Exclusive to Which? members

Stay safe online

Which?

Welcome

The internet is a fantastic environment for exploring and creating, and it's changing the way we live and work. The pace of change is rapid. Staying connected and being able to adapt to the constant changes can be both a necessity and a challenge.

As more and more of our lives take place on the internet, online safety has become an important life skill for consumers. Awareness of cyber attacks and online threats is high, but not many people actually know how to protect themselves online.

Nine in ten members of the UK public say they feel concerned about their online safety and security. Yet, a quarter of the public believe that they have only a limited understanding of the risks they face when going online.

As the largest independent consumer organisation in the UK, Which? has a long history of providing help and advice on the issues that matter most to people. The UK has one of the largest digital economies in the world, and consumers play a crucial role within it. We want everyone to enjoy the benefits of the internet and minimise the risks.

Learn how to spot and avoid the latest and most common online scams and threats with simple steps that everybody can apply easily in their daily lives.

RP

Richard Parris
Editor, *Which? Computing*

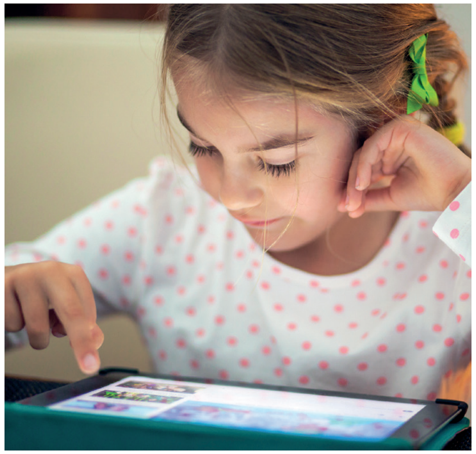
This guide has been produced for general information and interest only. Which? makes every effort to ensure that the information in the guide is correct but we cannot guarantee that it is 100% free of inaccuracies, errors and omissions.

Although Which? Ltd has endeavoured to make every effort to ensure that all steps and advice detailed in this guide are accurate and up to date, this is not guaranteed. Please note that the software and hardware features referred to can and do change and this may invalidate certain steps. Any such changes are beyond the control of Which?. All implied warranties and conditions are excluded to the maximum extent permitted by law. In particular, we will not be responsible for ensuring that the advice given in this guide is suitable for your purposes or for any data loss that may be incurred as a result of following the advice.

Contents

Common security questions

Computer security problems can be a cause for concern. Thankfully, by following some simple guidelines, it's possible to deal with almost any security threat and, in most cases, avoid problems altogether



Computers are vulnerable to a wide range of security risks – from virus attacks and spyware to hackers, scams and fraud. If a threat slips past your computer's defences, at the very least you'll be left dealing with slowdown and system conflicts. At worst, you could fall victim to identity theft and credit card fraud.

Thankfully, staying safe involves employing a simple mixture of digital tools and good common sense. Special software is needed to help protect your computer from online threats, and they should be kept up to date. It's also vital to use secure passwords for all the online services that you log in to.

Stay on the lookout for anything suspicious and learn how to spot scams, too. We show you how to manage passwords and protect your identity, as well as avoid scams. Here are some of the most frequently asked questions about computer security.

Q Should I worry about spam and junk emails?

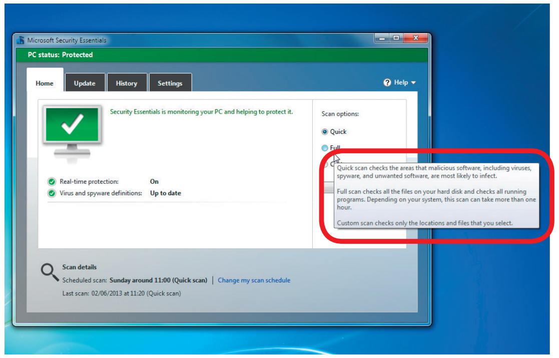
A It's an unfortunate fact of the web that having an email address can lead to all sorts of unwanted emails, known as junk or spam. Plenty of these messages are harmless – they're little more than adverts. You'll receive these having signed up to newsletters from online sites, sometimes inadvertently. But other spam messages can be more dangerous.

Spam is one of the easiest ways for virus-writers to spread their infections, and for scammers to trick victims into handing over personal details. Any unexpected emails with strange attachments, unusual links or unknown senders should be treated with caution. The good news is your spam or junk folder will often catch these for you.

Q How often should my antivirus software update and scan?

A It's vital to keep your computer's protection up to date, otherwise newer threats may be able to slip past your defences. Most security software automatically checks for updates at least once a day, although it's worth investigating your program's settings to make sure this is the case.

Your security software gives real-time protection against threats as they emerge, but regular system scans are important, too. Most security suites are configured to perform an automatic scan once a week, often offering the choice of a 'quick', 'deep' or 'full' scan. We recommend carrying out a full scan once a week. You can do a manual quick scan any time you choose if your computer is exhibiting suspicious behaviour.



PC status: Protected

Security Essentials is monitoring your PC and helping to protect it.

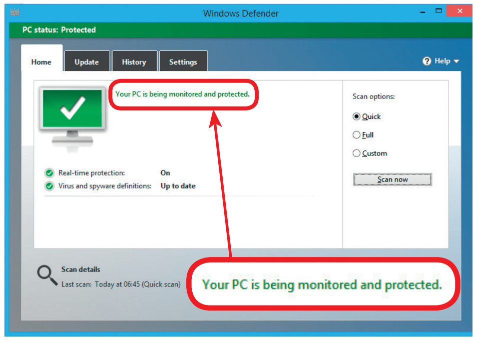
Real-time protection: On
Virus and spyware definitions: Up to date

Quick scan checks the areas that malicious software, including viruses, spyware, and unwanted software, are most likely to infect.

Full scan checks all the files on your hard disk and checks all running programs. Depending on your system, this scan can take more than one hour.

Custom scan checks only the locations and files that you select.

Scan details
Scheduled scan: Sunday around 11:00 (Quick scan) | Change my scan schedule
Last scan: 02/06/2013 at 11:20 (Quick scan)



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On
Virus and spyware definitions: Up to date

Scan details
Last scan: Today at 06:45 (Quick scan)

Your PC is being monitored and protected.

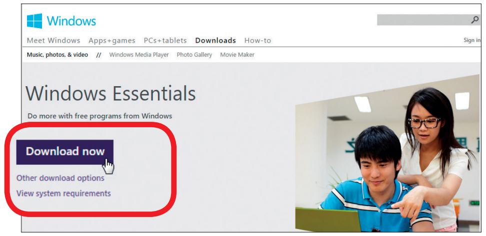
Q What type of security software do I need on my device?

A The three key tools to have on your side are a firewall, an anti-spyware tool and an antivirus program. Recent versions of Windows have these tools built in. Windows 10 offers the most complete protection; its updated version of Defender (shown above) includes antivirus, firewall and anti-spyware capabilities. If you're using any earlier version of Windows, you'll need some additional antivirus security software. There are some excellent free and paid-for security tools to keep you protected.

Q Can I control how my children use the internet?

A Plenty of antivirus programs and security apps for tablets and phones let you set limits for the ways that your children can access the internet. This could involve blocking access to adult websites, to limiting the amount of time they can spend online, or how long they can access specific apps, such as social media apps.

Windows 10 also lets you set permission levels for child accounts, allowing only pre-agreed sites and services, for example, or blocking adult sites. These controls only work if the child is logged into your computer using their own account, so make sure that any children in your household have a login of their own set up on your computer.



Windows Essentials

Do more with free programs from Windows

Security threats: know your foe

The internet is a wonderful melting pot, but it also attracts the world's con artists and tricksters. This guide will help you identify the different threats and learn how to keep the web's shadier characters at arm's length

What is it?

How do I beat it?

Malware

Malware is the catch-all term for infections on your PC, including viruses. It covers many subsets of digital nasties, including spyware, Trojans, viruses and worms.

Make sure you install and run an antivirus tool, and keep it up to date so it can counter the latest threats. The same goes for other software you use, as well as your PC's operating system. Set Windows, your internet browser and add-ons, such as Flash and Java, to update automatically.

Ransomware

Ransomware is software used by crooks to take over your PC and charge for returning it. It can lock the screen, making the machine unusable, or even encrypt all your files.

The best defence is to keep a backup of all your files on an external hard drive, rendering the threat empty. If you can't use your PC, note any details about the virus message and use another PC to search for fixes. Antivirus companies have created tools to neutralise more common ransomware.

Phishing scams

Phishing attacks are an attempt to gain personal information, such as bank or credit card details or passwords, by posing as a respectable company.

Banks and card companies say they'll never ask you to sign in via an email link, so be on high alert if you receive such emails. Place your mouse over a link – without clicking – to preview the web address and see where the link really takes you. Always type addresses directly to visit the real website.

Adware

Adware is software placed on your computer by advertising companies. You may see pop-up adverts in new windows and ads for items that you've already looked at in the past.

The free SuperAntiSpyware (**superantispyware.com**) will track down adware lurking on your hard drive. A browser extension, such as the free Ad-Block Plus, can stop all adverts appearing as you browse the internet. It won't remove any adware, but it will treat the symptoms.

Tall-tale scams

Whether it's promises of love in a romance scam, or asking for money in order to release a lottery win or unclaimed inheritance, email tricksters will try any tall-tale scam.

The old adage remains true – if it looks too good to be true, it probably is. Never respond to unsolicited emails promising money for nothing, and take extreme caution before giving any money to people you've met online. Websites such as Gumtree and dating sites warn against such scam approaches.

