the Internet of the student having a sexual encounter with a man. Also in 2010, Donna Witsell, the mother of a 13-year-old Florida girl who had committed suicide in 2009 after a cyberbullying incident, formed a group called Hope's Warriors to help curb abuse and to warn others of the threat. Most U.S. states have enacted laws against bullying, although very few of them include cyberbullying.

*Michael Aaron Dennis*

*The Editors of Encyclopaedia Britannica*

Internet Explorer

Table of Contents

HomeTechnologyThe Web & Communication

Science & Tech

# Internet Explorer

## Internet browser

Print Cite Share Feedback

Also known as: IE, Microsoft Internet Explorer

Written and fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

**Internet Explorer (IE)**, World Wide Web (WWW) browser and set of technologies created by Microsoft Corporation, a leading American computer software company. After being launched in 1995, Internet Explorer became one of the most popular tools for accessing the Internet. There were 11 versions between 1995 and 2013.


How Internet Explorer won the first “browser war”

See all videos for this article

In July 1995 Microsoft released Internet Explorer 1.0 as an add-on to the Windows 95 operating system. By November the company had produced IE 2.0 for both Apple Inc.’s Macintosh and Microsoft’s Windows 32-bit operating systems. This release featured support for the virtual reality modeling language (VRML), browser “cookies” (data saved by websites within the user’s browser), and secure socket layering (SSL). The success of IE and the rapidly expanding online world led Microsoft to produce several editions of the program in rapid succession. In August 1996 IE 3.0, designed for use with Windows 95, added important components such as Internet Mail and News (an e-mail and newsgroup client) and Windows Media Player, a computer graphics program that allowed users to view GIF (graphics interchange format) and JPEG (joint photographic experts group) files; IE 3.0 also supported MIDI (musical instrument digital interface) sound files. (Although new IE versions for the Macintosh often lagged behind Windows releases, Microsoft never discontinued its support for the Macintosh.)

Microsoft integrated IE 3.0 into its Windows operating system (that is, it came “bundled” ready-to-use within the operating system of personal computers), which had the effect of reducing competition from other Internet browser manufacturers. One of its competitors, Netscape Communications Corporation, the maker of the

Navigator Web browser, complained to the federal government, which in May 1998, along with 20 U.S. states and the District of Columbia, sued Microsoft for being an unlawful monopoly under the Sherman Antitrust Act. In April 2000 Judge Thomas Jackson found Microsoft guilty and ordered its breakup. On appeal, however, the breakup order was overturned, but the appeals court did agree that Microsoft was an illegal monopoly.

IE 4.0, which came out in 1997, was tightly integrated into the company's main operating systems, Windows 95, Windows 98, and Windows NT. This incarnation replaced Internet Mail and News with Outlook Express, a freeware version of Microsoft Office Outlook, the company's commercial e-mail and newsgroup client. IE 5, released in September 1998, expanded Web design capabilities and allowed for further personalization. IE 6, released in 2001 and designed to work with the Windows XP operating system, featured more privacy and security options. IE 6 was Microsoft's primary Web browser until the 2006 development of IE 7, which was compatible with the Windows Vista operating system. IE 8, which was released in 2009, added more support for Web 2.0 features.

IE 9 was released in 2011 and featured increased speed and compliance with the HyperText Markup Language (HTML) 5 standards for video and audio. Later that same year, IE 10 brought the browser further into complete adherence to the HTML 5 standards. IE 11, released in 2013, had features built for touch screens such as those on smartphones and tablets. In January 2016 Microsoft discontinued its active technical support for all other versions of Internet Explorer except IE 11. Microsoft Edge replaced Internet Explorer as the company's preferred browser in 2016. Microsoft ended support for IE 11 in June 2022 and announced that the browser would be disabled in a future update of Windows.

*The Editors of Encyclopaedia Britannica This article was most recently revised and updated by Adam Augustyn.*

# Instagram

Table of Contents

HomePolitics, Law & GovernmentBanking & Business

History & Society

## Instagram
## social networking service

Print Cite Share Feedback

Written by

Alison Eldridge

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Oct 23, 2023 • Article History

Table of Contents

Mike Krieger and Kevin Systrom

See all media

Category: History & Society

Areas Of Involvement:

social network

See all related content →

**Recent News**

Oct. 23, 2023, 12:30 PM ET (CBS)

Dwayne "The Rock" Johnson wants Paris museum to change the skin color of his new wax figure

Oct. 21, 2023, 9:15 PM ET (Daily Star)

Anil Kapoor resurrects iconic 'Mr. India' character

Show More

**Instagram**, online social media platform and social network service for photograph and video sharing. The app was launched in 2010 by cofounders Kevin Systrom and Mike Krieger, and it is now owned by Meta Platforms, Inc., the parent company of Facebook. One of the biggest social media platforms in the world, Instagram surpassed two billion monthly active users in 2022. The company's headquarters are in Menlo Park, California.

# History

Instagram, 2011

Instagram originated with Stanford graduate Kevin Systrom, who had previously worked at Google. His initial creation was Burbn, so named because of his interest in whiskey and bourbon. Inspired by the popularity of Foursquare and other location-based platforms, Burbn allowed users to post check-ins along with photos, which were not yet a staple of social posting. Systrom secured venture funding for Burbn and went on to recruit fellow Stanford graduate Mike Krieger, who had worked on the social media platform Meebo. They reworked the concept to focus on photographs taken on mobile devices and renamed it Instagram. Systrom and Krieger embraced minimalism with their prototype, concentrating on images (with the option to add filters), comments, and "liking" features. The duo also decided to eschew a Web version for an iOS app that would capitalize on the much improved photographic capabilities of the iPhone 4. They finalized the app in a few months, posting the platform's first photos in July 2010. Instagram was released to the public in Apple's App Store on October 6, 2010, and reached 25,000 users on its first day. Less than three months later it had one million users, a phenomenal achievement.

As Instagram's popularity grew rapidly, the company drew the interest of various investors and potential buyers. In April 2012, 18 months after its launch, Instagram was bought for $1 billion in cash and stock by Facebook. The acquisition came about a month before Facebook's initial public offering.

