Personal Cyber Security

Aim of this Guide

The objectives of this guide are to give you a quick overview of what cyber security is, why it's important, and the basic steps you can take to keep yourself, your connections and the organisations you work for safe from common threats.

Intro

What is Cyber Security?

In layman's terms, cyber security is simply the measures put in place to protect your digital life. There are two key aspects of a good cyber security approach:

- **The technical side:** ensuring that your digital life is secure and not easy for a hacker to exploit
- **The human side:** knowing how to spot, and how to deal with, a data breach or hack

Why does Cyber Security matter so much?

It matters because of the sheer volume of data on you and your activity which is collected and stored digitally. All this data may seem trivial and uninteresting, but it holds a high value, and in the wrong hands a lot of damage can be done.

The Bigger Picture

Although individuals are targets, more often than not criminals have their sights set on bigger things; usually exploiting the company or organisations you work for or are associated with. The weak point in any organisation is nearly always the people.

Bottom Line Up Front

- A worryingly high proportion of individuals and organisations have been, or will be, hacked.
- The weak point in any computing system are the people - i.e. you. This often puts your contacts, the organisation you work and yourself for at risk.
- A few very simple steps can make you significantly less vulnerable.
- Sometimes there is a trade off between security and convenience. It's beneficial to understand the risks in order to get the balance right.

Passwords

It is important to understand the best practice when setting passwords since most of your online logins (email, social media, finance, work accounts etc.) can be easily compromised by a hacker if these steps aren't followed. Consider using passphrases, which are made up of several words, or seemingly random characters.

Checklist

- Use a different passphrase for each account
- Ensure that each passphrase is strong (ideally 12+ characters, including numbers, symbols, upper and lowercase letters, but not dictionary words, names or places)
- Change all important passwords at least once a year

A password manager such as LastPass (or DashLine, OnePass, KeePass) will make applying these points significantly easier. It will securely store, and auto fill, each of your passwords, so that you don't have to remember them all.

2 Factor Auth

2 Factor authentication is a method of logging into your secure accounts on different computers/ devices in which you provide both something you know (a password), and something you have (a 6-digit number generated on your smartphone).

Checklist

- ○ Enable 2-Factor-Authentication on any online account that allows it. Most sites (such as email, social media, finance etc.) will almost certainly have the option of setting up 2FA

Authy, Google Authenticator, Microsoft Authenticator and LastPass Authenticator are all good choices. They're easy to set up, hassle-free to use and significantly increase the security of your accounts.

Firmware Updates

You'll probably be familiar with notifications prompting you about a new update for Windows, OS X, Android, your iPhone, your anti-virus, your router and individual software applications. These updates usually contain patches and fixes for recently discovered security vulnerabilities. If ignored, you are leaving devices and yourself open to being exploited by hackers.

Checklist

- Always install the latest operating system (Windows, OSX, Android and iOS) updates, when prompted to. Don't ignore or postpone them.
- Keep all apps and software on both your PC and phone up to date
- Ensure your antivirus definitions are kept up-to-date, or turn on auto-update.
- Remember to update your router firmware.

As well as vital security patches, updates often also include bug fixes, efficiency and speed upgrades as well as new features.

Social Media

Social media hacks are some of the most common, so it is important to stay vigilant. Social media hacks often put not only yourself at risk, but also the organisations you work for, so it's a good idea to not disclose any work details on your profile.

Checklist

- Check your privacy settings. Very carefully, and reasonably regularly
- Don't put too much trust in privacy settings. There's often a way for people to get round them. Instead, for everything you post, think *"would I mind if this ever became public?"*
- Don't give away too many personal details. It can leave you vulnerable to social engineering
- Watch out for third-party apps and integrations. Only connect apps from reputable publishers to your social accounts, and don't give them permissions or data access that they don't need. Unlink apps that you are no longer using
- Monitor accounts for suspicious activity, such as logins that you don't recognise, changes in settings, or general activity that wasn't you.
- Watch out for impostor accounts

Change your password immediately if there is any activity that you don't recognise and report anything suspicious. A good approach, is to think of everything you post or upload as potentially public, even once you've tightened your privacy settings.

Encryption

Preventing security breaches is important, but equally so is reducing the amount of data that is available in the case of such an incident. This can be done through encryption, where sensitive data can only be accessed by someone who knows the device passphrase or code.

Checklist

- Encrypt your devices. Windows has BitLocker, and OS X comes with FileVault installed. Alternatively VeraCrypt is a free, fast and secure cross-platform encryption utility
- If you store either personal, or work related data on a USB stick, or external hard drive, set up encryption with VeraCrypt
- Backup all media and data that you wouldn't want to lose.

If your phone or computer is not encrypted then all data stored on it can be readily available to a hacker, even if you have a strong password. Equally, if you don't make regular backups of important data, and anything happens to the original copy (such as ransomware, data corruption or just losing or breaking a device), there may be no way of recovering it. Either with a cloud backup solution, (such as Dropbox, iCloud, or OneDrive), or locally with an external hard drive, USB pen, or NAS.

Safe Browsing

You probably use the internet on a daily basis; for emails, shopping, news, social media or work. But what you may not realise it that without following a couple of simple guidelines you are exposing yourself up to many common breaches of security while you're sending or receiving data from web pages.

Checklist

- Find a reputable VPN provider to use on any public, shared or potentially insecure networks.
- Avoid entering data on any site that isn't secured via HTTPS, or use a browser extension such as HTTPS Anywhere
- Install Privacy Badger to block spying ads and invisible trackers
- Be wary when installing new browser extensions, as there are malicious ones out there, and they can access everything you do on your browser
- When using the internet on either a public device, or someone else computer, use Incognito or private browsing mode, so that cookies, browsing history and your passwords don't get stored
- You could consider using a safer browser, such as Brave, Epic or Comodo Dragon. These browsers will disallow trackers, fingerprinting, cryptomining, ultrasound signalling and more

Always remember, that everything you do online is being tracked and monitored, so don't overshare, don't trust websites that may not be reputable, and keep an eye on your cookies.

Smart Phones

Smartphones accumulate a large amount of personal information on you. From the obvious things like photos, calendar entries and notes but equally things like contacts, call and message logs, and location data. All of this can be used to build up a detailed picture of you, the people you know, and your habits. For this reason it's essential to take basic measures to protect this data from getting into the wrong hands.

Checklist

- Encrypt your phone. Both Android and iOS have this feature built in, and it can be enabled it from the settings menu
- Have a passphrase or PIN over 6 digits to access your phone
- Don't grant apps permissions that they don't need
- Turn of connectivity features that aren't currently being used
- Enable find my phone, for iPhone or Android. If it gets stolen, you can remotely erase the data

The data collected by your phone, holds enormous value to advertisers, hackers, scammers and sometimes even stalkers. That's why it is important to keep an eye on what's being collected and which apps have permission to access it. Ensure you know how to remotely erase your phone, in case gets stolen.

Think before you Click

Scams target everyone are getting increasingly more sophisticated and they can target anyone. Often they succeed because they appear to be legitimate, but the effects can be detrimental. They may be after money, personal details or attempting to get access to something related to the organisation you work for. It's important to know how to protect yourself from falling victim.

Checklist

- Don't plug unknown USB flash drives into your computer
- Double check who an email is from, before replying or clicking any links
- Don't open attachments from unknown senders
- Check that a domain you are entering secure information is HTTPS, and that it is defiantly correct