Understand computer viruses

Protect your computer from dangerous viruses with a few simple security measures that will combat digital threats

As with venturing out in the real world, there are risks when you go online. But, with a few simple precautions, you can enjoy all the benefits of the internet, secure in the knowledge that your personal information is protected. Above all, don't be afraid to use your computer. Scams and viruses can be avoided with a little good sense and some basic know-how. We'll show you how to enjoy the best of the web while remaining secure.

What are viruses?

A virus is a piece of malicious software, or 'malware' as it's commonly known. Typically, viruses are created by criminals to steal personal information or damage your computer. Spread over the internet, malware comes in a number of guises.

> *"It's easy to pick up a virus by doing certain activities, such as downloading files from unusual websites"*

Much like the common cold, a virus spreads quickly from computer to computer. It's easy to pick one up by doing certain things, such as downloading files from unusual websites, opening suspicious email attachments, or visiting infected websites. Viruses are often disguised as funny photos, greeting cards, music and video files.

Scan for viruses in Windows

Windows 10 has an antivirus program built-in, called Windows Defender. This scans for malware on your PC. To run a scan with Defender, type Defender into the Windows search panel and select Windows Defender to bring up the software's control panel.

You can choose to run a Quick Scan or Full Scan from the options on the right-side of the home page. A quick scan examines only the drives and folders most likely to contain bugs, while a full scan can take a long time, but will look in every nook and cranny or your PC for malware. Infected files will be cleaned, and the sources of the virus will be quarantined or deleted.

> *"Viruses are often disguised as funny photos, greeting cards, music and video files"*

How can I tell if I have a virus?

Look out for these signs of a virus – it may be time to run a scan for malware

Pop-up alerts
Unexpected pop-up windows and error messages may indicate a virus.

Sending spam
If friends receive strange emails or messages from you asking them to click on attachments or links, a virus may have hijacked your account. Change your email account's password immediately.

Sluggish computer
A virus can result in a slow-to-start computer or sluggish running speeds.

Glitchy programs
Programs may open or close automatically, or your computer system may freeze or shut down for no reason.

Files locked
Files that are encrypted, so you can't open them, could signal a virus attack.

Antivirus disabled
Some viruses disable your computer's protection: so, if you're struggling to open or install an antivirus program, your computer may be infected.

High activity
A hard drive that's more active than normal – continually making a noise – can be a sign of an infection. Likewise, a busy home broadband connection may be caused by a virus sending information back and forth across the internet.

How to control spam

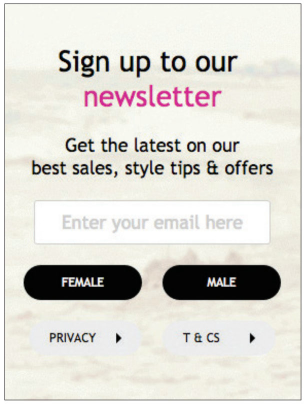
Keep your email inbox clutter-free with our top tips for tackling and avoiding unwanted spam messages

What is spam?

Spam is any email message you didn't ask for. It often originates from a person or company that you don't know. Think of spam as being the digital version of paper-based junk mail.

Its content can be hugely varied. Look in your Junk folder and you'll see offers for cut-price handbags, health supplements and adult drugs, financial loans and get-rich-quick schemes.

As it's easy and free to contact anyone with an email address, many bona fide companies such as Amazon, Marks & Spencer and John Lewis use email to promote their products and services. Using your email address when shopping online or registering on websites such as Groupon, Facebook or Twitter can result in a flood of emails hitting your inbox. Spam can also be sinister. It's easy for criminals to get their hands on email addresses and send out millions of emails in the hope that a few people respond. From phishing scams looking to steal your money to messages containing viruses and malware, some spam is potentially dangerous.



Sign up to our newsletter

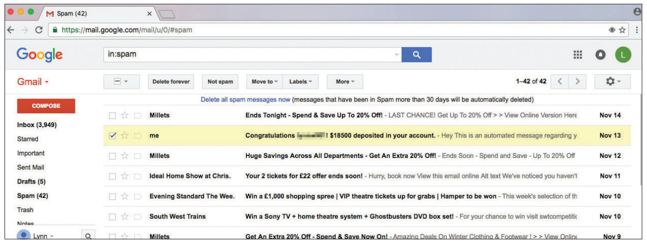
Get the latest on our best sales, style tips & offers

> "Using your email address when shopping online can result in a flood of emails hitting your inbox"

Should you worry about spam?

The good news is that your email program has a built-in filter that automatically intercepts spam heading for your inbox. It directs emails instead to a folder called **Junk** or **Spam**. If these folders are full of messages, that's a good thing! It shows that your email program's spam filters are working effectively. Messages held here are automatically deleted, normally after 30 days – so you don't need to do anything to remove them.

If a spam message slips into your inbox, click the options to report it. Your email program will now know to filter future emails from this sender, moving them to your Spam or Junk folder.



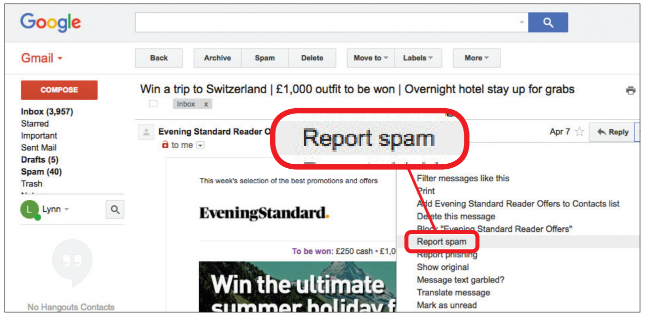
Spam (42)

https://mail.google.com/mail/u/0/#spam

in:spam

Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

Millets	Ends Tonight - Spend & Save Up To 20% Off! - LAST CHANCE! Get Up To 20% Off > > View Online Version Here	Nov 14
me	Congratulations [redacted]! $18500 deposited in your account. - Hey This is an automated message regarding y	Nov 13
Millets	Huge Savings Across All Departments - Get An Extra 20% Off! - Ends Soon - Spend and Save - Up To 20% Off	Nov 12
Ideal Home Show at Chris.	Your 2 tickets for £22 offer ends soon! - Hurry, book now View this email online Alt text We've noticed you haven't	Nov 11
Evening Standard The Wee.	Win a £1,000 shopping spree | VIP theatre tickets up for grabs | Hamper to be won - This week's selection of th	Nov 10
South West Trains	Win a Sony TV + home theatre system + Ghostbusters DVD box set! - For your chance to win visit swtcompetitic	Nov 10
Millets	Get An Extra 20% Off - Spend & Save Now On! - Amazing Deals On Winter Clothing & Footwear ! > > View Online	Nov 9



Win a trip to Switzerland | £1,000 outfit to be won | Overnight hotel stay up for grabs

Evening Standard Reader O
to me

Apr 7

This week's selection of the best promotions and offers

EveningStandard.

To be won: £250 cash • £1,0

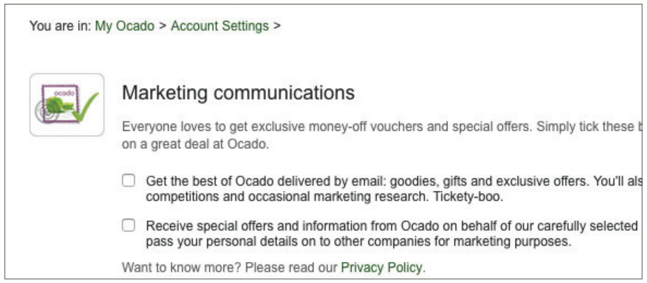
Win the ultimate summer holiday f

How to avoid spam

The best way to avoid spam is to be on as few mailing lists as possible. A mailing list holds the details of people who are happy to receive emails from a company. For example, you may agree to receive future promotions from a retailer when buying online.

But your details can be passed on to other businesses. This can lead to you receiving spam from other sources. Companies must ask your permission before adding your email address to their mailing list or sharing it with others. When you're shopping online, remember to tick or untick the relevant checkboxes asking if you're happy to receive emails from the company and from other partner companies. Read a website's privacy policy to see how your email address will be used.

Finally, never reply to spam emails. Doing so just confirms your email address, meaning you'll receive even more spam. Simply mark it as spam so your email program can add the sender to its spam list. You can usually do this by clicking **Report as spam** (or similar) when prompted.



You are in: My Ocado > Account Settings >

Marketing communications

Everyone loves to get exclusive money-off vouchers and special offers. Simply tick these b
on a great deal at Ocado.

□ Get the best of Ocado delivered by email: goodies, gifts and exclusive offers. You'll als
competitions and occasional marketing research. Tickety-boo.

□ Receive special offers and information from Ocado on behalf of our carefully selected
pass your personal details on to other companies for marketing purposes.

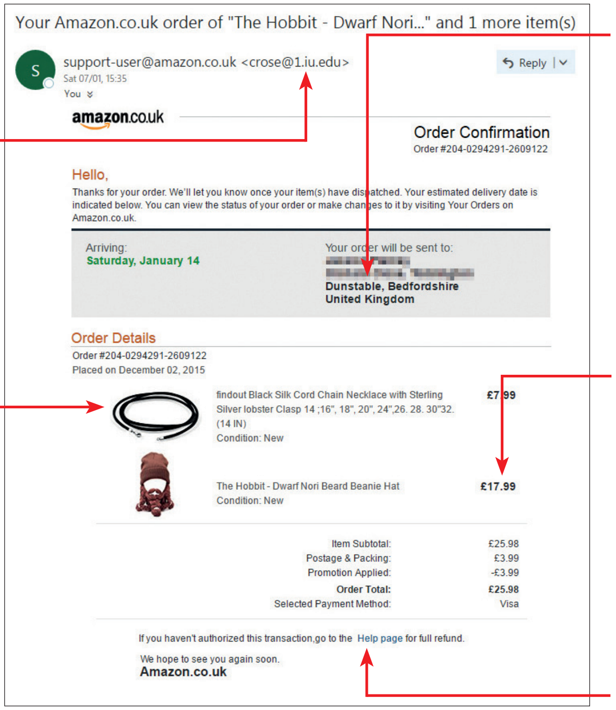
Want to know more? Please read our Privacy Policy.