## Description and features

Instagram's service is relatively straightforward. It focuses on posts containing images and/or short-form videos. These posts are contained within a user's profile and may be displayed publicly within Instagram or privately to the user's followers. There are two main channels for posting: into the user's permanent feed or into their "Stories," a special section where content remains for 24 hours before disappearing (unless specifically archived). It is also possible to go "live," streaming video directly from a camera to the platform.

Users may connect with each other via private message (known as a direct message [DM]), where they can share permanent photos or videos or vanishing photos or videos (similar to Snapchat). Users are able to "follow" each other, with all of the accounts one is following being aggregated into a single feed. The platform also

allows for browsing by topic or hashtag, and a user can view a random mix of popular posts.

Instagram includes the ability to take photographs or videos in-app and also to edit new or existing photos or videos with the use of text, gifs, icons, and filters that add various lighting effects, distortions, or other features, including hats or cat ears. Images were originally required to be square, 640 by 640 pixels to fit the width of the iPhone. However, in 2015 size restrictions were expanded to 1080 pixels.



Feed posts may contain a caption from the user, geotagging data, and/or tags linking to other user accounts. Captions frequently feature hashtags to make posts readily findable and searchable by other users. The platform also allows for text comments to be added to feed posts and for users to “like” posts through the use of a heart icon. For Stories, users are able to send emoji-based reactions or reply by private message.

The service is free to use and, similar to sister company Facebook, brings in revenue largely from advertisements. Originally available only on Apple’s iOS, it released versions for Android (2012), Web (2012), Fire OS (2014), and Windows 10 (2016).

## Influence and criticisms

The popularity and nature of the service brought many advertisers to Instagram and helped launch the era of the “influencer”—individuals who have built a considerable social media following and use that influence to advertise particular products or services. Influencers are often courted by brands and may receive financial

compensation and free products for posting information or reviews or name-dropping a product in their posts or videos.

Although widely lauded for its meteoric rise and extreme popularity, Instagram has come under fire for issues that plague social media platforms: inappropriate content, misinformation and disinformation, and insufficient moderation. Studies have also shown that it can have a detrimental effect on teen mental health, especially impacting the self-esteem of young girls.
*Alison Eldridge*

# Google Knol

Table of Contents

HomeLiteratureLibraries & Reference Works

Arts & Culture

## Google Knol
## encyclopaedia

Print Cite Share Feedback

Also known as: Knol

Written and fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

**Google Knol**, free Internet-based encyclopaedia hosted (2007–12) by the American search engine company Google Inc.

On December 13, 2007, Google announced that it was entering the online encyclopaedia business with Knol. (The company defined a *knol* as a unit of knowledge.) The Knol Web site was opened to the general public on July 23, 2008. Participation in Knol required a confirmation of an individual's identity before any articles or edits were allowed at the Knol Web site.

In exchange for giving up their anonymity, authors were given an opportunity to allow ads from Google's AdSense on their Knol Web pages. By sharing with its authors any ad revenue generated by "page views" of their articles, Google hoped to induce submissions by professionals and highly qualified individuals. Authors were able to choose to allow edits by specific collaborators or open up their articles for editing by the entire Knol community. In addition, Knol had no limit to the number of articles on the same subject: Google expected that well-written and maintained articles would rise to the top through user ratings.

In November 2011 Google announced that it would be discontinuing Knol, and in May 2012 articles became accessible only to their authors.
*This article was most recently revised and updated by Adam Augustyn.*



# Tim Berners-Lee
# British scientist



Also known as: Sir Tim Berners-Lee

Written by

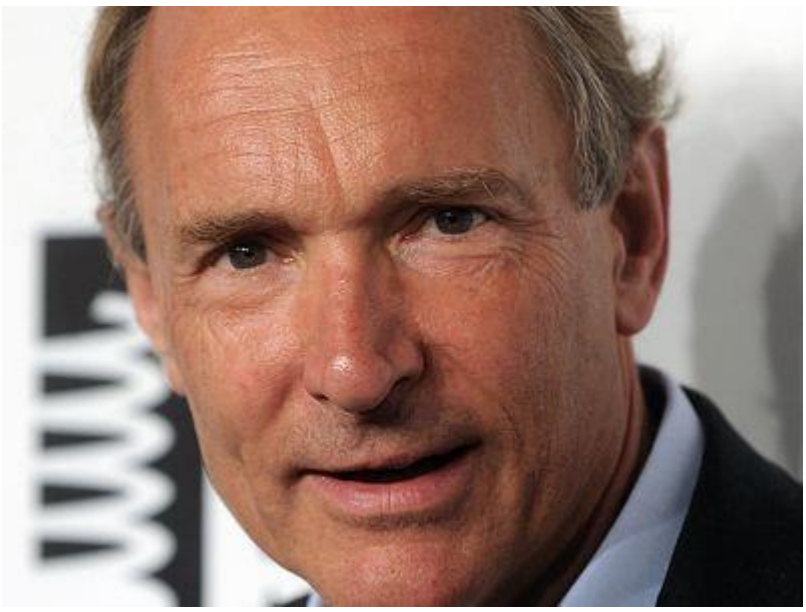
Michael Aaron Dennis

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents



Tim Berners-Lee

See all media

Category: Science & Tech

**In Full:** Sir Tim Berners-Lee

Born:

June 8, 1955, London, England (age 68)

Founder:

World Wide Web Consortium

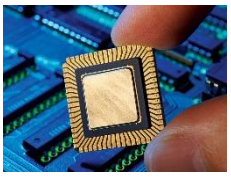
Inventions:

World Wide Web World Wide Web

See all related content →

**Tim Berners-Lee**, in full **Sir Tim Berners-Lee**, (born June 8, 1955, London, England), British computer scientist, generally credited as the inventor of the World Wide Web. In 2004 he was awarded a knighthood by Queen Elizabeth II of the United Kingdom and the inaugural Millennium Technology Prize (€1 million) by the Finnish Technology Award Foundation.

Computing came naturally to Berners-Lee, as both of his parents worked on the Ferranti Mark I, the first commercial computer. (*See* computer: The first stored-program machines.) After graduating in 1976 from the University of Oxford, Berners-Lee designed computer software for two years at Plessey Telecommunications Ltd., located in Poole, Dorset, England. Following this, he had several positions in the computer industry, including a stint from June to December 1980 as a software engineering consultant at CERN, the European particle physics laboratory in Geneva.



