sure. business

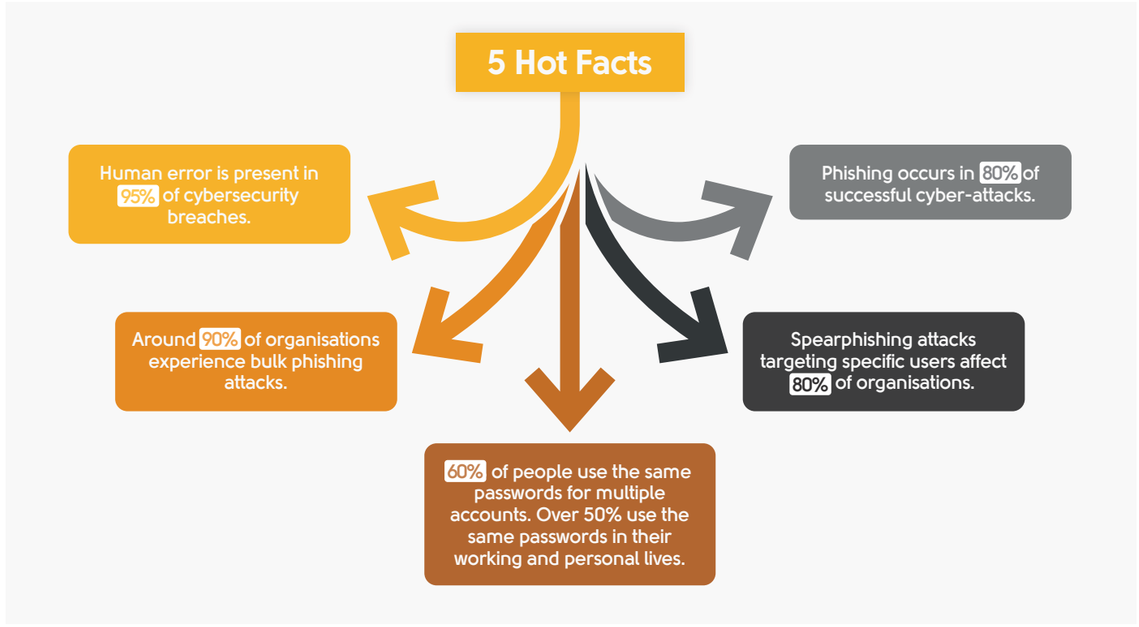
Security Best Practice

Top tips for staff

business.sure.com

Staff awareness to protect against cybercrime

With cybercrime at epidemic proportions, criminals are constantly inventing new scams and tricks to steal and extort money, we provide some behavioural context and highlight simple ways to keep this ever-growing menace to a minimum.



What is driving cyberbreaches & events?

Employee Behaviour and Security Best Practice

Best Practice Behaviours & Top Tips... the Do's and Don'ts

Phishing... Be Alert

Phishing thrives on the vulnerabilities of human nature, taking advantage of our curiosity, complacency and lack of awareness. Criminal attacks try to trick us into some of the following - all with malicious consequences:

- Divulging and providing sensitive information.
- Opening infected attachments in the email.
- Clicking on tempting links to bogus malicious websites.

Phishing attacks often target large numbers of people in the hope of striking it lucky with few targets. More focused spearphishing attacks are aimed at specific individuals, organisations, and industries where detailed knowledge has been obtained.

- Phishers can use publicly available information about you to appear genuine, and we should all review our social media information and privacy settings - and think about what we post.
- The current social and business environment is used as a backdrop for messages that appear convincing.
- Urgent and authoritative messages pressure you to act, often pretending to be from a public body, or a senior company executive – all disguised as 'normal' business communications.
- If in any doubt, always check policies and processes to spot unusual activity, and if you think you've made a personal mistake - report it immediately to minimise the potential harm.

Passwords & Identity Theft

Attackers will try to access systems using stolen or common usernames and passwords - often across multiple platforms and applications, in the hope that the login details are the same. Weak passwords and authentication help smart attackers to access systems and information.

- Create strong and memorable passwords for all account and especially the important ones, avoiding predictable options like dates, sports teams, and family or pet names.
- Create separate passwords for work and personal accounts, and use two factor authentication (2FA), if available, for important websites like banking and email. 2FA provides a way of 'double checking' that you really are the person you're claiming to be.
- And if you do write passwords down, store them away from your devices, and never use stickers on devices with login details.
- DO NOT reveal your passwords to anyone – as your IT team and application providers will always provide a secure password reset option if you forget.

Use a reputable password manager to help secure your details. Most require a strong master password and 2FA to access the store, they can also help you to create strong passwords.

Your passwords will be :

- Remembered for you
- Unique and complex
- Encrypted

Devices, USB Sticks & Removable Media

Removable storage devices, like USB memory sticks, are ways for malware to access systems through auto-run features. Just like dangerous attachments and bogus weblinks, criminals load disguised malware onto such devices.

- A tactic is to randomly place USB devices and removable media around an organisation in the hope that curious employees check them out, and unknowingly facilitate an attack.
- Software upgrades are released for a reason, so please don't ignore them as they contain updates to keep your devices secure.
- Always lock or set up auto-lock on devices when not in use, and use PIN numbers, passwords and or fingerprint/face recognition. This will make it harder for an attacker to exploit a device if it's left unlocked, lost or stolen.
- Ensure you only download apps from official app stores (like Google Play or the Apple App Store), as this provides protection from viruses – DO NOT download apps from unofficial or unknown vendors and sources.

If in doubt – Shout!

If something doesn't look or feel right - it probably isn't, so please PLEASE report it. If it turns out to be a false alarm, that's absolutely fine. Immediately reporting incidents or anything suspicious to your IT department or line manager is welcomed, and it could significantly reduce the impact of any cyber incident.

- Cybercriminals are clever, so if you have an inkling that something isn't right, raise the alarm ... you'll be helping everyone and everything in your organisation.
- Report the issue as soon as possible - don't assume someone else will have done it. And if you've clicked on a worrying link yourself, or think you've made a mistake, please report it so it can be checked out as soon as possible.
- And please raise or challenge any policies or processes that you feel are either wrong or unnecessary. Clunky security procedures get in the way of work, are probably ineffective, and in need of improvement.