

DO YOU NEED TO PAY FOR ANTIVIRUS?

For most people, the answer is no. Windows includes **Microsoft Defender**, an antivirus program that's free, switched on automatically and regularly updated. As long as Windows itself is kept up to date, it consistently achieves top marks for protection in independent tests.

COMPARING YOUR OPTIONS

1 BEST FOR MOST	Windows' built-in protection Benefits: It costs nothing, is already running and updates itself automatically. It performs very well in independent tests and rarely interrupts you or slows your computer down. Drawbacks: It relies on Windows updates being installed, and it has fewer extra features than paid packages.
2 OPTIONAL	A paid security package Benefits: Well-known providers include extras that some people find useful, such as parental controls, a VPN or identity monitoring. Drawbacks: There's a yearly cost, which often rises sharply at renewal, and more pop-ups and reminders. It offers no better protection against scams than Windows already provides.
X AVOID	Avoid running two antivirus programs at the same time, installing free "cleaner" or "speed-up" tools, and installing or buying any software because a pop-up, advert, email or unexpected caller says your computer has a problem. These often lead to a convincing checkout page, but the software is fake, and your card details go straight to the scammer.

KEEPING YOUR PROTECTION UP TO DATE

Let Windows install its updates, and restart your computer when it asks you to. Now and then, it's also worth opening **Windows Security** from the Start menu to check that each section shows a green tick. If your computer still runs Windows 10, please make sure it's still receiving security updates. If you're not sure, we can check this for you as part of one of our [health checks](#).

AWARENESS IS YOUR BEST DEFENCE

Most of the problems we see today aren't caused by viruses at all, but by deception: phone calls, emails, text messages, fake websites and pop-ups designed to persuade people to hand over money, passwords or access to their computer. No antivirus program can stop you being talked into something, but knowing the warning signs can.

POP-UP SCAMS ARE NOT VIRUSES

A typical scam message fills the screen, claims your computer is infected and urges you to call "Microsoft" on the number shown, sometimes with an alarm sounding too. Antivirus software won't usually stop these messages, because they aren't viruses. They're web pages designed to frighten you into making the call or entering card details.

What to do: don't call the number. Close your web browser, or restart your computer if it won't close, and say no to any offer to restore the previous pages. As long as you haven't called the number or installed anything, your computer is almost certainly fine.

SIMPLE RULES TO FOLLOW

- Microsoft, BT, Virgin Media, Sky, TalkTalk, other internet service providers and your bank will never call you out of the blue about your computer.
- Never allow an unsolicited caller to connect to your computer or to install anything on it.
- Never pay anyone with gift cards or vouchers. No genuine organisation will ask you to.
- Avoid clicking links in unexpected emails or text messages, however official they look.
- If in doubt, end the call and contact us, or call your bank on **159**.

IF YOU'VE BEEN CAUGHT OUT

Switch off your computer straight away and call **159**, which will put you through to your bank so it can protect your accounts. If you'd like peace of mind, we can then check your computer over and make sure it's safe to use again. You can report what happened to Report Fraud on **0300 123 2040**.