Cyber Threats in 2022

Managing the risks to your business

When it comes to cyber security, it's more important than ever to ensure you're **getting the basics right**. Take a look at this guide for some practical tips and useful resources that can help.

AVIVA

What can you do?

Some practical guidance

The National Cyber Security Centre (NCSC) has asked organisations in the UK to bolster their online defences in the light of recent viruses and hacking against Ukrainian organisations.[1]

Any business can be a target, not just large corporate companies. In fact, 91% of UK companies asked had at least one successful email-based attack in 2021[2].

It's important to remember that hackers don't discriminate. They can send out mass emails containing links or attachments that, if opened, could introduce a virus into your computer or device. This could then lead to data loss or breaches or even a disruption to your business if systems or networks are compromised.

7 practical steps to help protect yourself and your business:

Learn to spot malicious emails:

try to avoid being a victim of an email-based attack. If in doubt about what to do, contact your IT team or call the sender to validate the email

Surf the web carefully:

hover your mouse over a link to check the link is correct and as expected because hackers will create links that look very similar to real ones

Update your computer when prompted:

don't delay implementing updates to your computers and devices as these will help you stay protected

Check for the padlock icon:

this should be in your internet browser to the left of the website name. Be on the lookout for warnings such as 'Not Secure'

Store passwords in a secure service:

don't store passwords in word documents or spreadsheets

Don't reuse passwords:

Create different passwords for different accounts e.g. email, social media and websites. Hackers will try the same passwords across different accounts

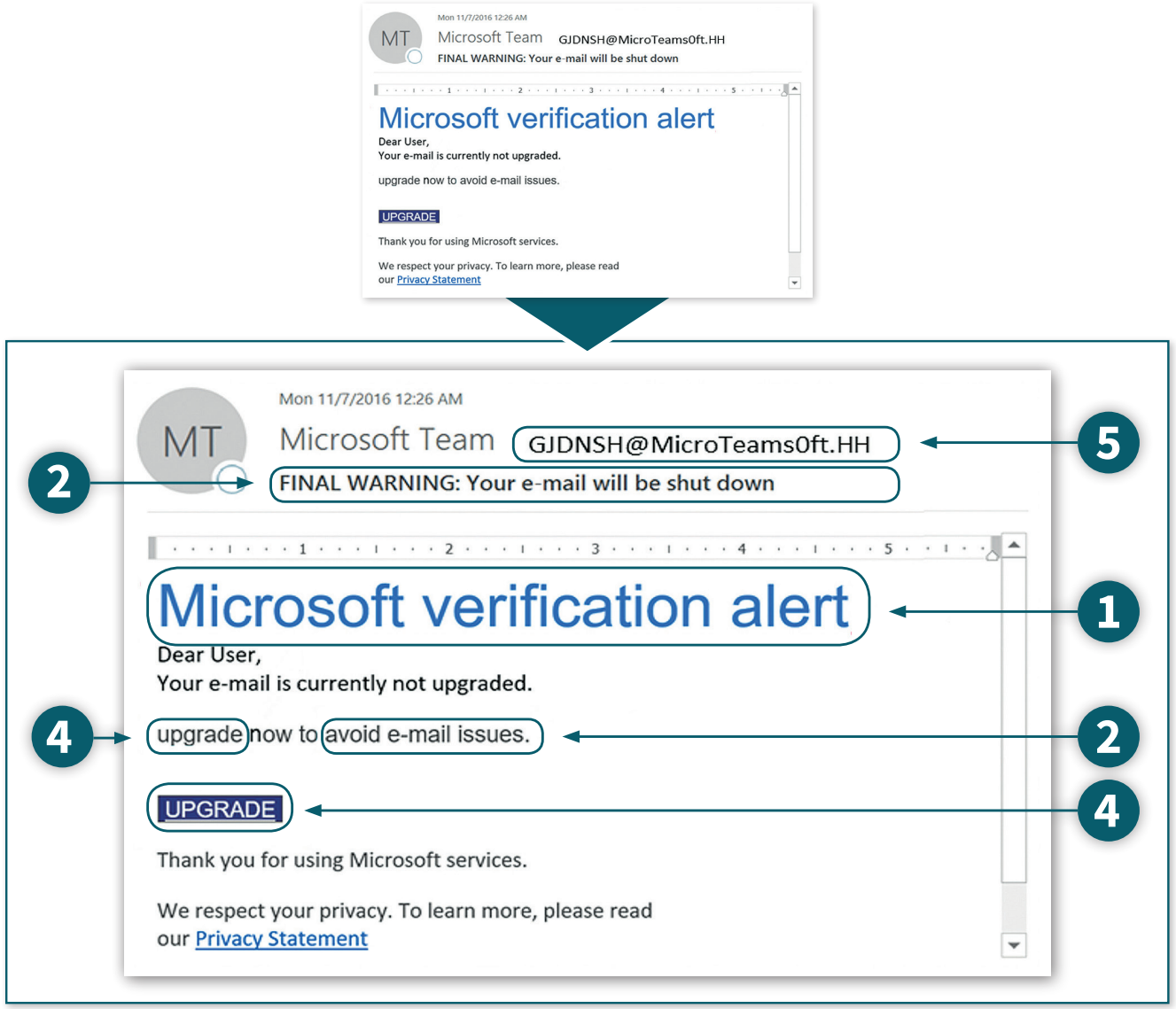
Validate unexpected calls or messages:

hackers will use the same methods as scammers to trick you into revealing sensitive information e.g. passwords or business information, sometimes by pretending to be someone you can trust

What can you do?

How to spot malicious emails

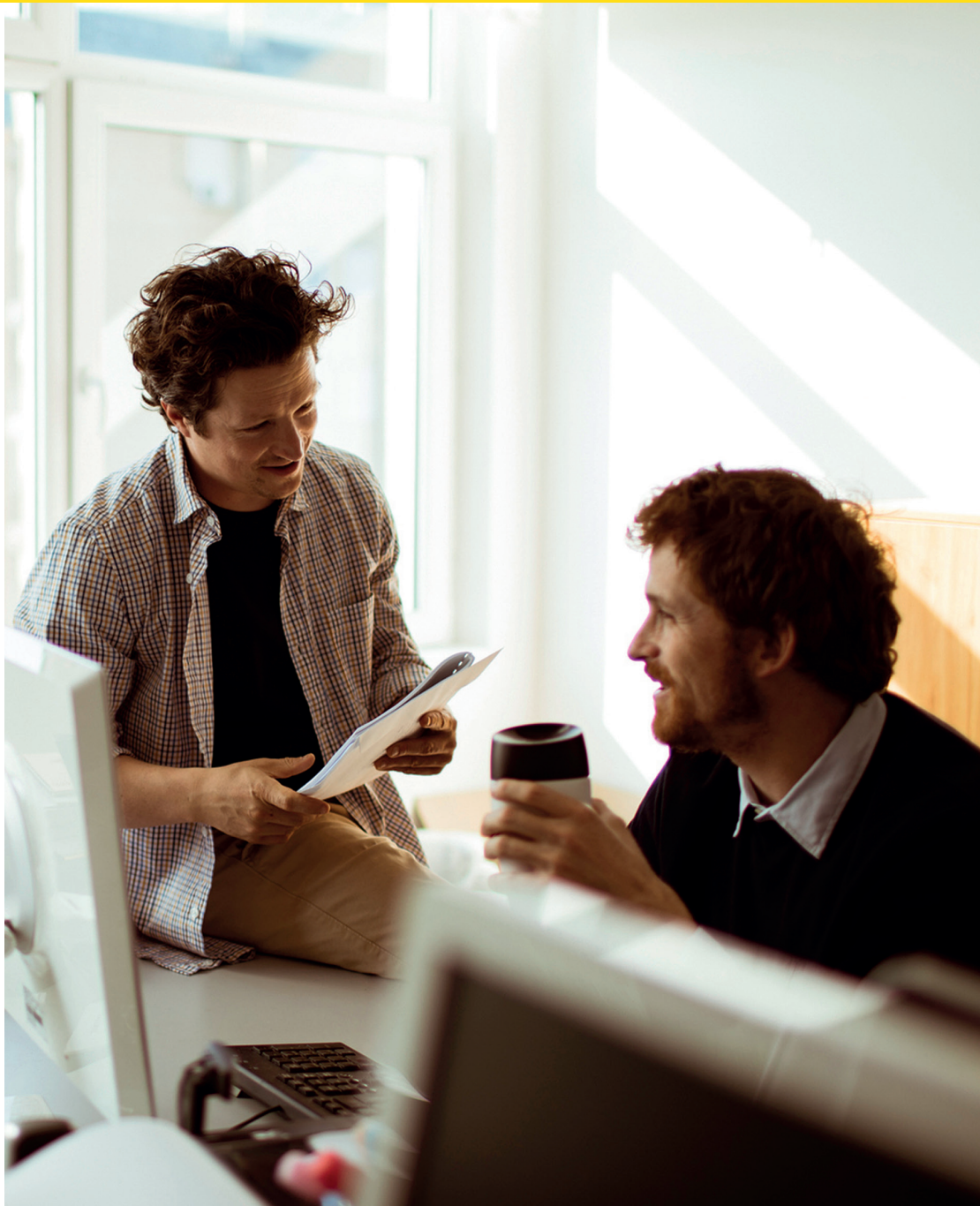
1. **Authority –** The message may claim to be from someone official with authority like a manager or your bank. This is designed to trick you into following instructions
2. **Urgency –** The message may tell you that you've got a limited time to respond, such as 'within 24 hours' or 'immediately'. Hackers will often threaten you with fines or other consequences to cloud your judgement
3. **Emotion –** Check whether the message makes you panic, fearful, hopeful or curious; hackers will try to make you respond out of emotion
4. **Scarcity –** Is the message offering something in short supply, like money or missing out on a good deal or opportunity to make you respond quickly.
5. **Unexpected –** The message could be unanticipated or posing to be from someone you know or trust but not in their usual style or email subject. Be aware of this because hackers may be in control of one of your contact's mailboxes.



What can you do?

Best practice for managing your IT

- Ensure your continuity and recovery plans are still relevant for the current heightened threat. e.g. backs-ups are secure, tested and useable
- Review how your supply chain can impact your business and the information you hold – you may need your suppliers to bolster their own cyber security
- Check your organisations security tools and software are up-to-date and working as expected e.g anti-virus, firewall and intrusion detection software
- Reassess previous risk management decisions to check they're appropriate considering the heightened cyber threat e.g. un-patched vulnerabilities, old software, and single factor authentication (password only)
- Evaluate whether the update and patching cycle could be more frequent
- Review staff security training e.g. how to report malware, phishing attacks or scams, and see whether refreshers need to be offered
- Check privileged or administrative access and remove unnecessary access e.g. unused or old accounts
- Register for the Early Warning service so NCSC can quickly inform you of any malicious activity reported regarding your organisation



If you'd like to learn more about a cyber insurance policy from Aviva, please speak to your insurance broker.

Useful links:

Actions to take when the cyber threat is heightened, NCSC

Weekly threat report, NCSC

Cyber and Data Management: Preparing your business for cyber-related risks, Aviva Risk Management Solutions

[1] NCSC advises organisations to act following Russia's attack on Ukraine, NCSC, March 2022
[2] Weekly Threat Report on Email attack statistics, NCSC, 25 Feb 2022

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

PCCRB5814 03/2022

AVIVA