Amazon invoice scam

This scam email looks remarkably like the real deal. However, it's designed to steal your email password

Always check the email address of the sender. This one – crose@1.iu.edu – isn't an Amazon account. It's one of the main clues that the email is fake.

Remarkably, clicking through on the items does take you to the genuine listings for them on Amazon. This helps build confidence that the email might be the real deal.



Your Amazon.co.uk order of "The Hobbit - Dwarf Nori..." and 1 more item(s)

support-user@amazon.co.uk <crose@1.iu.edu>
Sat 07/01, 15:35
You

amazon.co.uk

Order Confirmation
Order #204-0294291-2609122

Hello,

Thanks for your order. We'll let you know once your item(s) have dispatched. Your estimated delivery date is indicated below. You can view the status of your order or make changes to it by visiting Your Orders on Amazon.co.uk.

Arriving:
Saturday, January 14

Your order will be sent to:
[redacted]
Dunstable, Bedfordshire
United Kingdom

Order Details
Order #204-0294291-2609122
Placed on December 02, 2015

findout Black Silk Cord Chain Necklace with Sterling Silver lobster Clasp 14 ;16", 18", 20", 24",26. 28. 30"32. (14 IN)
Condition: New — £7.99

The Hobbit - Dwarf Nori Beard Beanie Hat
Condition: New — £17.99

Item Subtotal:	£25.98
Postage & Packing:	£3.99
Promotion Applied:	-£3.99
Order Total:	**£25.98**
Selected Payment Method:	Visa

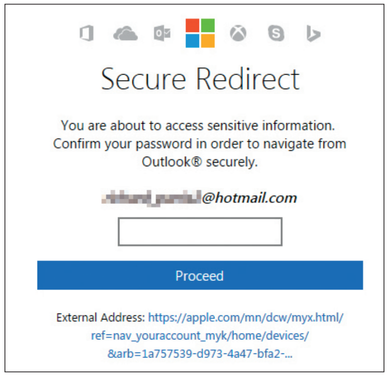
If you haven't authorized this transaction,go to the Help page for full refund.

We hope to see you again soon.
Amazon.co.uk

The order is being sent to an address in someone else's name. This is to panic you into thinking your Amazon account has been hacked.

A lot of care has gone into the design of this scam email. It's laid out exactly like a genuine invoice from Amazon, with a list of purchased items and total fee including postage.

There is only one clear link in the email, to a help page that supposedly lets you cancel the order. Click on the link and you're taken to a 'Secure Redirect' page (see below).



Secure Redirect

You are about to access sensitive information. Confirm your password in order to navigate from Outlook® securely.

[redacted]@hotmail.com

External Address: https://apple.com/mn/dcw/myx.html/ref=nav_youraccount_myk/home/devices/&arb=1a757539-d973-4a47-bfa2-...

This has nothing to do with Amazon. Instead, it's attempting to harvest your email password. This could give a hacker the means to log into multiple accounts that use this email address and password.

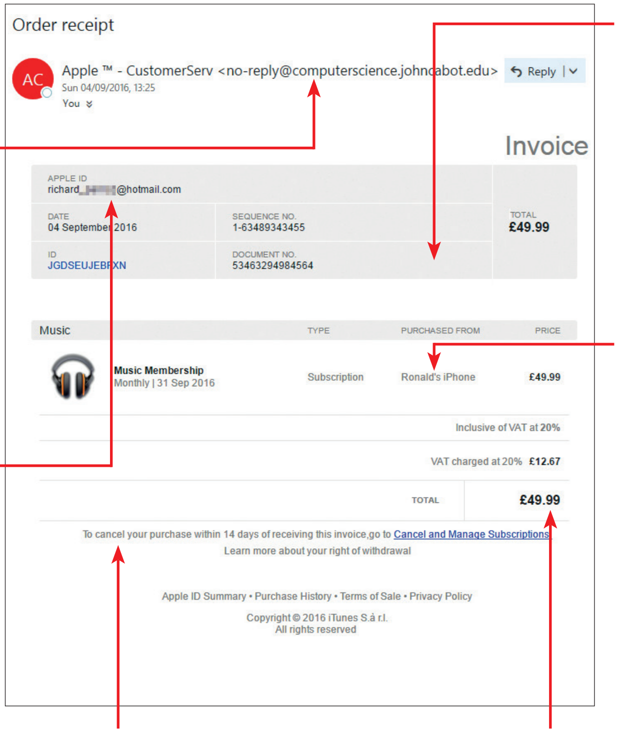
The page has convincing branding for Microsoft services. There's a link at the bottom that appears to be Apple-branded. Clicking this simply takes you in circles, refreshing the same 'Secure Redirect' page.

Apple iTunes scam

We've seen a big increase in this sort of scam, wherein victims are sent a fake invoice following a supposed Apple purchase

Though the email is allegedly from Apple, the email sender shows an address that clearly has nothing to do with the genuine company.

The Apple ID may indeed be your own, if you use your email address for this. That can make the invoice look as though it's genuine, at first glance.



Order receipt

Apple ™ - CustomerServ <no-reply@computerscience.johncabot.edu>
Sun 04/09/2016, 13:25
You

Invoice

APPLE ID
richard_[redacted]@hotmail.com

DATE 04 September 2016	SEQUENCE NO. 1-63489343455	TOTAL **£49.99**
ID JGDSEUJEBFXN	DOCUMENT NO. 53463294984564	

Music	TYPE	PURCHASED FROM	PRICE
Music Membership Monthly | 31 Sep 2016	Subscription	Ronald's iPhone	£49.99

Inclusive of VAT at 20%

VAT charged at 20% £12.67

TOTAL **£49.99**

To cancel your purchase within 14 days of receiving this invoice,go to Cancel and Manage Subscriptions
Learn more about your right of withdrawal

Apple ID Summary • Purchase History • Terms of Sale • Privacy Policy

Copyright © 2016 iTunes S.à r.l.
All rights reserved

A genuine Apple invoice (see *p16*) will have your billing address and card details listed. This scam email can't supply such detail.

The details within the invoice may not match your own. This email claims the purchase was made on 'Ronald's iPhone', despite the message being sent to a Richard.

The link claims to take you to a page that lets you cancel your order. However, this doesn't lead to a genuine Apple page. Instead, it takes you to a scam page where you submit your details.

The order is for a high value item – a monthly subscription of £49. This large amount is designed to panic victims into clicking the link to cancel the expensive order.

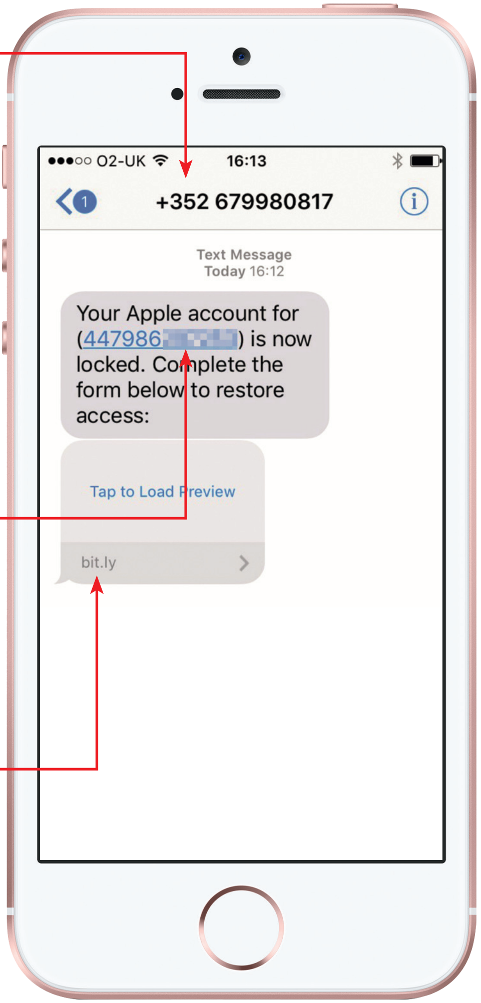
Text message scams

Scams aren't simply sent by email – these days, you're just as likely to receive one on your phone by text message

! The message arrives from an unknown sender. Though the text claims to be related to your Apple account, there's no Apple name for the sender. The +352 prefix is Luxembourg's country dialling code.

! The phone number will genuinely be your own. The wording of the message is alarmist, telling you that your Apple account has been locked.

! You're told to complete a form by following a link. Where this leads is disguised by a shortened address, with no preview detail for the page it goes to.



