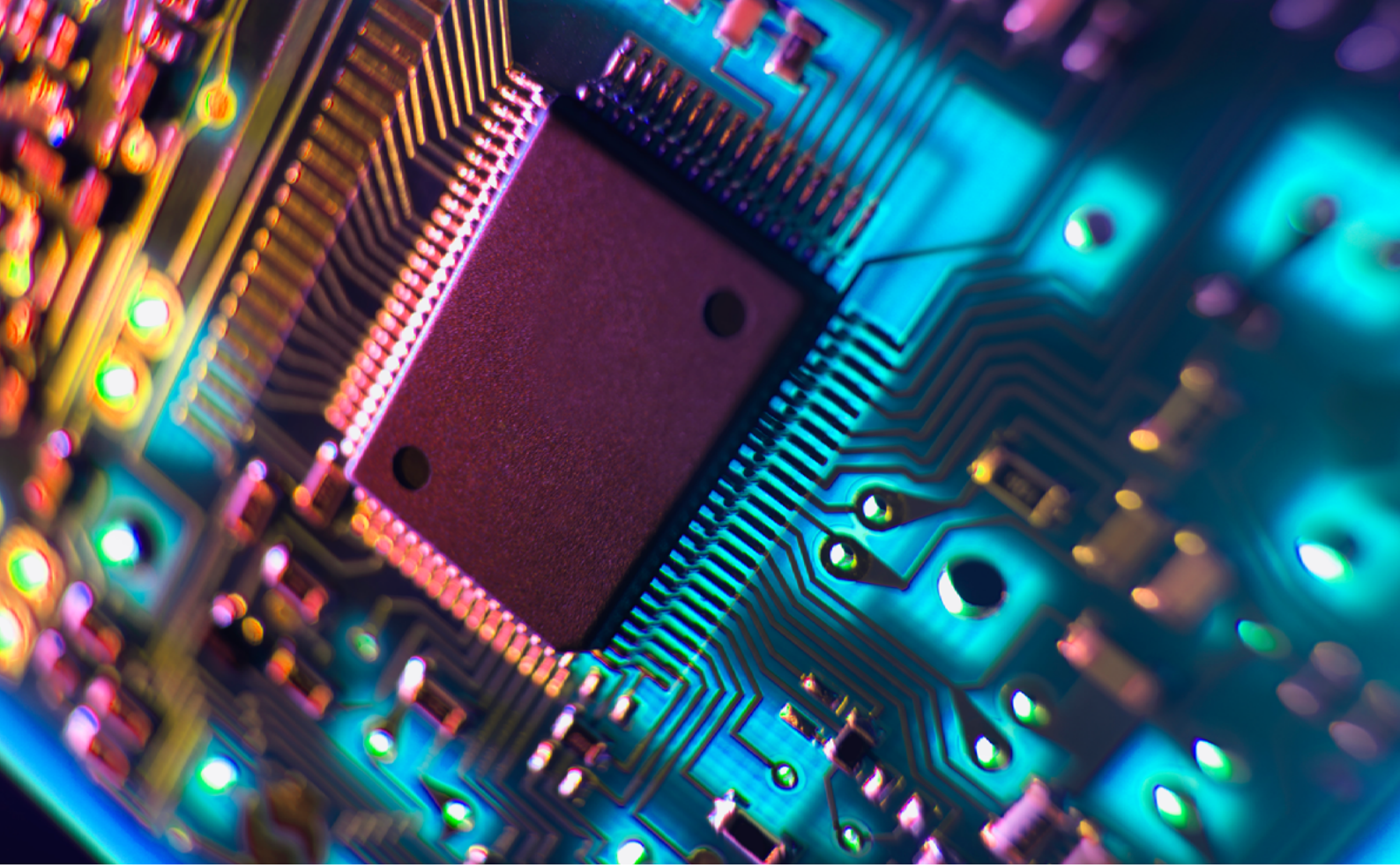


It's time to talk about cybercrime

Does everyone in your team realise they're all responsible for protecting the business against cybercrime? It's time they did...

We've all heard about the potential threat of cybercrime to businesses of all sizes and how cyber criminals are getting ever more sophisticated.

Protecting your business is the responsibility of **everyone** in the team, not just the IT department, so training staff to be cyber safe is more important than ever.

We've produced this quick guide for you to take back to your business, get people talking about cybercrime, and share some top tips on how you can stay safe together.

Visit **business.hsbc.uk/cybercrime**, or take a look at our **top cybersecurity tips overleaf.**

HSBC UK | TAKE FIVE TO STOP FRAUD

Together we thrive

Quiz: Test your cyber knowledge

Get your team to take this quick quiz to see how cyber aware they really are.

1. **How can hackers access your information?**
   a. Applications
   b. Social media
   c. Email or phone conversations
   d. All of the above

2. **What percentage of malware is delivered via email?**
   a. 30%
   b. 60%
   c. 90%
   d. 100%

3. **When you receive a suspicious message you should…**
   a. Delete it
   b. Report it to your IT manager
   c. Ignore it
   d. Click on the links

4. **In 2017, cyber attacks on organisations cost the UK:**
   a. £50m
   b. £500m
   c. £5bn
   d. £10bn

5. **What percentage of UK businesses experienced a cyber-attack in the last 12 months?**
   a. 27%
   b. 43%
   c. 51%
   d. 64%

Share these top tips with your team

Whether they're experts already or have a bit more to learn, sharing these top tips with your team could help keep your business cybersafe.

1 Never disclose security details

Be aware of unexpected solicitations asking for your full password or security details. A genuine bank or organisation will never ask you for your PIN, full password or token code in an email, on the phone or in writing. If someone rings asking for this information, don't provide it.

Instead, hang up and call the number on your account statement, in the phone book or on the company's or government department's website to check whether the call was genuine. Wait at least five minutes before making the call – this ensures the line has cleared and you're not still speaking to the fraudster or an accomplice.

2 Don't be rushed or pressured into making a decision

Under no circumstances would a genuine bank or other trusted organisation force you to make an on-the-spot transaction or transfer. Nor would they rush you while you pause to think. Slow down, and consider your actions. What are you being asked for, why is it needed, and are you sure who you're talking to?

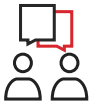
3 Listen to your instincts

If something feels wrong, question it. Criminals aim to pressure or lull you into a false sense of security while your defences are down, and they can even falsify phone numbers and pose convincingly as bank employees or trusted officials. So whether you're focusing on a project at work or relaxing at home, think carefully about the information you're giving.

4 Keep yourself up to date

No matter the size of your business, vulnerabilities could arise at any time. A simple start to protection is ensuring all of your software is current and enabled, from your standard desktop software to malware protection to firewalls and encryption.

5 Don't stay silent



Whether you've received a fraudulent email or have been targeted by phone, it's good to share your experience with others. By discussing the cause, you can work to find a solution to protect you and your business now and in the future.

For more information on tackling the threat of cybercrime, visit: **business.hsbc.uk/cybercrime** ›

Quiz answers: 1 – d; 2 – c; 3 – b; 4 – d; 5 – b

Issued by HSBC UK Bank plc.