Digital Security

The protection of digital devices, systems and information.

According to the UK Government Department of Business Innovation and Skills survey, inadvertent human error was the cause of 50% of the worst security breaches in 2015.

IT security is 10% technology and 90% people and processes – we are all responsible. To guide you in your personal quest for digital security, we have compiled a list of best practices and tips for your apps, passwords, devices, personal information and money.

Your apps

Configure individual app permissions

Most apps offer privacy settings for users, enabling you to determine what types of information and how much of it you share and store. Always choose the least amount of data sharing possible.

Check push notifications

If you are using applications that use push notifications, review your settings to ensure that sensitive data isn’t shared unexpectedly on your home screen. You don’t want your health or banking data in full view.

Don’t over-share

Sharing too much personal information on your social media apps can be dangerous. For instance, many hackers have successfully guessed passwords through trial-and-error, using combinations of common information (such as children’s names, addresses, and other details) easily found on social media profiles.

Two-step verification/authentication

Many sites and apps now offer members the ability to turn on two-step verification for their email, banking and social media accounts. This requires a password, as well as verification of a numeric code sent to your phone via SMS. This ensures that even if your password is compromised, your accounts cannot be accessed unless the hacker also has your phone.

Your passwords

Never write them down or share them

It is tempting to write your password on a post-it, or in a notebook, but this is on a par with keeping your house key sellotaped to your front door – there is no easier way for your data to be stolen.

Use multiple passwords

It is a good idea to have different passwords for different sites, or at least have a special password for your most sensitive information. This way, if a hacker cracks your password on one website, they won’t have instantly cracked your password for a dozen more.
Use password managers

Many people find it impossible to remember all the different passwords they use on a daily basis, so they use a password manager such as LastPass and Sticky Password. Password managers can generate strong passwords for all your accounts, with no need for you to remember any of them.

Your devices

Encrypt your data

Encryption used to be the sole province of IT programmers and mathematicians, but a lot has changed in recent years. It is a highly effective method of protecting data stored on portable devices, encoding data so that it can only be read by someone who has the right encryption key (password) to decode it. You could use Bitlocker for a Windows device or Concealer for Mac. On an Android, encrypt your phone within the Security section of the Settings menu. On iOS devices, set a passcode and custom alphanumeric code in the Settings menu to enable encryption.

Backup your data

Often overlooked, one of the most basic data protection tips is backing up your data. This creates a duplicate copy of your data so that if your device is lost, stolen, or compromised, you don’t also lose your important files. Backup your University work on your personal network filespace – the H: drive. You might also consider using an external hard drive or Cloud storage.

Install Updates

Although system updates can be a pain, always popping up when you’re at your busiest, failing to install them leaves your computer at risk. Programmers build these updates to bolster security and fight off known attackers by installing critical security patches.

Secure your wireless network

By setting a password for your wireless network you prevent unauthorised individuals within the area hacking into your network.

Log out of accounts and turn off your computer

Leaving computers on and connected to the internet leaves your device open to attacks from malware and cyber crimes. It’s also a good idea to log out of online accounts when you are finished.

Cover your webcam

Some sophisticated hackers can hijack your webcam and use it to collect keystrokes and other details about your life. Even Mark Zuckerberg tapes over his webcam for security – you might want to do the same.

Be selfie aware

Worryingly, hackers have also managed to recreate fingerprints from images where the subject is holding their hand up in a peace sign.

---

Disable Bluetooth
Most threats exploiting Bluetooth connectivity are dependent on the active Bluetooth connection, and while they aren’t typically devastating or dangerous, they’re certainly inconvenient and can be serious.

Set automatic lock
It’s a good idea to set up your devices to lock automatically after a specified period of inactivity, prompting you to re-enter your password or pin code when you want to use it — just in case your phone or tablet falls into the wrong hands.

Our in-house, IT Security Officer, said
“If you want to use your mobile device (phone, pad or tablet) for your University email and calendar, it must be protected by a PIN code. Setting a PIN code protects both you and the University from unauthorised access to your University Exchange account.”

Your personal information

Vigilance about impersonators
Do not give out personal information on the phone, through the mail or over the Internet unless you’ve initiated the contact or know who you’re dealing with. If a company that claims to have an account with you sends email asking for personal information, don’t click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service.

Use a firewall
Firewalls assist in blocking dangerous programs, viruses or spyware before they infiltrate your system. You can also install firewalls on your personal devices.

Anti-virus
When it comes to our computers, anti-virus and anti-malware is now ubiquitous; but did you know that your mobile devices can also be protected? Consider using AVG Free or McAfee LiveSafe.

Your money

Use your PIN
Using your PIN instead of contactless payments mean you can keep better track of your outgoings. Contactless payments can take up to 10 working days to show on your statement and balance, whereas a PIN payment shows within 24 hours.

Review your accounts
Look at your bank and store card statements regularly for suspicious transactions. There have been cases in Britain recently where small amounts of between £1 and £3 were taken every month. While this might not seem like much, if scammers can count on as few as 500 people per month not noticing, they can make thousands of pounds. Be vigilant with your own finances.

Get a credit report
You can get a free credit report which allows you to check for suspicious activity and identify any accounts or services that were opened maliciously.