+352 679980817

Text Message
Today 16:12

Your Apple account for (447986[redacted]) is now locked. Complete the form below to restore access:

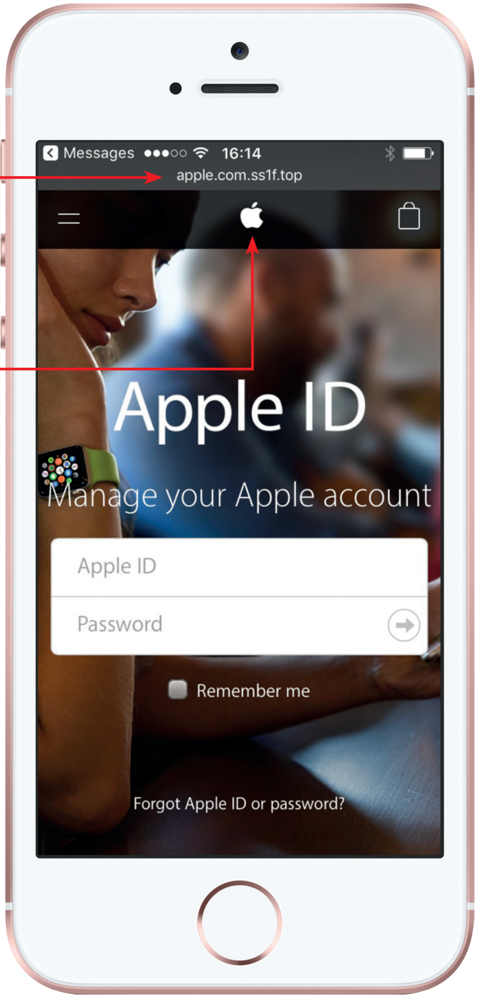
Tap to Load Preview

bit.ly

If you tap on the link, you're presented with a page that looks very similar to an Apple login.

! The address at the top appears to be real, but is actually mimicking a genuine Apple website address.

! If you attempt to tap on any of the logos or icons at the top, these lead nowhere and give no further dropdown options.



apple.com.ss1f.top

Apple ID

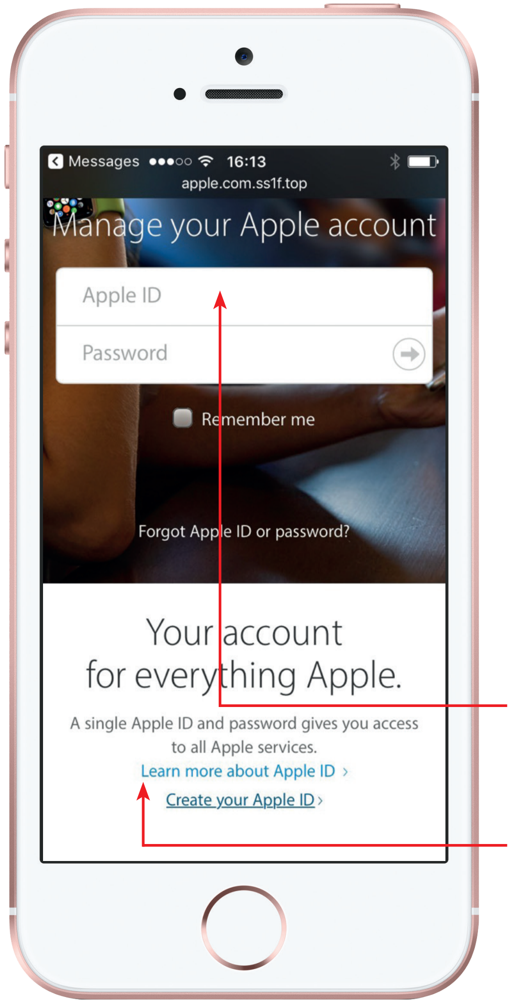
Manage your Apple account

Apple ID

Password

□ Remember me

Forgot Apple ID or password?



apple.com.ss1f.top

Manage your Apple account

Apple ID

Password

□ Remember me

Forgot Apple ID or password?

Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID ›

Create your Apple ID ›

! Entering your Apple ID and password is the risk here – you're submitting your details to a scammer that can then misuse these, potentially for financial gain.

! The options at the bottom of the page to **Learn more** about your ID or create a new one simply loop you back to the same login page.

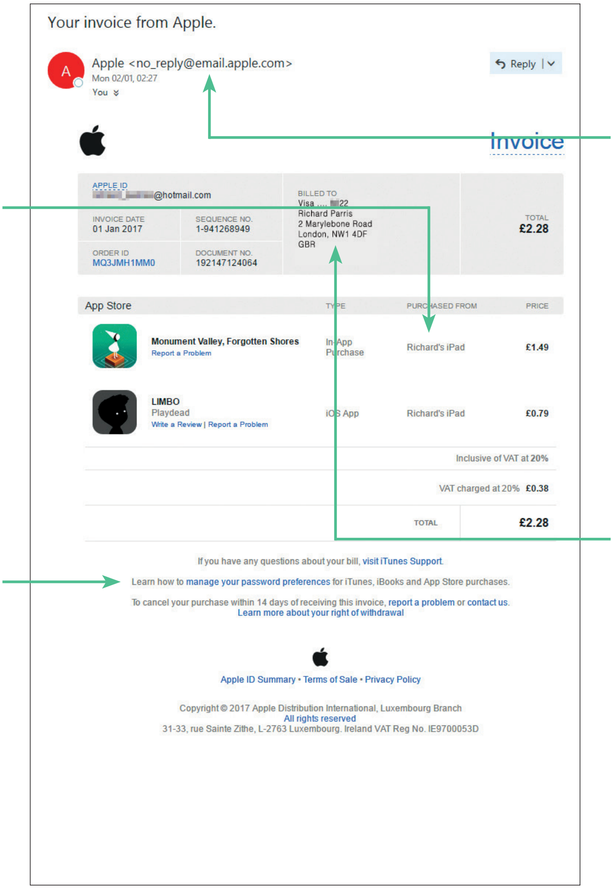
How to spot genuine emails

With so many scam emails clogging up inboxes, it's easy to doubt even genuine email messages. We show you the signs that you can trust

Real Apple invoices Fake invoices for iTunes or App Store purchases are a common scam. The real deal can look only subtly different, but there are some important distinctions.

✓ A real App Store or iTunes invoice will list the device used to make the purchase. Look out for this and check that it matches up to the name of your iPad, iPhone or computer.

✓ There are multiple links at the bottom, taking you to various genuine Apple pages. If you're in doubt, hover over the links with your cursor – a preview address should show at the bottom of your browser.



Your invoice from Apple.

Apple <no_reply@email.apple.com>
Mon 02/01, 02:27
You

APPLE ID
[redacted]@hotmail.com

INVOICE DATE
01 Jan 2017

SEQUENCE NO.
1-941268949

ORDER ID
MQ3JMH1MM0

DOCUMENT NO.
192147124064

BILLED TO
Visa .... [redacted]22
Richard Parris
2 Marylebone Road
London, NW1 4DF
GBR

TOTAL
£2.28

App Store	TYPE	PURCHASED FROM	PRICE
Monument Valley, Forgotten Shores Report a Problem	In-App Purchase	Richard's iPad	£1.49
LIMBO Playdead Write a Review | Report a Problem	iOS App	Richard's iPad	£0.79
		Inclusive of VAT at 20%	
		VAT charged at 20%	£0.38
		TOTAL	£2.28

If you have any questions about your bill, visit iTunes Support.

Learn how to manage your password preferences for iTunes, iBooks and App Store purchases.

To cancel your purchase within 14 days of receiving this invoice, report a problem or contact us.
Learn more about your right of withdrawal

Apple ID Summary • Terms of Sale • Privacy Policy

Copyright © 2017 Apple Distribution International, Luxembourg Branch
All rights reserved
31-33, rue Sainte Zithe, L-2763 Luxembourg. Ireland VAT Reg No. IE9700053D

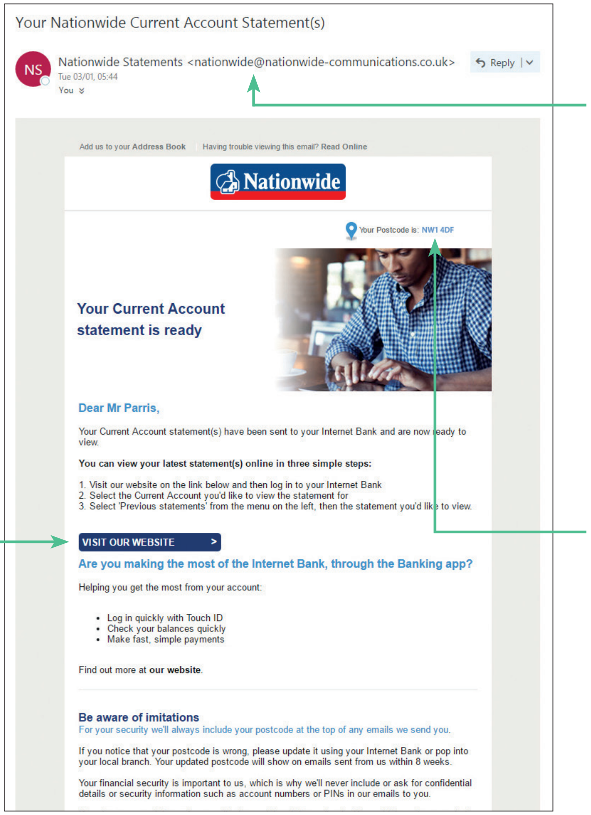
✓ When you check the email sender, you should see an address that relates to Apple. Addresses that urge you not to reply directly are usually genuine – it's the scam messages that prompt you to reply or act quickly.

✓ Genuine Apple invoices will always list your billing address and the last digits of your card details. A scammer won't have access to such 'offline' information.

Real bank emails Banking email scams are among the most dangerous, but a genuine email from your bank will have certain protections in place.