**Britannica Quiz**

Computers and Technology Quiz

Tim Berners-Lee

While at CERN, Berners-Lee developed a program for himself, called Enquire, that could store information in files that contained connections (“links”) both within and among separate files—a technique that became known as hypertext. After leaving CERN, Berners-Lee worked for Image Computer Systems Ltd., located in Ferndown, Dorset, where he designed a variety of computer systems. In 1984 he

returned to CERN to work on the design of the laboratory's computer network, developing procedures that allowed diverse computers to communicate with one another and researchers to control remote machines. In 1989 Berners-Lee drew up a proposal for creating a global hypertext document system that would make use of the Internet. His goal was to provide researchers with the ability to share their results, techniques, and practices without having to exchange e-mail constantly. Instead, researchers would place such information "online," where their peers could immediately retrieve it anytime, day or night. Berners-Lee wrote the software for the first Web server (the central repository for the files to be shared) and the first Web client, or "browser" (the program to access and display files retrieved from the server), between October 1990 and the summer of 1991. The first "killer application" of the Web at CERN was the laboratory's telephone directory—a mundane beginning for one of the technological wonders of the computer age.

From 1991 to 1993 Berners-Lee evangelized the Web. In 1994 in the United States he established the World Wide Web (W3) Consortium at the Massachusetts Institute of Technology's Laboratory for Computer Science. The consortium, in consultation with others, lends oversight to the Web and the development of standards. In 1999 Berners-Lee became the first holder of the 3Com Founders chair at the Laboratory for Computer Science. His numerous other honours included the National Academy of Engineering's prestigious Charles Stark Draper Prize (2007). Berners-Lee was the author, along with Mark Fischetti, of *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (2000).
*Michael Aaron Dennis*

# Social network

Table of Contents

HomeTechnologyThe Web & Communication

Science & Tech

## social network
## computing

Print Cite Share Feedback

Written by

Michael Ray

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Oct 11, 2023 • Article History

Table of Contents

social networking

See all media

Category: Science & Tech

Key People:

Sean Parker Stewart Butterfield Mark Zuckerberg

Related Topics:

virtual community USENET newsgroup netiquette bulletin-board system

See all related content →

**Recent News**

Oct. 5, 2023, 10:41 AM ET (AP)

Media entrepreneur unites young activists with power brokers for fight to make social media safe

Oct. 3, 2023, 9:40 AM ET (AP)

Facebook and Instagram users in Europe could get ad-free subscription option, WSJ reports

**Social network**, in computers, an online community of individuals who exchange messages, share information, and, in some cases, cooperate on joint activities. Social networking and social media are overlapping concepts, but social networking is usually understood as users building communities among themselves while social media is more about using social networking sites and related platforms to build an audience.

# The online experience

Eschewing the anonymity that had previously been typical of the online experience, billions of people have flocked to social networking sites where members create and maintain personal profiles that they link with those of other members. The resulting network of “friends” or “contacts” who have similar interests, business goals, or academic courses has replaced for many people, especially youth, older concepts of community. The most basic social networks allow friends to comment on one another’s profiles, send private messages within the network, and traverse the extended web of friends visible in each member’s profile. More advanced networks enable members to enhance their profiles with audio and video clips, and some open their software source code to allow third-party developers to create applications or widgets—small programs that run within the member’s profile page. These programs include games, quizzes, photo-manipulation tools, and news tickers. At its best, a social networking site functions as a hive of creativity, with users and developers feeding on each others’ desire to see and be seen. Critics, however, see these sites as crass popularity contests, in which “power users” pursue the lowest common denominator in a quest to gain the most friends. With billions of unique visitors using many such sites worldwide, it is certainly possible to observe both extremes—often within the same group of “friends.”

computer: Social networking

## From USENET to 21st-century social networks

## USENET

The earliest online social networks appeared almost as soon as the technology could support them. E-mail and chat programs debuted in the early 1970s, but persistent communities did not surface until the creation of USENET in 1979. USENET began as a messaging system between Duke University and the University of North Carolina, but it rapidly expanded to other American universities and government agencies. USENET allowed users to post and receive messages within subject areas called newsgroups. Initially, there was no standard convention for the naming of newsgroups. This led to confusion as the number of newsgroups grew throughout the 1980s. In 1987 USENET groups were reorganized into broad hierarchies such as news, talk, misc (for miscellaneous), and alt (for alternative; the last was created for newsgroups that dealt with taboo or niche topics, and it was the most populous category on USENET). USENET and other discussion forums, such as privately hosted bulletin board systems (BBSs), enabled individuals to interact in an online

social network, but each was essentially a closed system. With the release in 1993 of the Mosaic Web browser, those systems were joined with an easy-to-use graphical interface. The architecture of the World Wide Web made it possible to navigate from one site to another with a click, and faster Internet connections allowed for more multimedia content than could be found in the text-heavy newsgroups.

## Early pioneers

The first companies to create social networks based on Web technology were Classmates.com and SixDegrees.com. Classmates.com, founded in 1995, used an aggressive pop-up advertising campaign to draw Web surfers to its site. It based its social network on the existing connection between members of high school and college graduating classes, armed service branches, and workplaces. SixDegrees.com was the first true social networking site. It was launched in 1997 with most of the features that would come to characterize such sites: members could create profiles for themselves, maintain lists of friends, and contact one another through the site's private messaging system. SixDegrees.com claimed to have attracted more than three million users by 2000, but it failed to translate those numbers into revenue and collapsed with countless other dot-coms when the "bubble" burst that year for shares of e-commerce companies.

## 21st-century social networks

Others were quick to see the potential for such a site, and Friendster was launched in 2002 with the initial goal of competing with popular subscription-fee-based dating services such as Match.com. It deviated from this mission fairly early on, and it soon became a meeting place for post-"bubble" Internet tastemakers. The site's servers proved incapable of handling the resulting spike in traffic, however, and members were faced with frequent shutdowns. Members were further alienated when the site actively began to close down so-called "fakesters" or "pretendsters." While many of these were little more than practical jokes (profiles for Jesus Christ or the Star Wars character Chewbacca), some, such as universities or cities, were helpful identifiers within a friends list. Once again, there was a void in the social networking Web, and MySpace was quick to fill it.

