



Staying Safe Online at Work:

Cyber Hygiene Essentials for Staff

Intro.

Cyber Hygiene Essentials for Staff

In the wake of recent high-profile cyber-attacks on UK companies, it's more important than ever for all staff to practise good cyber hygiene.

Major retailers like M&S, the Co-op, and Harrods have suffered serious disruptions, forcing systems offline and costing millions in lost business.

The good news is that many attacks can be prevented by simple, everyday security habits. This friendly guide summarises key best practices – **no technical jargon, just practical steps to help keep you and your company safe.**

Contents

- Password Hygiene
- Phishing & Email Safety
- Incident Reporting
- Mobile Devices
- Remote Work Practices
- Need Support?

“We’re here to help everyone stay safe, wherever they’re working from – follow the basics and let us know if you’re ever unsure”

Mark Williams, Head of Client Relations, b2b IT services

Password Hygiene.

Strong And Secure Logins

- Use strong, unique passwords for your work accounts. Many sites require a mix of uppercase, lowercase, numbers and special characters, but even then, length and unpredictability matter.

Combine three or more random words to create a memorable but strong password like: blue-piano-cheese-92!

- Never reuse your work password on any other website or account. If an external site is breached, you don't want attackers to also have your work login.
- Enable multi-factor authentication (MFA) on your accounts (such as Microsoft 365/Outlook) whenever possible. MFA adds a second step (like a code from your phone) to verify it's really you.
- Keep passwords private. Never share your passwords with anyone – even IT staff. Legitimate support will never ask for your password.

Password & Security Tips

✓ Choose a passphrase like "blue-piano-cheese-92!" - it's long, hard to guess, and (nearly!) easy to remember.

🔒 Use a password manager if you find it hard to remember everything.

🔑 The "USB Test": If you find a USB stick in the car park, don't plug it in! Just like your passwords, never trust something you pick up from outside.

🧠 Attitude: Think of passwords like toothbrushes - don't share them, don't reuse them, and change them regularly.

Phishing and Email Safety.

Think Before You Click

- Be vigilant with emails and messages. Scammers often send phishing emails that look genuine but are designed to trick you into clicking a malicious link or giving up information.
- Check the sender and content for signs of a scam. Look out for slight misspellings, strange tone or grammar, and urgent language designed to panic you.
- Know your organisation's typical procedures. If an email doesn't follow the standard process (e.g. a payment request without usual checks), be suspicious.
- Guard your personal information online. Limit what you share on social media that could be used to craft convincing phishing attacks.
- **When in doubt, verify or report.** Contact the sender via another method (e.g. a phone call) or forward the email to your IT team. If you use Outlook, use the "Report Phishing" button if available.

Phishing Awareness Tips

📧 Examples of phishing: fake invoice emails, "your password is expiring" messages, or unexpected DocuSign requests.

🎧 Heard a voicemail from the MD asking you to urgently pay an invoice? Could be a deep-fake scam. Always verify.

💬 Attitude: Be politely paranoid. If something feels off, it probably is. Better to double-check than regret.

Incident Reporting.

Speak Up About Suspicious Activity

- Report issues immediately if you think you may have clicked a bad link, shared info you shouldn't have, or noticed something suspicious.

Don't wait – early reporting can stop problems from escalating.

- **No blame, no panic – we're all human.**
Mistakes happen. What matters most is reporting it quickly.
- Know how to report. Save your IT support contact details so you can act fast. If your device is behaving oddly or you've lost a device, let IT know straight away.
- Ask if you're unsure. If something doesn't feel right, get a second opinion. It's always better to double-check.

Incident Reporting Tips

🕒 Quick guide: If you click something dodgy, tell IT. If you're unsure, tell IT. If your device acts weird, tell IT.

📄 A flowchart on the wall or intranet is useful:

Clicked a suspicious link? ->
Yes -> Contact IT.

Lost phone? -> Yes -> Contact IT.

💡 Attitude: It's not about blame, it's about teamwork. One quick email could protect the entire company.

"It's always easier to fix a problem when we know about it early. Don't worry about raising a false alarm – we'd rather you ask than stay silent."


Sebastian Needs, Solutions Delivery Manager, b2b IT services


Mobile Device Security.


Protect Your Smartphone and Tablet


- Treat your phone like a work computer. Phones often carry work email and contacts, so keep them secure.
- Use a strong PIN or password and enable fingerprint or face ID where possible. Set your device to auto-lock.
- Only install trusted apps. Stick to official app stores and be cautious with app permissions.
- Watch for phishing on mobile too. Scam texts and dodgy links can appear in SMS, WhatsApp or other apps.
- If your phone or tablet is lost or stolen, report it to IT immediately.

Mobile Security Tips

 Set a 6-digit PIN or longer password – avoid birthdays or "123456".

 Download apps only from the Google Play or Apple App Store.

 At trade shows or client sites? Avoid public Wi-Fi or use your mobile hotspot.


 Attitude: Your phone is a mini-office – treat it with the same care you would your desk PC.


Remote Work Practices.


Stay Secure Outside The Office


- Use approved secure access methods when working remotely – such as VPN or remote desktop.
- Keep your home Wi-Fi password protected and up to date. Never leave your home network open.
- Be cautious on public Wi-Fi. If you need to work in a public space, use a VPN or your mobile hotspot.
- Don't work on confidential files in public areas where others can see your screen or access your devices.
- Stick to company-approved tools and cloud storage. Avoid emailing documents to your personal address.

Remote Work Tips

 Secure your home Wi-Fi with a strong password – no more "admin123".

 Working in a café? Keep your screen private and documents closed when not in use.

 Only use approved cloud tools – no more emailing files to yourself.

 Attitude: Security doesn't stop at the office door – it travels with you.

Need Support?

Or if Something Doesn't Feel Right

📞 Call your internal IT support or the b2b IT services helpdesk straight away.

✉️ Forward suspicious emails to your designated phishing/reporting email address.

💬 Unsure what to do? Ask a manager or tech lead – it's always OK to check.

🙋 We're a no-blame culture – the sooner you speak up, the quicker we can help.

"Don't be afraid to report something – you're not getting anyone in trouble. You're helping us all stay safe."

Lauren Martin, Service Desk Manager, b2b IT services

Essential Contact Details.

Support Line: 029 2076 2337

Support Email: support@b2bitservices.co.uk

Senior Team: slt@b2bitservices.co.uk