✓ Most genuine emails from a bank or building society will contain warnings about imitation emails at the bottom. The bank should flag that it will never ask for password, Pin or account numbers by email – these are scam tactics.

✓ Clicking the link in this example takes you to the front page of Nationwide's site. If you're in doubt about whether or not to click through, navigate to the webpage separately by typing the official address in a new window.



Your Nationwide Current Account Statement(s)

Nationwide Statements <nationwide@nationwide-communications.co.uk>
Tue 03/01, 05:44
You

Add us to your Address Book | Having trouble viewing this email? Read Online

Your Postcode is: NW1 4DF

Your Current Account statement is ready

Dear Mr Parris,

Your Current Account statement(s) have been sent to your Internet Bank and are now ready to view.

You can view your latest statement(s) online in three simple steps:

1. Visit our website on the link below and then log in to your Internet Bank
2. Select the Current Account you'd like to view the statement for
3. Select 'Previous statements' from the menu on the left, then the statement you'd like to view.

Are you making the most of the Internet Bank, through the Banking app?

Helping you get the most from your account:

- Log in quickly with Touch ID
- Check your balances quickly
- Make fast, simple payments

Find out more at **our website**.

Be aware of imitations
For your security we'll always include your postcode at the top of any emails we send you.

If you notice that your postcode is wrong, please update it using your Internet Bank or pop into your local branch. Your updated postcode will show on emails sent from us within 8 weeks.

Your financial security is important to us, which is why we'll never include or ask for confidential details or security information such as account numbers or PINs in our emails to you.

✓ The sender will have an email address that's clearly branded as belonging to your bank. Anything that looks non-official should be treated with caution.

✓ Your real bank will have some 'offline' detail about you, such as your home address or postcode, to prove this is an official email.

Use public wi-fi safely

Public wi-fi networks keep you connected on the move
– stay safe with just a few precautions

When you're out and about with your tablet or phone, the public wi-fi networks in coffee shops, cafes and pubs can be a godsend, enabling you to connect your tablet to the internet at higher speeds than with some 3G or 4G services, and without the expense. Unfortunately, free wi-fi isn't always safe wi-fi. There's a small possibility of hackers creating dummy public wi-fi networks and siphoning off data, usernames and passwords when you connect to the internet through them. Or, hackers may join unsecured or open networks and try to steal data from other users. You may never even know.

This doesn't mean you should avoid using public wi-fi, but you need to be more cautious when using it than when connecting to a network at work or at home.

Safe steps for public wi-fi

Take care when choosing your network. If you're in a coffee shop or other public space, ask staff for the network name or look for a sign. Then go to Settings and tap Wi-Fi, or drag your finger down from the top-right corner of the screen and tap the Wi-Fi icon. You'll see all the wi-fi networks in range listed. Tap the one that matches the details you've been given. Be wary if several similar networks are listed, or if the network name is slightly different.

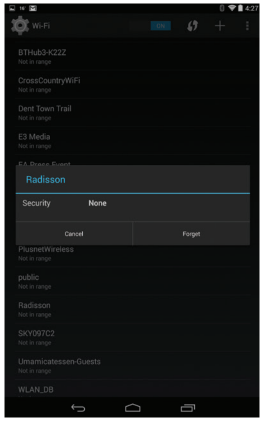
Secure networks – ones with a closed padlock over the wi-fi symbol – are safer than open ones. You may need to enter a password to use them – ask staff or look for a sign or poster with details. Many public wi-fi networks operate without a password to make it easier for customers to connect, but this also makes it easier for anyone to connect if they're in range. Be extra careful on an open network, but be aware that a password-protected network isn't necessarily more secure if the passwords are displayed prominently.

NO BANKING

Public wi-fi is generally safe and reliable, but it's worth being cautious in one regard. Don't trust the wi-fi in a coffee shop or any other public area for your online banking.

Even with the security measures in place on your mobile banking app, it's a little risky to make financial transactions over a wi-fi network you can't fully trust. The chances of someone intercepting your data are exceptionally small, but it pays to be cautious.

Rather than using the wi-fi in a shop or restaurant, you're better off using your phone's 3G or 4G signal. If possible, wait until you get home or to work, where you can use a wi-fi signal you know for sure is secure.



BTHub3-K22Z
Not in range

CrossCountryWiFi
Not in range

Dent Town Trail
Not in range

E3 Media
Not in range

FA Press Event

Radisson

Security None

PlusnetWireless
Not in range

public
Not in range

Radisson
Not in range

SKY097C2
Not in range

Umamicatessen-Guests
Not in range

WLAN_DB

What to do with scam emails

If you think you've slipped up with a scam email, don't fret
– there are quick ways to recover from mistaken clicks

"I receive lots of scam emails

RISK: LOW

Scam emails are an unpleasant, but common, part of the web. It's not unusual for your **Junk** or **Spam** folder to fill with them. This simply shows that your email filtering is working as it should. If such emails make it to your main inbox, use your email system's tools to mark them as **Spam**, or simply delete them.

"I opened a scam email

RISK: LOW

If you open a scam email and read its contents, don't worry. This alone isn't enough to install a virus or lift any personal or financial details. You would need to take further steps to put your data or your PC in danger. For instance, you'd need to click a link, fill in personal details, or open a file to put yourself at risk.

"I clicked a link in a scam email

RISK: MEDIUM

If you click through on a link contained within a scam email, there is some risk. Occasionally, this can install a virus onto your device, or create mischief with your web browser, such as displaying annoying pop-up messages. The best defence is to run a full scan with your antivirus software to make sure everything is secure.

"I replied to the email

RISK: MEDIUM

Most scam emails don't want you to reply directly – they're sent in their thousands by an automated service, rather than by an individual person. However, if you reply, this can validate your email address in the eyes of the spammer. It shows that yours is a live account and worth sending further messages to. Mark any further messages as **Spam** or **Junk** to keep them under control.

"I downloaded a file

RISK: HIGH

Downloading files attached to scam emails is more serious – this is one of the most common ways that viruses can be distributed between computers. You will definitely need to run an antivirus scan to stay protected if you've already downloaded a dodgy file from an unusual email. This process should quarantine and remove the file in question, and make sure your computer is safe.

"I gave my details

RISK: HIGH

If you entered a password, login or financial details on a scam site, you need to act fast. Change your password for the service in question at its official site. You may need to change your email password, too, if you use the same one as you do on the website. If you've supplied financial details, alert your bank. Your bank may need to temporarily freeze payments from your account as a precaution.

Windows security

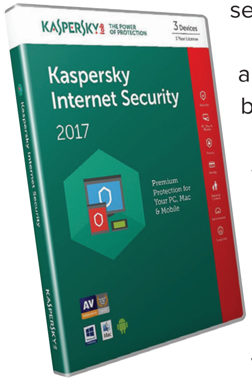
Protect your PC with a few simple security measures

Windows PCs

The best way to protect a Windows PC is to use additional antivirus software. This stops malware from being installed, and removes existing malware before it can cause damage. Windows 10 has security built-in (Windows Defender) and it's certainly competent. But our tests have found it's not as water-tight as the very best paid-for security software.

There are lots of good-quality, free antivirus programs available. Or, you can buy a security suite with an annual fee.

A paid-for security suite costs between £20 to £60. As well as antivirus, they have extra features, such as automatic updates to protect against the latest types of malware, along with some handy tools for maintenance, backup and recovery. These can help restore your PC, should it get a virus infection.


KASPERSKY THE POWER OF PROTECTION
3 Devices
Kaspersky Internet Security
2017
Premium Protection for Your PC, Mac & Mobile

PAID-FOR SOFTWARE

● Multi-device
Covers several computers, tablets and smartphones with one subscription.

● Aggressive defence
Proactive scanning and up-to-date virus protection.

● Parental controls
Manage the websites that children can access and hours of internet usage.

● Identity protection
Feel secure when you do online banking and shopping.

● Extra features
Some will back up files, protect your passwords and tune your PC performance.

FREE PROTECTION

● Basic security
Eliminates malware, but few added extras and limited scan options.

● Anti-phishing browser tools
Some free software gives you extensions for your web browser to spot scam websites.

● Single device
If you want to protect more than a single device, you'll have to install the software individually on each one, without being able to oversee the protection from one central hub.

Best paid-for antivirus software

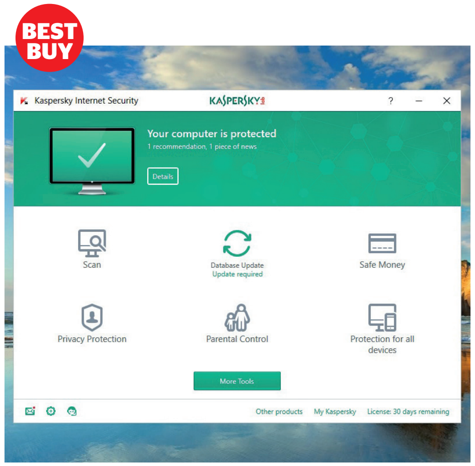
Kaspersky Internet Security 2017

£25 per year **81%**

Our best security suite on test, we love Kaspersky Internet Security's proactive approach. Insert a USB memory stick and the program scans it immediately, and it's just as quick to react against infected files being copied to the desktop. It also protects well against online phishing scams.

The package has some useful features to protect your online identity. It gives you secure browsing for shopping and banking online, plus an on-screen keyboard to fool malicious programs that try to steal your passwords as you type them.

