Will our IT systems stop a cyberattack?

This email seems a bit odd … maybe I shouldn't click on the link

Why am I getting this request for a payment?

In a business, cybersecurity is *everybody's* business.

GET SAFE ONLINE .org

www.getsafeonline.org

Renfrewshire Council

Whatever size or type of business you own, manage or work in, it's a target for cybercriminals, desperate to steal your money, customer data, intellectual property and other vital assets. The consequences can include financial losses, reputational damage, regulatory penalties, litigation or even business failure. And inevitably, a substantial amount of recovery work and trauma.

We recommend investing in the best security you can afford, which may mean physical measures as well as data security on computers, networks and storage. But even the most robust systems can be compromised by the behaviours of colleagues, employees and, maybe, yourself. In fact, 95% of cybersecurity issues can be traced to human error, and insider threats – either intentional or accidental – account for 43% of all breaches *(source: World Economic Forum Global Risks Report 2022)*. Not only this, but the chance of cyberattacks succeeding has increased with more home and hybrid working.

What can go wrong?

Prevalent types of cybercrime affecting businesses right now include:

- Payment diversion fraud, where businesses are tricked into changing regular or one-off payments into fraudulent bank accounts. Also known as invoice fraud.
- CEO fraud, where an employee receives an email, text or phone call from someone impersonating a senior manager, instructing them to make an urgent one-off payment.
- Other types of impersonation or 'social engineering', where an employee is tricked into providing bank login details or other confidential information that could result in theft of money or data.
- Ransomware, where your computers or systems are infected by malware and files locked, accompanied by a ransom demand.

Make online security part of your business culture. Start safeguarding your business *now* by following these top tips.

- Ensure all employees receive regular, up-to-date training on protecting the business and themselves from online threats.
- Introduce acceptable usage policies including what websites may and may not be visited and what employees post or publish online about the business.
- Have a robust password policy that includes choosing, using and protecting passwords carefully, having a different one for every account, use of password managers and two-factor authentication (2FA). When creating secure passwords, you could start by using three random words and adding capital letters, numbers and symbols.
- Ensure that computers and mobile devices are physically protected from theft and loss as they generally contain – and provide access to – confidential business information. All devices should be protected with a password or passcode.
- Ensure that reputable internet security software and apps are loaded to all devices, kept updated and switched on.
- Ensure all data that the business needs to retain is backed up so that it is secure and accessible.
- Have and enforce a BYOD policy to govern employees' use of their own devices for business purposes.
- Always download updates to software, apps and operating systems when prompted, as they frequently contain vital security fixes. Better still, set them to update automatically.
- Never reveal too much personal or financial information in response to emails, phone calls or letters. Check that such requests are genuine, as senders or callers may not be who they seem and can spoof sender addresses and caller numbers.
- email attachments and links in emails, texts and posts should be treated with caution – and not clicked on – if the source is not 100% known and trustworthy. If in doubt, call the organisation or individual on the phone number you know to be correct, to check the request is genuine.

- If you or an employee receives instructions to change payee details for supplier payments or subscriptions, again, call the organisation to check.
- If your business falls victim to a ransomware attack, do not pay the ransom but seek professional assistance.
- Carefully control access to your data – both by employees/contractors and externally. Protect your customers and employees from breaches, and your business from contravening the Data Protection Act.

You should also consider gaining certification to the government's Cyber Essentials scheme. If you want to do business with the government or are in a government supply chain, you may be obliged to do this anyway.

For expert, practical, free advice on the above topics and much more, visit www.getsafeonline.org/business

To check if a website is likely to be legitimate or a scam, enter its address in our Check a website tool at www.getsafeonline.org/checkawebsite

#SafeBusiness

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on **0300 123 20 40** or at **www.actionfraud.police.uk**

In Scotland, report fraud to Police Scotland by calling **101**.

> ***"Smaller organisations took little proactive action on cyber security, driven by a lack of internal knowledge and competing priorities with their budgets. They often had a fear of the technicalities of cyber security and a preference to not research and mitigate against the risks they presented."***

DCMS Cyber Security Breaches Survey 2022

GET SAFE ONLINE .org

www.getsafeonline.org

Renfrewshire Council

OFFICIAL PARTNERS

TESCO · NatWest · Standard Life · first direct · HSBC · Royal Air Force · Army Be the Best · Royal Bank of Scotland · M&S Bank · Lloyds Bank · Halifax · Bank of Scotland · creativevirtual · City of London Police · NPCC · National Trading Standards eCrime Team · cifas · Stop Fraud · Europol EC3 European Cybercrime Centre · ActionFraud · Metropolitan Police · Ofcom · Victim Support · Neighbourhood Watch · neighbourhood ALERT · Llywodraeth Cymru Welsh Government