Whereas Friendster, as part of its mission as a dating site, initially appealed to an older crowd, MySpace actively sought a younger demographic from its inception in 2003. It quickly became a venue for rock bands to connect with fans and to debut new material. Unlike Friendster, MySpace had the infrastructure to support its explosive growth, and members joined by the millions. In 2005 MySpace was purchased by News Corporation Ltd. (the media-holding company founded by the Australian entrepreneur Rupert Murdoch), and the site's higher profile caused it to draw scrutiny from legal authorities who were concerned about improper interactions between adults and the site's massive population of minors.

The spectre of online predators did little to diminish MySpace's membership (which reached 70 million active monthly users in 2007), but it did open the door for other social networking sites to seize some of its momentum. Facebook took the Classmates.com formula and turned it on its head, with a network that was initially open only to students at universities. After its 2004 launch by founders Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes at Harvard University, Facebook at first was an academically oriented alternative to MySpace, but in 2006 it opened the service to anyone over 13 and surpassed MySpace as the most popular social network in 2008.

social media logos

In the early 2020s, Facebook was the most popular social network in the world with three billion users. Meta Platforms, the name of Facebook's parent company that reflected an emphasis on the "metaverse," where users interact in virtual reality environments, also owned the popular photo- and video-sharing network Instagram and the instant-messaging services WhatsApp and Facebook Messenger. Other widely used social networks included YouTube for sharing videos, Snapchat for temporary sharing of videos and images, and Telegram for instant messaging. China was home to several of the world's most popular social networks, such as the instant messaging services Weixin (WeChat outside China) and Tencent QQ, and the short-video-sharing service Douyin (TikTok outside China).

# deep web



## deep web
## computer science

Also known as: Deepnet, hidden web, invisible web

Written by

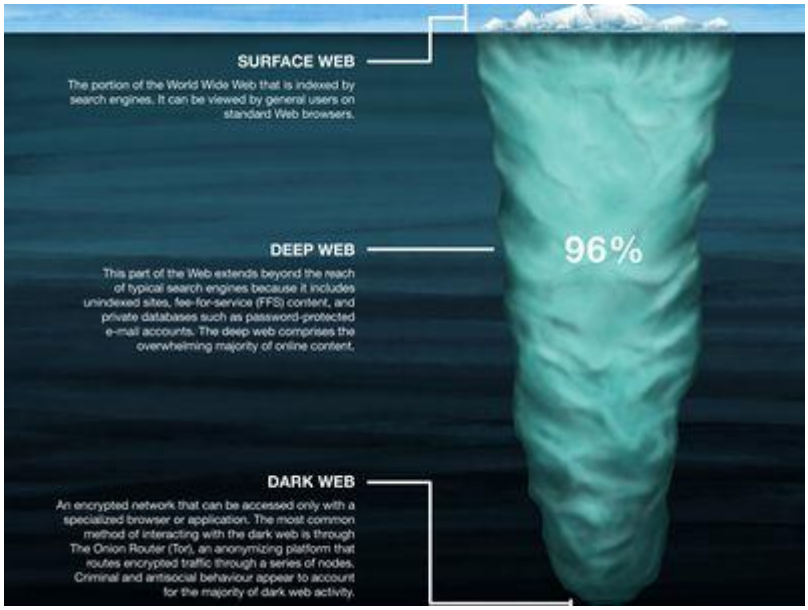
Samuel Greengard

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Oct 12, 2023 • Article History

Table of Contents




proportions of World Wide Web content constituting the surface web, deep web, and dark web

See all media

Category: Science & Tech

Related Topics:

Internet computer network

See all related content →

**Deep web**, a part of the Internet that extends beyond the reach of search engines such as Google, Yahoo!, and Bing because it includes unindexed sites, fee-for-service (FFS) content, and private databases such as password-protected e-mail accounts. As such, it is a widely effective source of mass media. The term “deep web” was coined in 2001 by computer scientist Michael K. Bergman,

who differentiated it from the “surface web,” where openly viewable and retrievable content resides. The deep web is also known as the “invisible web” or “hidden web,” but it should not be confused with the “dark web,” where encrypted content with hidden IP addresses resides. Called “dark” because it is accessible with anonymity and only through certain networks and software such as Tor, this part of the Internet represents a small fraction of the overall Web.

The deep web represents a vast array of data and content. In fact, it is likely some 500 times larger than the surface web and may contain as much as 96 percent of online content. Much of this content is in the form of databases that are accessible only by password or subscription or for a fee.

## How the deep web works

Content that resides on the surface web is accessible because software robots called “spiders” or “crawlers” capture and index it, and search engines assign it rankings. These systems typically scan websites that contain .com, .org., .net, or a similar domain as well as some data and posts at social media sites. As these spiders capture Web pages, they follow embedded links to uncover additional content. Later, when people search for specific content, the results appear in a search engine such as Google, where the content is then openly viewable.

With only about 4 percent of all online content freely accessible (making up the surface web), the remainder is tucked away in the deep web. This means there is no easy, direct way for the general public to search this vast amount of unindexed content. In some cases, websites use various methods to block spiders and prevent indexing. These methods include using CAPTCHAs, multiple IP addresses for the same content, non-HTML content or data that spiders cannot pick up, password protection, and unlinked content.

## Types, viewability, and risks of deep web content

There are numerous types of deep web content. These include websites with registration requirements; fee-based video and media on-demand services such as Netflix, HBO Max, Apple TV+, Amazon Prime, and Spotify; and various password-protected entities. Among these are e-mail systems, legal and medical databases, corporate intranets, document libraries, image archives, financial records, scientific databases, and police and government resources as well as gaming sites, cloud storage services such as Dropbox or iCloud, and private sites and services that are not registered and thus do not appear in search engines. However, university researchers and commercial search services such as Google and Microsoft have explored ways to index deep web content, and law enforcement agencies have attempted to develop deep web crawlers that can spot illicit activities, including drug dealing, sex trafficking, and terrorist activity. The success of these efforts has been limited.