> *“Our best security suite on test, we love Kaspersky's proactive approach”*



Your computer is protected

1 recommendation, 1 piece of news

Update required

License: 30 days remaining

Best free antivirus software

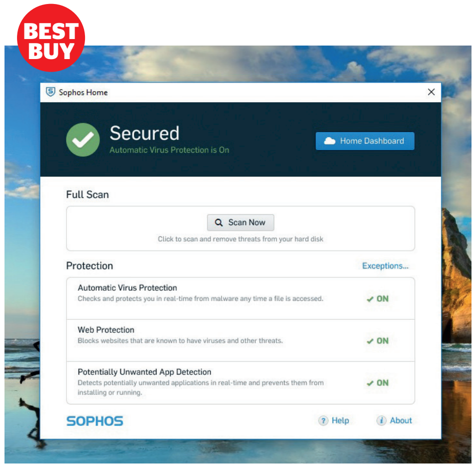
Sophos Home

Free **78%**

This is easily the best free Windows security we've tested. Sophos Home is a basic product that's superb at keeping your PC safe from harm with Best Buy virus protection to keep you secure.

It found pretty much every virus we planted on our test PC. Hook up an infected Android device and Sophos will block the malware on it before it has a chance to do any damage. And, if you're concerned about getting taken in by online phishing scams, Sophos's protection will give you peace of mind. Scam websites are flagged the moment you land on them.

> *“Hook up an infected Android device and Sophos will block the malware on it”*



Secured

Automatic Virus Protection is On

Click to scan and remove threats from your hard disk

Automatic Virus Protection — Checks and protects you in real-time from malware any time a file is accessed. ✓ ON

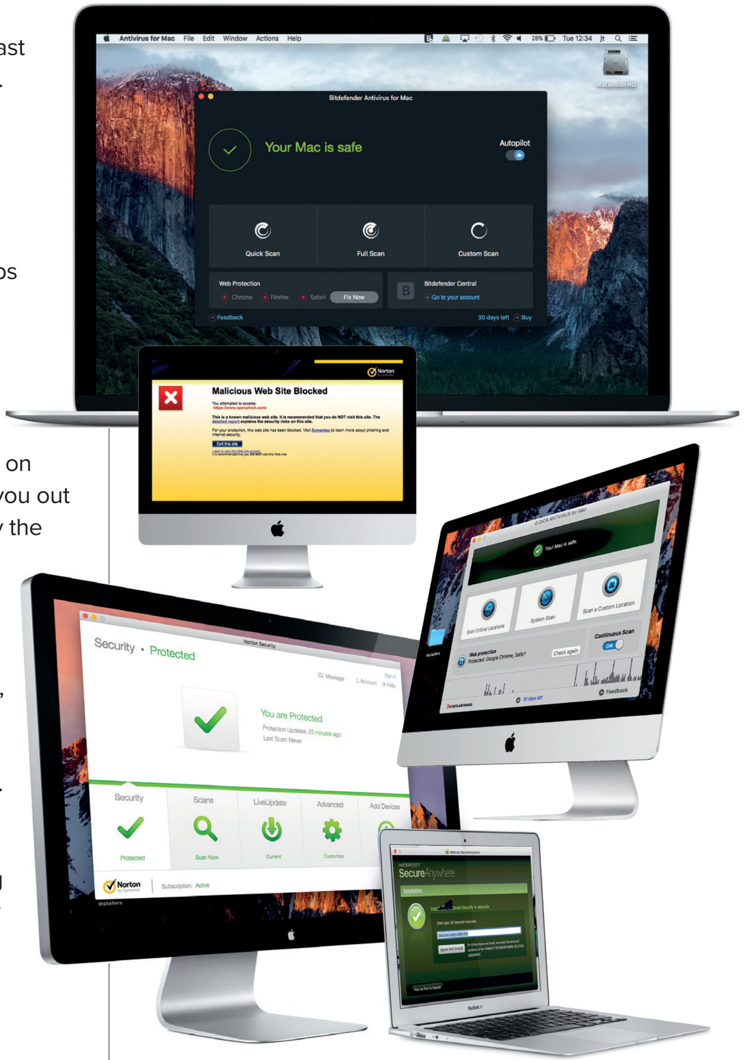
Web Protection — Blocks websites that are known to have viruses and other threats. ✓ ON

Potentially Unwanted App Detection — Detects potentially unwanted applications in real-time and prevents them from installing or running. ✓ ON

Mac security software

Protect your Apple computer against scams and pop-up messages

One of the happy reasons for owning an Apple Mac is missing out on the vast gamut of Windows-targeted malware. But, although Macs are less prone to viruses, they're not watertight.



Adware

Macs are increasingly falling prey to adware attacks. These lead to pop-ups that interrupt your web browsing or day-to-day computing with annoying messages and new windows.

Ransomware

We've also seen ransomware attacks on Macs – a type of malware that locks you out of your files or system unless you pay the scammer behind the malware.

Non-Mac viruses

Mac systems can store infected files that affect Windows or Android users, even if they don't create problems for Mac OS. A Mac user could inadvertently pass on such infections.

Phishing scams

Mac users can land on scam phishing sites just as easily as a Windows user might. These fraudulent websites imitate genuine brands in an attempt to steal login or financial data.

The good news is there is a range of quality security software available for Mac OS. In our tests, we've found that the best Mac security tools will cost around £30 per year.

Free Mac security software is also an option. We've found that this can give you good basic protection – letting you do a manual scan of your system at your own prompting. But free software doesn't give you as strong a defence, and often lacks protections against phishing scams.

Best paid-for software

Bitdefender

£39 per year **76%**

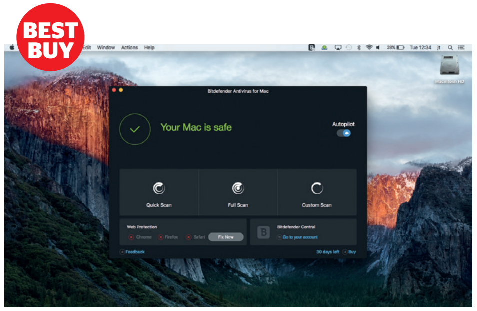
When it comes to the most common type of infection for Mac users – adware pop-ups – it takes stern stuff to get past Bitdefender's hardy defences. The software scans new files copied to your desktop or from USB sticks in real time and barely misses a thing. Infected files that we downloaded from the internet were also dealt with effectively by Bitdefender.

The program's anti-phishing tool is among the very best we've tested on security software for Macs, blocking fraudulent websites. Bitdefender also prevents you from passing Windows or Android malware on to other devices.

While it's running or performing a scan, Bitdefender works smoothly in the background, without noticeably affecting how your Mac starts up or opens programs. The virus-alert messaging could be a little more detailed, but this is a minor complaint.

VERDICT The best Mac security we've tested this year, providing great protection.

BEST BUY


Bitdefender Antivirus for Mac

Your Mac is safe

Autopilot

Quick Scan | Full Scan | Custom Scan

Web Protection: Chrome, Firefox, Safari — Fix Now

Bitdefender Central — Go to your account

Feedback — 30 days left — Buy

Best free software

Avast Free Mac Security

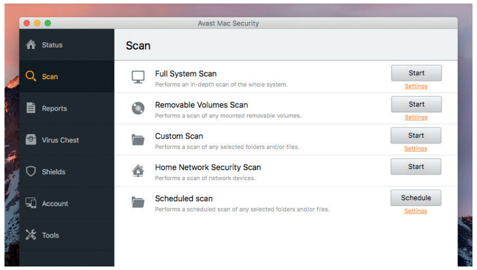
Free **70%**

Avast's free antivirus for Macs is back-to-basics software that handles threats pretty well. It's not as strong as paid-for software, but as a free layer of protection, it will give you some peace of mind and won't slow down your computer as it runs, either.

It's simple to perform full manual scans of your computer, and few pieces of software for Mac are more thorough. When the powerful malware detector identifies a threat, the warning messages are clear and consistent. But, it doesn't scan files automatically as you port them onto your computer, and you can't set scheduled scans.

While you're browsing online, it protects you against phishing scams – fraudulent imitation websites. However, you need to use the Google Chrome browser for this protection – Avast won't help if you use Safari, the built-in browser for Macs.

VERDICT A great free tool for manual scanning, but not a particularly proactive defence – you'll need to initiate scans.


Avast Mac Security

Status
Scan
Reports
Virus Chest
Shields
Account
Tools

Scan

Full System Scan — Performs an in-depth scan of the whole system. — Start — Settings

Removable Volumes Scan — Performs a scan of any mounted removable volumes. — Start — Settings

Custom Scan — Performs a scan of any selected folders and/or files. — Start — Settings

Home Network Security Scan — Performs a scan of network devices. — Start

Scheduled scan — Performs a scheduled scan of any selected folders and/or files. — Schedule — Settings

Tablet and phone security

Don't take chances with your tablet or smartphone – we round up the best security apps

Q Do I need a mobile security app?

A Yes. Smartphones and tablets are mini-computers. You can do almost anything with them that you'd be able to on a PC – open emails, download apps, browse the web and make online transactions. As such, they're open to a number of online risks.

Q What are the main threats?

A It's possible to install a virus on a phone or tablet (see right), though unlikely. The main security risk is the possibility of landing on a dangerous phishing website. These are scam sites that imitate genuine brands in an attempt to harvest your login or financial data. A good security app will block you from reaching such sites or display a warning message.

Q I thought tablets and phones can't get viruses?

A It's highly unlikely a mobile device will contract a virus, compared to, say, a Windows computer. But it's not impossible. Viruses that lock the screen or cause errors and crashes have been reported on both Android and Apple devices, though they remain uncommon.

