SYSTEM FORCE IT · CYBER SAFETY

New User Cyber Safety Pack

A practical guide to staying safe at work

Phishing | Passwords | MFA | Devices | Social Engineering | Reporting

v1.0 – August 2026

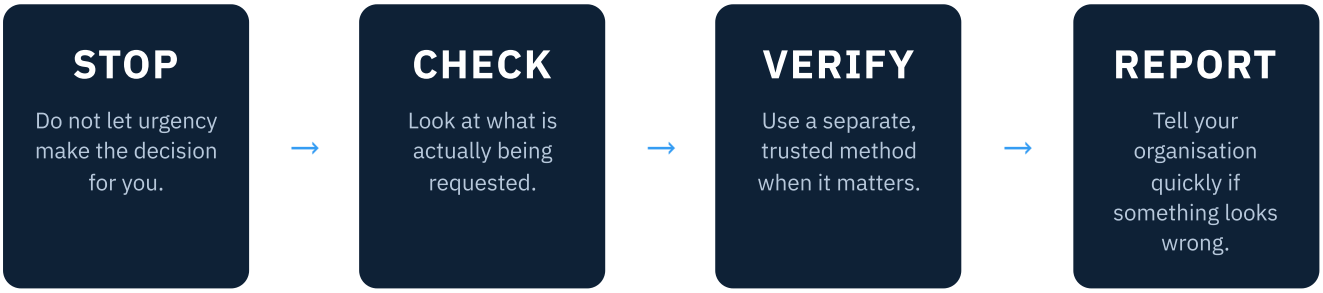
For employees and new starters

Cyber security is everyone's job

You do not need to be a cyber security expert to make a big difference.

Most of the important decisions happen in ordinary working moments: opening an email, approving a sign-in prompt, downloading a file, responding to a payment request, or deciding whether something feels unusual.

This guide gives you a few simple habits that will help protect you and your organisation. No technical knowledge is required, and nobody expects you to get everything right on your own. When in doubt, ask.



Keep these four words in mind and you will already be ahead of most online scams. The rest of this guide simply explains what each one means in practice.

Phishing does not always look like phishing

Phishing is any message designed to trick you into doing something that helps an attacker, usually giving away a password, approving a login, opening a file, or making a payment. It no longer arrives only by email. Today it can reach you through:

- Email
- Microsoft Teams
- Text message (SMS)
- WhatsApp
- Social media
- QR codes
- Phone calls
- Fake login pages

Artificial intelligence has made these messages far more convincing. Modern phishing may use perfect spelling, know your name and job role, refer to real suppliers or colleagues, imitate normal business language, and even mimic a familiar voice or create realistic images.

Look at the request, not just the spelling

Bad spelling is no longer a reliable warning sign. Instead, pay attention to what you are actually being asked to do. Be cautious of:

Unexpected sign-in request | **Urgency** | **Secrecy** | **Changed bank details** | **Request for an MFA code**

Unexpected attachment | **Unusual payment** | **"Bypass the usual procedure"**

The simple test: was I expecting this, does the request make sense, and is someone creating unnecessary urgency? If any answer gives you pause, slow down and check.

Trust, but verify

A familiar name, email address, phone number, or even a voice is no longer proof of who you are dealing with. Consider:

- A message can display a familiar name while coming from somewhere else.
- A genuine email account can be compromised and used to message you.
- Caller ID can be spoofed to show a trusted number.
- A voice can be cloned from a few seconds of audio.

So for anything unusual, sensitive, or financially important, verify it using a separate method you already trust: call the person on their known number, speak to them in person, use your company directory, or ask your manager or IT team.

A common scam: your Managing Director emails asking for an urgent bank transfer to a new account.
Do not use the phone number supplied in that email. Use the number already in your company directory, or speak to them directly, before doing anything.

Urgency does not override company procedure. Genuine, important requests can wait the two minutes it takes to check.

Protect your account

Your work account is part of your organisation's security. A few habits keep it strong:

- Use a strong, unique work password or passphrase.
- Never reuse your work password on personal websites.
- Use your organisation's approved password manager where one is provided.
- Use multi-factor authentication (MFA) wherever it is available.
- Never tell anyone an MFA code, and never share your password with a colleague.
- Never approve an MFA prompt you did not start yourself.
- Contact IT if you receive unexpected authentication prompts.