There is no inherent risk associated with searching the surface web or entering the deep web. In fact, both acts are common and part of daily life and business today. However, some websites contain digital dangers such as malware, viruses, spyware, and keyloggers (a kind of surveillance software that can monitor and record every keystroke on a computer). It is also possible to find sensitive data on the deep web that can be stolen or abused, and, of course, the possibility of encountering

individuals who engage in cybercrime and unethical, even harmful, activities is always a risk in the online world.



*Samuel Greengard*

# wide area network

Table of Contents



## wide area network
## computer science



Also known as: WAN, long-haul network

Written by

David Hemmendinger

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

Category: Science & Tech

Related Topics:

computer network network

See all related content →

**Wide area network (WAN)**, a computer communications network that spans cities, countries, and the globe, generally using telephone lines and satellite links. The Internet connects multiple WANs; as its name suggests, it is a network of networks. Its success stems from early support by the U.S. Department of Defense, which developed its precursor, ARPANET (*see* DARPA), to let researchers communicate readily and share computer resources. Its success is also due to its flexible communication technique. The emergence of the Internet in the 1990s as not only a communication medium but also one of the principal focuses of computer use may be the most significant development in computing since its invention. *See also* local area network (LAN).
*David Hemmendinger*

DNS

Table of Contents

HomeTechnologyThe Web & Communication

Science & Tech

# DNS
## network service

Print Cite Share Feedback

Also known as: domain name system

Written and fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

Category: Science & Tech

**In Full:** domain name system

Related Topics:

Internet computer network domain name

See all related content →

**DNS**, in full **domain name system**, network service that converts between World Wide Web "name" addresses and numeric Internet addresses.

The concept of a name server came about as a result of the first computer networks in the mid-1970s. Each computer on a network was identified by a unique number, but, as the size of computer networks grew, users had a hard time keeping track of which machine corresponded to each number. To keep track, researchers developed a database that translated each computer's numeric address into a domain name, which is a string of letters and numbers that is generally easier for users to remember than numeric addresses.

Modern DNS servers work in a similar fashion, with a set of databases running on servers scattered around the Internet. DNS servers use a hierarchical structure to organize domain names. There are two basic types of DNS servers: primary, which contain the databases, and secondary, which provide redundancy for the primary servers. The basic form of this structure is the name of a machine, followed by a top level domain (TLD), separated by dots (periods). For example, britannica.com has the domain name "britannica" and the TLD "com." The most common type of TLD is a generic one such as "com," "gov," or "edu," though there are also country code TLDs, such as "uk," "ca," or "au," and sponsored TLDs, such as travel or jobs. Domain and TLD names are registered and controlled by the Internet Corporation for Assigned Numbers and Names (ICANN).

DNS, which operates on top of the transmission control protocol/Internet protocol (TCP/IP) architecture, is likely to continue for the foreseeable future as the standard for accessing Internet sites.
*The Editors of Encyclopaedia Britannica This article was most recently revised and updated by Erik Gregersen.*

# Facebook

Table of Contents

HomePolitics, Law & GovernmentBanking & Business

History & Society

## Facebook
social network

Print Cite Share Feedback

Written by

Mark Hall

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Oct 23, 2023 • Article History

Table of Contents


Mark Zuckerberg

See all media

Category: History & Society

Date:

2004 - present

Headquarters:

Menlo Park

Areas Of Involvement:

open source social network

Related People:

Nick Clegg Sheryl Sandberg Sean Parker Mark Zuckerberg

See all related content →

**Recent News**

Oct. 23, 2023, 4:41 AM ET (Yahoo News UK)

Brexit means UK can be global leader on AI, says Facebook co-founder

Oct. 19, 2023, 1:25 PM ET (AP)

EU demands Meta and TikTok detail efforts to curb disinformation from Israel-Hamas war

Show More

**Facebook**, American online social media platform and social network service that is part of the company Meta Platforms. Facebook was founded in 2004 by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes, all of whom were students at Harvard University. Facebook became the largest social network in the world, with nearly three billion users as of 2021, and about half that number were using Facebook every day. The company's headquarters are in Menlo Park, California.

Access to Facebook is free of charge, and the company earns most of its money from advertisements on the website. New users can create profiles, upload photos, join a preexisting group, and start new groups. The site has many components, including Timeline, a space on each user's profile page where users can post their content and friends can post messages; Status, which enables users to alert friends to their current location or situation; and News Feed, which informs users of changes to their friends' profiles and status. Users can chat with each other and send each other private messages. Users can signal their approval of content on Facebook with the Like button, a feature that also appears on many other websites. Other services that are part of Meta Platforms are Instagram, a photo- and video-sharing social network; Messenger, an instant-messaging application; and WhatsApp, a text-message and VoIP service.

The attractiveness of Facebook stems in part from cofounder Zuckerberg's insistence from the very beginning that members be transparent about who they are; users are forbidden from adopting false identities. The company's management argued that transparency is necessary for forming personal relationships, sharing ideas and information, and building up society as a whole. It also noted that the bottom-up, peer-to-peer connectivity among Facebook users makes it easier for businesses to connect their products with consumers.

The company has a complicated early history. It began at Harvard University in 2003 as Facemash, an online service for students to judge the attractiveness of their fellow

students. Because the primary developer, Zuckerberg, violated university policy in acquiring resources for the service, it was shut down after two days. Despite its mayflylike existence, 450 people (who voted 22,000 times) flocked to Facemash. That success prompted Zuckerberg to register the URL http://www.thefacebook.com in January 2004. He then created a new social network at that address with fellow students Saverin, Moskovitz, and Hughes.

The social network TheFacebook.com launched in February 2004. Harvard students who signed up for the service could post photographs of themselves and personal information about their lives, such as their class schedules and clubs they belonged to. Its popularity increased, and soon students from other prestigious schools, such as Yale and Stanford universities, were allowed to join. By June 2004 more than 250,000 students from 34 schools had signed up, and that same year major corporations such as the credit card company MasterCard started paying for exposure on the site.