> *“The main security risk is the possibility of landing on a dangerous phishing website”*

Q How would I get a virus on a mobile device?

A Both Apple and Android do a good job of vetting their app stores to prevent dodgy, virus-ridden apps. But you can add apps outside of the Google Play app store on Android devices. Attachments to texts and emails can potentially carry viruses, too.

Q What else can security apps do to help?

A A good security app will usually have 'lost device' features, which build on those supplied by Android or Apple. You could use your security app to track its whereabouts, lock it from access, wipe it remotely, or take a picture of the person trying to access it.

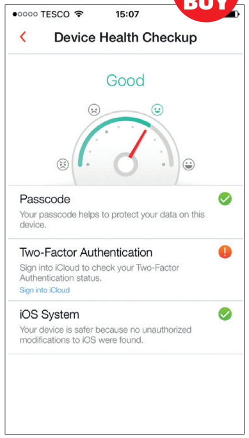
Apple iOS security apps

Protect your iPhone or iPad with a security tool to guard against scam phishing sites and lost devices.

Trend Micro Mobile Security Web Protection

£15 per year **83%**

BEST BUY



Device Health Checkup

Good

Passcode ✓
Your passcode helps to protect your data on this device.

Two-Factor Authentication !
Sign into iCloud to check your Two-Factor Authentication status.
Sign into iCloud

iOS System ✓
Your device is safer because no unauthorized modifications to iOS were found.

This is the tightest security app we've tested for Apple iOS. Its anti-phishing is almost perfect, catching nearly every scam we tried to get past it. The downside, however, is that you have to use Trend Micro's own browser for this to work, rather than Safari.

It has a remote location feature. This helps you find your phone if you've lost it. We found this easy to set up, and it located our phone quickly. It's easy to use this clearly laid-out app, and there's no noticeable slowdown while it runs on your device.

VERDICT The best Mac security we've tested this year, providing great protection.

> *“Its anti-phishing is almost perfect, catching nearly every scam we tried to get past it”*

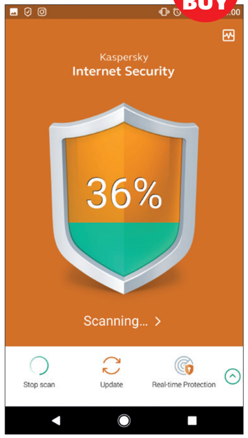
Android security apps

It's easier to get a virus on an Android device than it is on an Apple, so guard against such threats with the right security app.

Kaspersky Antivirus & Security

£10 per year **76%**

BEST BUY



This app does well at detecting malware on a scan. You can prompt manual scans or schedule them. You don't have to do anything to get rid of malware – the app wipes it automatically.

Many mobile security apps for Android only detect and delete Android-specific malware. Kaspersky will even spot Windows viruses on your Android device. It protects brilliantly against phishing sites, plus lets you remotely locate, lock or wipe a lost device. You can get this app as part of a multi-device Kaspersky licence, too.

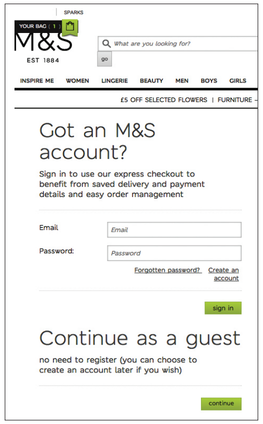
VERDICT Excellent paid-for protection for Android tablets and smartphones.

> *“This app lets you remotely locate, lock or wipe a lost device”*

Online shopping

Grab yourself a bargain online with our guide to buying things securely on the internet and paying safely.

Set up an online shopping account



SPARKS

YOUR BAG (1)

M&S EST 1884

What are you looking for?

go

INSPIRE ME WOMEN LINGERIE BEAUTY MEN BOYS GIRLS

£5 OFF SELECTED FLOWERS | FURNITURE

Got an M&S account?

Sign in to use our express checkout to benefit from saved delivery and payment details and easy order management

Email: Email

Password: Password

Forgotten password? Create an account

sign in

Continue as a guest

no need to register (you can choose to create an account later if you wish)

continue

Before you buy from most online shops, you'll need to create a customer account with them. This involves making a username – usually your email address – and choosing a password.

Go to the website (such as amazon.co.uk) and click either **Create an account** or **Register**. Follow the instructions to create an account. When you visit the website again, you can click **Sign in** and enter your username and password.

You'll need to enter your contact details, delivery address and the details of the credit or debit card you wish to pay with. The online store saves this information securely, so the next time you visit the website, it remembers who you are.

Getting a refund

To get a refund, you will need to return the item to the seller. You can either return items to one of the online retailer's physical stores or via Royal Mail, Collect+ or other courier services. The online shop will list the return methods on its website, normally under the website's **Returns & Refunds** section.

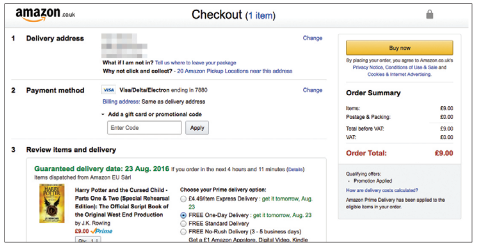
Checkout and payment

1 **Add to your basket** Most online shops use virtual shopping baskets. When you see an item you wish to buy, click the button that says **Add to basket** (or similar). You can carry on shopping, or click **View your basket** to delete items or change quantities.

2 **Proceed to checkout** When you've finished shopping, click the **Proceed to Checkout** button (or similar). You should be given the chance to check details of your chosen items before placing the order.

You can also select delivery details. Standard delivery for most online stores is typically three to five working days. Many offer faster delivery for an extra charge.

3 **Pay and confirm** You'll now see a confirmation page with details of what you've just bought and an order number. Keep a note of this until your goods arrive. A confirmation receipt will be emailed to you.



amazon.co.uk Checkout (1 item)

1 Delivery address [redacted] Change

What if I am not in? Tell us where to leave your package

Why not click and collect? - 20 Amazon Pickup Locations near this address

2 Payment method VISA Visa/Delta/Electron ending in 7880 Change

Billing address: Same as delivery address

▾ Add a gift card or promotional code

Enter Code Apply

3 Review items and delivery

Guaranteed delivery date: 23 Aug. 2016 If you order in the next 4 hours and 11 minutes (Details)

Items dispatched from Amazon EU Sàrl

Harry Potter and the Cursed Child - Parts One & Two (Special Rehearsal Edition): The Official Script Book of the Original West End Production

by J.K. Rowling

£9.00 ✓Prime

Qty: 1

Choose your Prime delivery option:

○ £4.49/item Express Delivery : get it tomorrow, Aug. 23

● FREE One-Day Delivery : get it tomorrow, Aug. 23

○ FREE Standard Delivery

○ FREE No-Rush Delivery (3 - 5 business days)

Get a £1 Amazon Appstore, Digital Video, Kindle

Buy now

By placing your order, you agree to Amazon.co.uk's Privacy Notice, Conditions of Use & Sale and Cookies & Internet Advertising.

Order Summary

Items:	£9.00
Postage & Packing:	£0.00
Total before VAT:	£9.00
VAT:	£0.00
Order Total:	£9.00

Qualifying offers:

- Promotion Applied

How are delivery costs calculated?

Amazon Prime Delivery has been applied to the eligible items in your order.

RETURNING AN ITEM

You can cancel an online order as long as you do so within 14 working days from receiving your goods. You then have another 14 days to return the unused item. Some online shops, including Marks & Spencer and John Lewis, will offer a more generous window for returns.

Online banking

Once you get started with online banking, you can transfer money or check on your bank balance from your computer.

I've never banked online before – how do I get started?

Banks actively want their customers to bank online, and generally aim to make the process of getting started straightforward. You can either begin in the local branch of your bank, explaining to the staff what you'd like to do, or head to the website of your bank and click **Register** or **Get Started** under the **internet banking** section. In both cases, you'll need to supply some details, including your account or card number. You'll also need to confirm your date of birth, full name and address.

Can I start immediately?

For first-time customers of online banking, there's typically a short wait. You may be posted some confirmation details to your home address. This letter will contain the information you need to log in for the first time. It's safer this way, ensuring that only genuine customers get to log into their own bank accounts.

How do I log in to my account?

The welcome letter you receive should explain everything you need to know. But generally, most online banks use a combination of security steps to log you in safely to your account. You may be sent a small card reader (it looks a bit like a calculator). You put your bank card into this and follow instructions on screen to receive a secure code.

It's likely you'll be sent a unique password or pass code by your bank, as well.

What can I do with online banking?

Online banking lets you check your bank balance, transfer money between your own accounts, and send money to other people instantly. There are security measures in place for all of this. For instance, if you tried to send money to someone's account and you'd never done so before, the bank would ask you to confirm some security details. Some banks will text a security code to your mobile phone, for example.

Can I bank on a tablet or smartphone?

All the main banks have apps you can install for free to a tablet or smartphone. They sometimes have additional security measures, such as fingerprint ID, if your phone supports it. You can check your balances and transfer funds via these apps with ease.

Do I need to be careful?

Some basic precautions will have you banking online safely. Never share your login information or passwords, and never keep them written down and stored somewhere obvious for others to find. When heading to your bank's website, always double-check that it's the official one. Remember, banks will never email you asking you to supply account details or update them by logging in. This is a classic ruse used by scammers.

How safe is your password?

Good passwords are essential for keeping online accounts and information secure – but is yours complex enough?

Should I use password software?