An unexpected MFA prompt can mean someone already has your password. Reject it, then report it. Do not approve repeated prompts just to make them stop.

A note on your IT team

A genuine IT team should not need to ask you for your password to help you. If someone does, treat it as suspicious and verify who they are through a trusted route.

Protect the device too

A secure account is only part of the picture. The device you work on matters as well.

- Lock your screen whenever you step away from your device.
- If your organisation manages updates centrally, allow the update or restart when your IT team asks you to.
- Only install approved software, and do not add unapproved browser extensions.
- Avoid plugging in unknown USB devices.
- Be mindful of who can see your screen in public.
- Keep laptops, phones and tablets physically secure, especially when travelling.
- Do not disable endpoint or security software running on your device.
- Report a lost or stolen work device immediately.

Managed devices help you. If your equipment is looked after by System Force IT or your own IT team, much of this happens automatically in the background. Your part is simply to allow the updates and restarts when prompted.

Think before you share

Handling information carefully is a big part of everyday security.

- Check the recipients before sending anything sensitive, and watch out for autocomplete choosing the wrong person.
- Use your organisation's approved storage, not personal Dropbox, Google Drive or similar.
- Do not email business information to your personal accounts.
- Treat confidential information carefully and only share it with people who genuinely need it.
- Follow your organisation's policy for AI tools and other online services.

On AI tools: do not paste confidential, personal, client or commercially sensitive information into public AI services unless your organisation has explicitly approved that use. Once it is submitted, you may not be able to get it back.

Clicked something? Tell someone.

Mistakes happen. What matters next is speed.

Report it straight away if you:

- Click a suspicious link
- Open a suspicious attachment
- Enter your password into a page you now distrust
- Approve an unexpected MFA prompt
- Send information to the wrong person
- Lose a device
- Respond to a suspected scam
- Notice unusual account activity

What to do

1. Stop what you are doing.
2. Do not delete anything unless IT tells you to, it may be useful evidence.
3. Contact your IT team or helpdesk immediately.
4. Explain exactly what happened.
5. Follow their instructions.

Reporting quickly gives your IT team the best chance of protecting you and the organisation. Do not wait until tomorrow to see what happens, and never try to hide it. Fast, honest reporting is exactly what a good organisation wants.

Your 60-second cyber safety checklist

Before you click, reply, sign in or pay, run through these:

- ✓ Was I expecting this?
- ✓ Does the request make sense?
- ✓ Is someone creating unnecessary urgency?
- ✓ Am I being asked to sign in or share a code?
- ✓ Am I being asked to change bank details?
- ✓ Am I being asked to bypass a normal procedure?
- ✓ Should I verify this another way first?

STOP → **CHECK** → **VERIFY** → **REPORT**

Read this online

Scan the code for the latest version of this guide, the free NCSC staff training and more free System Force resources.

systemforce.co.uk/resources/new-user-cyber-safety/

Keep learning

A short refresher every so often is far more effective than a single session. These free resources are a good next step.

NCSC Top Tips for Staff

Free official staff cyber awareness training from the National Cyber Security Centre. It takes under 30 minutes, needs no account, and includes a short quiz.

System Force: Safer Internet for Business

Our guide to phishing, social engineering, MFA, password hygiene and reducing human error.
systemforce.co.uk/resources/safer-internet-for-business-february-2026/

System Force: AI Scams, Deepfakes and Smarter Phishing

Why modern scams are harder to spot, and why good spelling no longer proves a message is genuine.
systemforce.co.uk/blog/2026/08/04/ai-scams-deepfakes-voice-clones-and-smarter-phishing/

System Force: The M&S Attack and Social Engineering

A real-world example of how a convincing phone call can lead to a major incident, and why identity verification matters.
systemforce.co.uk/blog/2026/07/29/marks-spencer-cyber-attack-social-engineering-lessons-uk-sme/

This guide provides general cyber security awareness information. It is informed by recognised UK cyber security guidance, including guidance from the National Cyber Security Centre. Organisations should supplement it with their own policies, procedures, reporting routes and role-specific training. The NCSC training is provided by the National Cyber Security Centre and is not a System Force IT product.