In September 2004 TheFacebook added the Wall to a member's online profile. This widely used feature let a user's friends post information on their Wall and became a key element in the social aspect of the network. By the end of 2004, TheFacebook had reached one million active users. However, the company still trailed the then-leading online social network, Myspace, which boasted five million members.



The year 2005 proved to be pivotal for the company. It became simply Facebook and introduced the idea of "tagging" people in photos that were posted to the site. With tags, people identified themselves and others in images that could be seen by other Facebook friends. Facebook allowed users to upload an unlimited number of photos. In 2005 high-school students and students at universities outside the United

States were allowed to join the service. By year's end it had six million monthly active users.

In 2006 Facebook opened its membership beyond students to anyone over the age of 13. As Zuckerberg had predicted, advertisers were able to create new and effective customer relationships. For example, that year, household product manufacturer Procter & Gamble attracted 14,000 people to a promotional effort by "expressing affinity" with a teeth-whitening product. This kind of direct consumer engagement on such a large scale had not been possible before Facebook, and more companies began using the social network for marketing and advertising.

Privacy remains an ongoing problem for Facebook. It first became a serious issue for the company in 2006, when it introduced News Feed, which consisted of every change that a user's friends had made to their pages. After an outcry from users, Facebook swiftly implemented privacy controls in which users could control what content appeared in News Feed. In 2007 Facebook launched a short-lived service called Beacon that let members' friends see what products they had purchased from participating companies. It failed because members felt that it encroached on their privacy. Indeed, a survey of consumers in 2010 put Facebook in the bottom 5 percent of companies in customer satisfaction largely because of privacy concerns, and the company continues to be criticized for the complexity of its user privacy controls and for the frequent changes it makes to them.

In 2008 Facebook surpassed Myspace as the most-visited social media website. With the introduction of Live Feed, the company also took a competitive swing at the growing popularity of Twitter, a social network that runs a live feed of news service-like posts from members whom a user follows. Similar to Twitter's ongoing stream of user posts, Live Feed pushed posts from friends automatically to a member's homepage. (Live Feed has since been incorporated into News Feed.)

Facebook has become a powerful tool for political movements, beginning with the U.S. presidential election of 2008, when more than 1,000 Facebook groups were formed in support of either Democratic candidate Barack Obama or Republican candidate John McCain. In Colombia the service was used to rally hundreds of thousands in protests against the antigovernment FARC guerrilla rebellion. In Egypt, activists protesting the government of Pres. Hosni Mubarak during the uprising of 2011 often organized themselves by forming groups on Facebook.

Facebook encourages third-party software developers to use the service. In 2006 it released its application programming interface (API) so that programmers could write software that Facebook members could use directly through the service. By 2009 developers generated about $500 million in revenue for themselves through Facebook. The company also earns revenues from developers through payments for virtual or digital products sold through third-party applications. By 2011 payments from one such company, Zynga Inc., an online game developer, accounted for 12 percent of the company's revenues.

In February 2012 Facebook filed to become a public company. Its initial public offering (IPO) in May raised $16 billion, giving it a market value of $102.4 billion. By contrast, the largest IPO of an Internet company to date was that of the search-engine company Google Inc., which had raised $1.9 billion when it went public in

2004. By the end of the first day of the stock's trading, Zuckerberg's holdings were estimated at more than $19 billion.

In October 2021 Facebook announced that it was changing the name of its parent company to Meta Platforms. The name change reflected an emphasis on the "metaverse," in which users would interact in virtual reality environments and weigh their novel opportunities and risks.
*Mark Hall*

# virtual community

Table of Contents



## virtual community



Written by

Howard Lee Rheingold

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

Category: History & Society

Key People:

Howard Rheingold

Related Topics:

Internet crowdsourcing crowdfunding instant messaging chat room

See all related content →

**Virtual community**, a group of people, who may or may not meet one another face to face, who exchange words and ideas through the mediation of digital networks.

The first use of the term *virtual community* appeared in a article by Gene Youngblood written in 1984 but published in 1986 about *Electronic Cafe* (1984), an art project by artists Kit Galloway and Sherrie Rabinowitz that connected five restaurants around Los Angeles and an art museum through a live video link. The term gained popularity after a 1987 article written by Howard Rheingold for *The Whole Earth Review*. In *The Virtual Community* (1993), Rheingold expanded on his article to offer the following definition:

*Virtual communities are social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace.*
Rheingold's article and book are cited as the foundational works of cyberculture studies. Many subsequent commentators have contested Rheingold's use of the word *community* and the terminology used to describe the technosocial phenomena of persistent computer-mediated relationships; *social media* and *participatory media* are also used to describe a very broad variety of human social activity online.

The first predictions of communities of computer-linked individuals and groups were made in 1968 by J.C.R. Licklider and Robert Taylor, who as research administrators for the U.S. Defense Advanced Research Projects Agency (DARPA) set in motion the research that resulted in the creation of the first such community, the ARPANET, which was the precursor of the Internet. Licklider and Taylor wrote,

*What will on-line interactive communities be like? In most fields they will consist of geographically separated members, sometimes grouped in small clusters and sometimes working individually. They will be communities not of common location, but of common interest.*
Even before the ARPANET, in the early 1960s, the PLATO computer-based education system included online community features. Douglas Engelbart, who ran the ARPANET's first Network Information Center, had grown a "bootstrapping community" at the Stanford Research Institute (SRI), located at Stanford University in California, through use of his pioneering oNLine System (NLS) before the ARPANET was launched.



By the beginning of the 21st century, the four computer nodes (University of California at Los Angeles, SRI, University of California at Santa Barbara, and University of Utah) that constituted the ARPANET community in 1969 had expanded to include some one billion people with access to the Internet. With several billion mobile telephones with Internet connections now in existence, a significant portion of the human population conduct some of their social affairs by means of computer networks. The range of networked activities has greatly expanded since Rheingold described bulletin board systems (BBSs), chat rooms, mailing lists, USENET newsgroups, and MUDs (multiuser dungeons) in 1993. In the 21st century people meet, play, conduct discourse, socialize, do business, and organize collective action through instant messages, blogs (including videoblogs), RSS feeds (a format for subscribing to and receiving regularly updated content from Web sites), wikis, social network services such as MySpace and Facebook, photo and media-sharing communities such as Flickr, massively multiplayer online games such as *Lineage* and *World of Warcraft*, and immersive virtual worlds such as Second Life. Virtual communities and social media have coevolved as emerging technologies have afforded new kinds of interaction and as different groups of people have appropriated media for new purposes.

