Tips & advice

Practice good online safety habits with these tips and advice. This section has been developed in coordination with Get Safe Online (UK) and the Department of Homeland Security (US)

- Protect your personal computer (PC) and portable devices
- Protect your personal information and identity
- Protect business information outside your organisation
- Connect with care
- Be Web wise

Protect your personal computer (PC) and portable devices

PC

- Use a firewall: Firewalls protect your network some viruses and hackers
- Install anti-virus software: Anti-virus software prevents virus infections from spreading on your computer
- Get the latest security updates: Keep your applications and operating system fit, healthy, and up-to-date
- Stop spyware: Don't let strangers get inside your computer by avoiding suspicious emails and attachments
- Make regular backups: Protect your data from disaster

Laptops

- Switch off wireless connections when not in use or required
- Connect your laptop to a trusted network regularly to update your security mechanisms.
- Backup the information stored in your laptop
- Don't leave your laptop unattended

USB drives

- Use an encrypted USB drive
- Put the USB flash drive in read-only mode using the physical switch to avoid virus transmission: some USB flash drives include a physical switch to put the drive in a read-only mode to avoid the host computer from writing or modifying the data on the drive
- Scan USB flash drive after copying files from an untrusted and/or unauthorised machine to avoid virus transmission
- Before plugging your USB drive into someone else's computer, delete all files which are not relevant for the purpose of that action

- Backup information in your USB to recover data in case of a disaster
- Attach USB drives to key chains/lanyards to avoid loss of media: the reduced size of USB flash drives makes these devices easier to lose or be stolen. Furthermore, the higher storage capacity increases the potential amount of data at risk for unauthorised access. USB flash drives are usually put in bags, backpacks, laptop cases, jackets, trouser pockets or are left on unattended workstations. The number of incidents has increased recently as USB drives get lost, misplaced, borrowed without permission or stolen

Mobile phones and handheld computers

Handheld computers like Windows Mobile, Palm, iPhone, Android and Blackberry devices, come with Internet links and the capability to store vast amounts of information. Their very portability means they need to be treated with extra care

- Switch off wireless connections (i.e., Bluetooth and WLAN) when not in use. Bluetooth technology enables electronic devices to communicate with each other by using a short-range radio link
- Don't leave your mobile phone and handheld computer unattended. Otherwise, it could lead to data loss
- Use the password function to prevent remote hacks into your smartphone

Protect your personal information and identity

- **Use a strong password**: Your password is the equivalent of the lock and key to your house on the Internet. Passwords are a major defence, and developing good password practices will help keep your sensitive personal information and identity more secure. The password of your computer is the key to access all information — both corporate and personal — you have stored on your computer and online accounts. Use a strong password to protect your data: use a complex set of characters; combine letters (capital and lowercase), numbers and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Don't use personal information — name, child's name, birthdates, etc. — that someone might already know or easily obtain and try to avoid common words: some hackers use programs that try every word in the dictionary
- **Change your password regularly**: If you believe your system has been compromised change passwords immediately
- **Keep your password secret**: Your password is unique and must not be shared with anybody. Whenever possible, try to commit your passwords to memory. Have a strategy to memorize them. If you write your passwords down, be careful where you store them. Do not leave these records of your passwords anywhere that you would not leave the information that they protect
- **Unique account, unique password**: Use different passwords for each online account you access (or at least a variety of passwords). If you use the same passwords on multiple

accounts, an attacker who gains the access to one account will be able to access to all of your accounts

- **Secure your accounts**: Many account providers offer additional ways to verify who you are before you conduct business on that site
- **Own your online presence**: When available, set the privacy and security settings on websites to your comfort level of information sharing. It is preferable to limit who you share information with
- **Use social networking sites carefully**: Be aware that social networking sites can bring together many of the risks associated with being online; online bullying, disclosure of private information, cyber-stalking, access to age-inappropriate content and, at the most extreme, online grooming and child abuse

Protect business information outside your organisation

- **Ensure you keep sensitive information secure**: When you are outside your organisation, ensure you keep sensitive information and equipment secure at all times to prevent theft or loss. In particular when you are in public places, handle information with care
- **Keep business information confidential**: Be aware that someone can overhear your conversation. Don't make your organisation's confidential information available to everyone
- **Be aware of shoulder surfing**: When travelling or working from a remote place protect yourself against shoulder surfing
- **Use webmail wisely**: Using an internet browser to read your mail needs the same caution as a desktop mail system and it has a few security risks of its own

Connect with care

- **Switch off wireless connections when in use or not required**
- **Get savvy about Wi-Fi hotspots**: While using Wi-Fi hotspots limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine
- **Protect your money**: When banking and shopping online, check the sites are security enabled. Look for web addresses with https:// or "shttp://", which means the site takes extra measures to help secure your information. Http:// is not secure
- **Stop unwanted email**: Spam email is a security threat. Don't open unknown e-mails and attachments
- **When in doubt, throw it out**: When links in emails, tweets, posts, and online advertising look suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email
- **Forward e-mail whether it is appropriate**. Consider deleting the history of the message before doing so
- **Surf the Internet carefully**

- **Don’t download documents and material from untrusted parties**
- **Use public computers carefully:** Only connect on a public computer when you have an encrypted connection (indicated by a padlock in the bottom right hand side of your browser window and the letters ‘https://’ at the beginning of the website address)
- **Use webmail services from well-known and trusted companies**

Be Web wise

- **Stay current:** Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with family, friends, and colleagues and encourage them to be Web wise. Make your browser safe
- **Think before you act**: Be careful with communications that suggest you to act immediately, offer something that sounds too good to be true, or asks for personal information
- **Back it up**: Protect your work, music, photos, and other digital information by making an electronic copy and storing it safely