Keeping track of multiple passwords can be a pain, but there are tools that can help. Password managers, such as LastPass, create strong passwords and store them safely. They can log you into sites automatically, too.

The beauty of password managers is that they can be set to work across multiple devices. All the details are controlled by one central 'master password'. Take great care of this, because if you're locked out of LastPass, you can't change any of the passwords that it has created.

To get started, head over to **LastPass.com**, create an account and download the relevant software for your computer or mobile device. LastPass mainly works within your web browser. It will store your login details when you visit a site, then automatically input these when you return.

You can sync LastPass software across different devices. If you were to lose your phone or laptop, for example, you could use another device to change the master password, log out of all active sessions, or create new passwords.

How to create a strong password

The easiest way to create strong passwords is to base them on a single phrase as a building block. A favourite song lyric can be easy to remember.

- **Core phrase** For example, you could use **strangersinthenight** as your password's starting point, or 'core'.
- **Add numbers and symbols** Next, strengthen the core password with a mixture of upper case and lower case letters, numbers and symbols. This could give you **$trang3rs1nTheN!ght**. This is already quite secure – plus it's hummable, if you need an extra trick to remember it.
- **Adapt the password** You can reuse the core password on multiple sites with a simple variation. For example, add 'Fb' to the end to tailor this password for your Facebook login – giving you a password of **$trang3rs1nTheN!ghtFb**.

HOW SAFE?

The Kaspersky password checker suggests this password could take over 10,000 centuries to crack. That's pretty good, for a souped-up Sinatra lyric.

Codes cracked in seconds

1 second

Popular passwords used on the web – including '12345' and 'password' – may be memorable, but they're not safe. Even an average home computer could crack these codes in under a second.

12345

qwertyuio

mitchell

7 minutes

Adding some complexity – extra numbers or letters – might seem like adequate protection. But these provide mere speed bumps. Password-cracking software can figure these out in minutes.

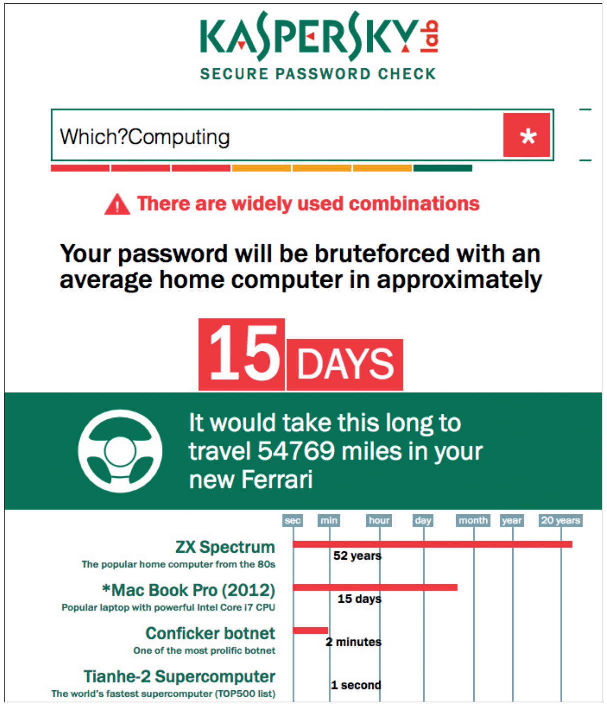
mitchell1970

tunasandwich

10,000 centuries

This is a secure and complex password, with a sufficient mix of letters, numbers and characters. An automated password hacking process would take decades or even centuries to break this type of code. Learn how we built this password in our guide to creating passwords, left.

$trang3rs1nTheN!ghtFb


KASPERSKY lab

SECURE PASSWORD CHECK

Which?Computing

There are widely used combinations

Your password will be bruteforced with an average home computer in approximately

15 DAYS

It would take this long to travel 54769 miles in your new Ferrari

sec
min
hour
day
month
year
20 years
ZX Spectrum
The popular home computer from the 80s
52 years
*Mac Book Pro (2012)
Popular laptop with powerful Intel Core i7 CPU
15 days
Conficker botnet
One of the most prolific botnet
2 minutes
Tianhe-2 Supercomputer
The world's fastest supercomputer (TOP500 list)
1 second

Test password strength for yourself at password.kaspersky.com

Security dos and don’ts

Staying secure online needn’t be a chore – common sense and the right amount of scepticism go a long way.

Do look before you leap

Most security threats require some input from you, whether it’s clicking a link in an email or viewing a funny Facebook video link that appears to be sent from a friend. By being sceptical about unexpected communications you can reduce the likelihood of infection, or of someone gaining access to your bank account or social network login. Avoid clicking links in emails even if they appear to be from a reputable company, because they can lead to phishing sites or web pages that host malware. Similarly, you can check with friends whether they really sent you an invitation that begins with: ‘You won’t believe this amazing video’.

Don’t be lazy with passwords

Always use different passwords for different websites. Otherwise, if you’re hacked just once, all of your accounts could be vulnerable. You also need to choose passwords that are hard to guess, using a mixture of letters, numbers and, ideally, symbols.

Do back up files on separate hardware

One of the nastiest threats that’s doing the rounds is ransomware, which locks your computer or encrypts files and won’t make them available again without a payment. Always keep a backup of your files on an external hard drive. This at least means that you won’t lose your files if you refuse to pay the ransom.

Don’t run two security programs

It’s easy to assume that two antivirus packages are better than one. But, in fact, they gum up your machine and fight with each other over which program should be fixing problems.

Do protect information when out and about

A laptop, tablet or smartphone contains personal information that you don’t want to fall into the wrong hands, and you can protect it with simple measures such as setting a password. Whether it’s an Android tablet, iPad or a laptop, there are options to set a password on startup or after a set period of inactivity. This can stop anyone who finds or steals your hardware from accessing your files.

Don’t treat wi-fi hotspots like your home connection

At home, you know your internet service is secure – assuming you have wireless security enabled, which you should. At free wi-fi hotspots, however, you are less secure, as hackers could lift personal data that you enter or even access files on your machine. It’s best to minimise the sensitive browsing you do at public hotspots, so try to leave banking or online shopping sessions until you are on a secured network. Make sure no-one is peering over your shoulder while you log into accounts in public places.

> *“At free wi-fi hotspots you are less secure, as hackers could lift the personal data that you enter”*

Do keep software up to date

Antivirus software is toothless if it doesn’t have the database to identify the latest threats before they arrive on your PC. Most software packages will update automatically, or after a notification, but they also often require a restart before they take effect, so don’t postpone the update installation just because it’s inconvenient.

Don’t give too much away

Social media is a great way of staying in touch with friends and family, but it’s easy to make too much information available. Set privacy settings so that only people you want can see your information, whether it’s details about a holiday or even your date of birth. In Facebook, go to **Settings** then **Privacy** and select **Friends** from the tab **Who can see your future posts?**

Do check online store security

Before you give any credit card details over the web, look for signs that the company you’re dealing with takes security seriously. Check for a padlock logo located in your web browser’s window, as well as an **https** prefix on the site’s address bar. This denotes that your information will be secure in transit.

Don’t panic if you receive a threat

Security software tends to notify it has encountered a threat, but scam versions of such warnings can be common online. They may take the form of an authentic-looking warning that you have a virus needing urgent treatment by downloading expensive software. In many cases, this can be ignored. Run a malware scan using your own security software to identify and remove any potential bugs on your system.

Jargon buster

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

■ **Add-on** An extension to a program that adds extra features. Web browsers let you install add-ons to enhance functionality, for example, an ad blocker.

■ **Anti-phishing** A technological service that helps prevent unauthorised access to secure and/or sensitive information.

■ **Antivirus** Software that scans for viruses and removes them from your computer.

■ **Backup** A copy of your files, documents or other data – often made to a separate hard drive or storage device, or using cloud storage – in case the originals are lost or damaged. See also 'Cloud storage'.

■ **Browser** The program you use to access the internet and view web pages. Popular browsers include Internet Explorer and Edge (both developed by Microsoft), Chrome (Google), Firefox (Mozilla) and Safari (Apple).

■ **Browser extension** A type of add-on that can be downloaded to add a new function to your web browser, eg an ad blocker. See also 'Add-on'.

■ **Encrypt** A way of protecting confidential data online, or when it is stored on a computer or hard drive.

■ **Firewall** A security system that blocks access to certain websites and online content that may harm your computer.

■ **Firewire** A type of computer connection, developed by Apple, for connecting accessories. It's mostly been replaced by Thunderbolt.

■ **Hard drive (or hard disk)** The main long-term storage space used by your computer to store files and programs. As well as built-in drives, you can also use external hard drives for backing up and storing data – you plug these into your computer, usually using a USB connection.

■ **Hotspot** A public place where you can log on to a wi-fi internet network with a laptop, smartphone or tablet.

■ **Mailing list** A list that holds the details of people who have signed up to receive emails, such as promotions or other advertising material, from a company.

■ **Malware** Malware or 'malicious software' is any program that is harmful to your computer, such as a virus.

■ **Phishing** A scam that tricks you into giving away personal details using a fake website or email that appears to be for an authentic service.

■ **Quarantine** Antivirus software isolates infected files on a computer's hard disk. Files put in quarantine are no longer capable of infecting their hosting system.

■ **Ransomware** A malicious program that holds your computer 'hostage', preventing you from accessing it, and asking you to make a payment.

■ **Spam** Unsolicited junk email.

■ **Spyware** Software that secretly installs on your computer and is able to track your internet behaviour and share the details.

■ **Virus** A malicious program that spreads from computer to computer via applications or documents.