The emergence of globally networked publics has raised a number of psychological, sociological, economic, and political issues, and these issues have in turn stimulated the creation of new courses and research programs in social media, virtual communities, and cyberculture studies. In particular, the widespread use of online communication tools has raised questions of identity and the presentation of self, community or pseudocommunity, collective action, public sphere, social capital, and quality of attention.

A number of different critiques arose as cyberculture studies emerged. A political critique of early online activism questioned whether online relationships offered a kind of comforting simulation of collective action. On close inspection, the question of what actually defines a community has turned out to be complex: American sociologist George A. Hillery, Jr., compiled 92 different definitions. Canadian sociologist Barry Wellman defined community as "networks of interpersonal ties that provide sociability, support, information, a sense of belonging, and social identity"—and offered empirical evidence that at least some virtual communities fit these criteria. As has happened in the past, what people mean when they speak of community is shifting.

As the early digital enthusiasts, builders, and researchers were joined by a more representative sample of the world's population, a broader and not always wholesome representation of human behaviour manifested itself online. Life online in the 21st century enabled terrorists and various cybercriminals to make use of the same many-to-many digital networks that enable support groups for disease victims and caregivers, disaster relief action, distance learning, and community-building efforts. Soldiers in battle taunt their enemies with text messages, disseminate information through instant messaging, and communicate home through online videos. With so many young people spending so much of their time online, many parents and "real world" community leaders expressed concerns about the possible effects of overindulging in such virtual social lives. In addition, in an environment where anyone can publish anything or make any claim online, the need to include an understanding of social media in education has given rise to advocates for "participatory pedagogy."

Students of online social behaviour have noted a shift from "group-centric" characterizations of online socializing to a perspective that takes into account "networked individualism." Again, quoting Wellman:

*Although people often view the world in terms of groups, they function in networks. In networked societies: boundaries are permeable, interactions are with diverse others, connections switch between multiple networks, and hierarchies can be flatter and recursive....Most people operate in multiple, thinly-connected, partial communities as they deal with networks of kin, neighbours, friends, workmates and organizational ties. Rather than fitting into the same group as those around them, each person has his/her own "personal community."*

It is likely that community-centred forms of online communication will continue to flourish—in the medical community alone, mutual support groups will continue to afford strong and persistent bonds between people whose primary communications take place online. At the same time, it is also likely that the prevalence of individual-centred social network services and the proliferation of personal communication devices will feed the evolution of "networked individualism." Cyberculture studies, necessarily an interdisciplinary pursuit, is likely to continue to grow as more human socialization is mediated by digital networks.

*Howard Lee Rheingold*

# blog
# Internet



Also known as: Web log, Weblog

Written by

Michael Aaron Dennis

Fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Article History

Table of Contents

Category: Arts & Culture

**In Full:** Web log or Weblog

Key People:

Ta-Nehisi Coates David Karp Frederik Pohl Biz Stone Evan Williams

Related Topics:

Internet social media WordPress journal

See all related content →

**Blog**, in full **Web log** or **Weblog**, online journal where an individual, group, or corporation presents a record of activities, thoughts, or beliefs. Some blogs operate mainly as news filters, collecting various online sources and adding short comments and Internet links. Other blogs concentrate on presenting original material. In addition, many blogs provide a forum to allow visitors to leave comments and interact with the publisher. “To blog” is the act of composing material for a blog. Materials are largely written, but pictures, audio, and videos are important elements of many blogs. The “blogosphere” is the online universe of blogs.

## From geeks to mainstream

The World Wide Web and the idea of a blog appeared at the same time. Tim Berners-Lee, often described as the Web's inventor, created the first "blog" in 1992 to outline and render visible the ongoing development of the Web and the software necessary to navigate this new space. Web history, especially the early growth of Web servers and sites, is chronicled on the various "What's New" pages in the archives of the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign. Another example of a blog that existed before the word was coined is Slashdot. Following its debut in September 1997, Slashdot operated as a clearinghouse for information in its "News for Nerds," with a small set of editors who decided what to publish of numerous articles and news items submitted by the "geek" community. Indeed, Web sites mentioned on Slashdot were often overwhelmed, leading to a condition now known as being "slashdotted."

In December 1997, Jorn Barger, an early online presence, coined the term *web log* to describe his Web site RobotWisdom.com. In early 1999 another individual with considerable online experience, Peter Merholz, began to employ the term *blog* on his site Peterme.com. While the history of the term is pretty well settled, the same cannot be said of the identity of the first blogger. Depending on the definition of a blog, Berners-Lee may not qualify as the first blogger. Claimants to this title include Justin Hall, a college student who started an online list at links.net in 1994; Carolyn Burke, who began publishing Carolyn's Diary online in 1995; and Dave Winer, who has published Scripting News online since April 1, 1997.

The growth of the blogosphere has been nothing short of remarkable. Technorati, Inc., a Web site and organization dedicated to mapping and searching the blogosphere, found that by October 2005 there were 19.6 million blogs, a number that has been doubling roughly every five months. Approximately 70,000 new blogs are created each day—or, more vividly, nearly one every second. Also of importance is the growth of blogs in languages other than English, especially Chinese.

Despite the overwhelming number of blogs, very few individuals make a living as a blogger. A few individuals earn money from their Web sites by carrying ads and appeals for funds, and some blogs are financed by corporate or organizational owners; nevertheless, most bloggers derive nonmonetary rewards from their activity. In particular, blogs offer ordinary individuals the ultimate soapbox and an opportunity to create their own digital identity or personal brand.

One reason for the proliferation of blogs is the ease with which they can be established and maintained. Many services and software systems are available that allow an individual to set up a blog in less than an hour. Of course, updating a blog is essential for maintaining its presence and importance. Statistics on blogs that are started but not updated remain elusive, but the proportion is undoubtedly substantial.



