mtechsystems

A Guide for Security Awareness

5 STEPS TO KEEP YOUR INFORMATION SECURE

1 Physical and Digital Safety

Keep Your Devices Safe

When taking any electronic devices out of the office, take stringent measures to ensure these don't fall victim to theft.

Don't leave devices in unattended vehicles. If they do have to be left, hide them.

You'll usually be required to take company issued portable devices off site at the end of the day. This ensures disaster recovery and business continuity plans can be implemented in case of loss of access to the building(s).

All devices should be protected by a PIN or password at start-up and unlocking.

Lost Devices

If you lose a device, inform your IT department immediately. They can work with you to protect both yours and the company's information.

Restrict Building Access

If your office has door entry policy, honour this and politely query the intentions of any unaccompanied visitors.

Take care to not let unknown persons slip through coded doors behind you.

Inform security immediately if you lose your entry badge or key fob.

2 Access Information Securely

Passwords

Passwords are the first defence in protecting your information. Common passwords like "123456" or `Password1", along with your favourite pet's name or your son's birthday are surprisingly easy for an attacker to figure out with a little prying.

- **Create a strong password:** Make it suitably lengthy, with a mix of upper and lowercase, numbers and punctuation. Try joining together some unconnected words, you won't remember random characters, e.g. *Swim4unIcorn!puppet*

If you think your password has been compromised, ***change it immediately***. It's not advisable to use the same password for multiple accounts, but if you have, change it on all affected accounts.

Passwords Are Like Underwear
Don't leave them lying around
Change them regularly
Don't share them with anyone

Public WiFi

Public WiFi connections are not all secure. When working on sensitive information, ensure you're using a secure connection or a VPN (virtual private network).

3 Protect Yourself from Attacks

Social Media

No matter how locked down your privacy settings are, you can never be too sure who is really seeing the personal information you post online. The more detail you share the easier it is for a criminal to infiltrate your life.

Software Downloads

Unauthorised software could cause malware to infiltrate the company network. Always get permission for new apps or fonts.

Phishing

Treat any unexpected emails with suspicion – particularly those with file attachments or links. Hover over any links to see if the web address looks legitimate or related to the email content.

Always check the email "from" address matches the person or company you expect it to. Look out for misspellings and numbers used in place of letters.

If there's an unusual urgency or phrasing from a colleague, check with the sender in person if their request is genuine.

Phishing isn't just limited to email. Callers can impersonate a business to phish for details, then use that information to either trick a real customer or exploit the information gathered.

4 Maintain a Secure Working Environment

How secure is your office?

The 'office' is a more fluid working environment than it used to be. For some, it will be the kitchen table, for others the local coffee shop and for many the typical open plan working space.

Regardless of the environment you're in, you'll need to stay vigilant about protecting your company information.

- **Lock Devices:** Log off or lock your screen on all devices when leaving your working space. From the curious 3 year old, to the disgruntled colleague, an open device invites prying fingers and deleted files, or worse.
- **Clear Desk:** When leaving your desk for any length of time, file and lock away all important paperwork on display, shred any company sensitive handwritten notes and don't leave post-it notes of passwords lying around.
- **Mobile Devices:** If you leave your working space, secure or take your portable devices with you.

Working in a Shared Space

Be extra vigilant of the information you expose if you work from a co-working space. This includes phone conversations.

5 Store Information Securely

File Storage

Your company will likely provide you with a secure, cloud-based storage facility for your data. Saving documents on your desktop or in local folders circumvents the security and backup provisions set up by the business.

If you're unsure where you should be securely saving your files, check with your IT department or line manager.

Don't store company related data on public cloud storage platforms (Dropbox, Google Drive, iCloud), without prior permission.

About M-Tech

M-Tech Systems offer ongoing IT support services and technology solutions for businesses and educational establishments of all shapes and sizes across the UK.

M-Tech will work with you however you need; stepping in for one off projects, working together on your IT strategy, supporting your day to day operations.

IT Services. IT Solutions. IT Support

t: 01323 404040 **e:** info@mtechsystems.co.uk

www.mtechsystems.co.uk