Like the fad for personal Web pages in the 1990s, the proliferation of blogs has led to the creation of Web sites that group blogs, often with a similar political emphasis or subject orientation, to form “superblogs.” An example of this phenomenon is The Huffington Post, founded in 2005 by American author and syndicated newspaper columnist Arianna Huffington, which hosts dozens of other bloggers who post mostly on politics and current affairs.

## Dialogue

In addition to the frequency of updates, the thing that distinguishes most blogs from ordinary Web pages is the inclusion of forums for readers to post comments to which the blogger might respond. The degree to which dissenting views are tolerated depends on the publisher, but most Web sites must regularly prune “spam”—insertions of commercial and pornographic ads into the text of an apparent comment or the use of insulting and defamatory language. Trackback, an Internet function, facilitates communication by allowing bloggers to monitor who is reading and discussing their site. In turn, bloggers often post a “blogroll,” or a list of other blogs that they read and respect. Blogging is a conversational activity that seeks to create a community or reflect an existing community.

For a corporation, blogs can be used to advertise corporate products and practices and for two-way communication with consumers. For nonprofit entities such as charities, blogs allow officials to discuss their goals and actions in pursuit of a common end.

A growing phenomenon involves people who start blogs, often anonymously, to disparage someone or something that they dare not attack openly—such as their

company, boss, school, or teacher—or to tilt at some organization that "done 'em wrong." In several instances, individuals have lost their jobs when employers discovered their blogs.

## Political blogs

The U.S. presidential election of 2004 brought blogs to a newfound prominence as bloggers for both parties used the Internet as another arena of debate and conversation—as well as fund-raising. Democratic presidential primary candidate Howard Dean was the most prominent user of the Internet and the blogosphere. Dean used bloggers as unpaid advisers and cheerleaders to help build his base; in turn, bloggers rallied to Dean's campaign against the Second Persian Gulf War.

Even before the election, bloggers played a central role in demoting Mississippi Senator Trent Lott from his leadership position in the U.S. Senate. The mainstream media initially paid little attention to Lott's comments praising Strom Thurmond's 1948 Dixiecrat presidential campaign when the latter ran as an ardent segregationist. Only after left-wing bloggers made it clear that Lott had a history of such comments did the mainstream media begin a series of stories that eventually forced Lott to step down as Senate majority leader. In Britain, bloggers forced Prime Minister Tony Blair to address the substance of the so-called Downing Street memo, which purportedly showed that the Bush administration had deliberately "juiced up" military intelligence to support war against Iraq. Criticism of the mainstream media has come not only from the left. Dan Rather, a news anchor for CBS TV, was no doubt ushered into retirement in part because of right-wing bloggers' criticism of his journalistic practices during the 2004 election—a view summed up in the name of a central site: RatherBiased.com.

## Media convergence and podcasting

Despite the overheated phrase "every person a blogger," blogs are not likely to replace the mainstream media. Instead, blogs will continue to complement existing news media by allowing anyone to set up a Web site dedicated to his or her particular interest or perspective. Blogs now exist on a vast array of topics, from the latest electronic gadgets to books and movies to sex and politics, and over time the most successful blogs may be those that cater to a wide audience while not offending an even wider group. Or success may be redefined. If the purported convergence of electronic technologies—cable television, movies, and the Internet—actually takes place, blogs may become gatekeepers to the new digital frontier, making criticism and discussion an essential element of search, the most basic Internet function. Hence, search engines such as Google and Yahoo are working to make blogs part of their respective digital empires. Similarly, America Online, Inc., has bought certain blogs to acquire both technological cachet and access to the blogs' readership. Blogs may become the new "portals" to the Web.

Nor is blogging the final frontier of individual expression online. Podcasting, the use of a personal computer to create a "radio show" that users can download and play on their computer or portable music player, became the "bleeding edge" of personal performance in 2005. Podcasting derives its name from the nearly ubiquitous iPod, Apple Inc.'s portable music player. Apple's iTunes software has also played a crucial role in the spread of podcasting, as users can access

thousands of podcasts for free with a simple click of their computer's mouse. Anyone with a computer and a microphone can create an audio podcast, and the release of Apple's video iPod in 2005 set the stage for video podcasting.
*Michael Aaron Dennis*

computer network

Table of Contents

HomeTechnologyThe Web & Communication

Science & Tech

# computer network

Print Cite Share Feedback

Written and fact-checked by

The Editors of Encyclopaedia Britannica

Last Updated: Oct 19, 2023 • Article History

Table of Contents

Category: Science & Tech

Key People:

Vinton Cerf Lawrence Roberts Douglas Engelbart Leonard Kleinrock J.C.R. Licklider

Related Topics:

Internet ARPANET e-commerce social network virtual community

See all related content →

**Computer network**, two or more computers that are connected with one another for the purpose of communicating data electronically. Besides physically connecting computer and communication devices, a network system serves the important function of establishing a cohesive architecture that allows a variety of equipment types to transfer information in a near-seamless fashion. Two popular architectures are ISO Open Systems Interconnection (OSI) and IBM's Systems Network Architecture (SNA).

Two basic network types are local-area networks (LANs) and wide-area networks (WANs). LANs connect computers and peripheral devices in a limited physical area, such as a business office, laboratory, or college campus, by means of links (wires, Ethernet cables, fibre optics, Wi-Fi) that transmit data rapidly. A typical LAN consists of two or more personal computers, printers, and high-capacity

disk-storage devices called file servers, which enable each computer on the network to access a common set of files. LAN operating system software, which interprets input and instructs networked devices, allows users to communicate with each other; share the printers and storage equipment; and simultaneously access centrally located processors, data, or programs (instruction sets). LAN users may also access other LANs or tap into WANs. LANs with similar architectures are linked by "bridges," which act as transfer points. LANs with different architectures are linked by "gateways," which convert data as it passes between systems.


**Britannica Quiz**

What Do You Actually Know About the Internet?

WANs connect computers and smaller networks to larger networks over greater geographic areas, including different continents. They may link the computers by means of cables, optical fibres, or satellites, but their users commonly access the networks via a modem (a device that allows computers to communicate over telephone lines). The largest WAN is the Internet, a collection of networks and gateways linking billions of computer users on every continent.

*This article was most recently revised and updated by Erik Gregersen.*