|  |  |
| --- | --- |
| Information Security: How to protect yourself and your personal information |  |

10 key information security tips

1. Do not click on a link in the email until you verified the source.
2. Never enter sensitive information in an email or text message.
3. Use antivirus software, run it regularly and keep it up to date.
4. Limit web usage in the office to core, business-related sites, to reduce the probability of compromise.
5. Make minimal use of unsecured, public networks and computers.
6. Create strong passwords and change them periodically, after core staff changes, and after every breach.
7. Do not use the same passwords for multiple accounts. Do not share passwords with others.
8. Create separate email accounts for work, personal use, alert notifications, hobbies and other interests.
9. At home, set up primary network and a separate network for kids and guests.
10. Be aware of what you share about yourself, family, friends, your location, and your job on social media.

Additional safeguards

## Laptops:

* Use a password. Laptop should be configured so that the password has to be entered every time you turn the machine on or when it comes out of hibernation, sleep or screensaver mode.
* Protect yourself from others: don’t connect to public wi-fi.
* Don’t disable antivirus software.
* Ensure that operating system and other software (productivity apps, browsers, etc.) have been updated with the latest security patches.
* Back up these devices to ensure that you can quickly recover the data. Secure your backups.
* Encrypt the hard drive. Macs have this ability built-in, and you can use Bitlocker for Windows.
* Use company VPN when working over publicly accessible networks.
* Use secure email.

## Passwords:

* Create passwords that are at least 10-14 characters long, use a mix of numbers, upper- and lowercase letters, and special characters.
* Change passwords periodically.
* Store them in a safe place, or use a password manager.
* Do not re-use passwords.
* Do not use dictionary words and other common passwords.
* Do not select “remember my password” on the sites that you visit.

## Email:

* Create separate email accounts for work, personal use, alert notifications, hobbies and other interests.
* Turn on two-factor authentication on all sites that support it.
* Encrypt important files before emailing them.
* Use spam filtering to stop unwanted emails from reaching your in-box.
* Scan attachments for viruses. Major email providers have this option; check to make sure that it is not disabled.
* Do not open emails from unknown senders.
* Do not reply to requests for financial / personal information.

## Virus and malware protection:

* Keep operating system software, browsers, applications up-to-date.
* Install anti-virus software and keep it up-to-date. Run it regularly.
* Turn on the firewall on the highest level.
* Regularly back up your data.
* Do not install pirated software.
* Do not install peer-to-peer file sharing programs.
* Do not set emails to auto-open attachments.

## Internet usage:

* Download software only from trusted sources.
* Log out of sites instead of simply closing the window.
* Look for https:// for secure session validation.
* Do not click on links from unknown or untrustworthy sources.
* Do not allow e-commerce sites to store your credit card information.
* Do not click on pop-up windows to close them; use “X” in the right upper hand corner of the screen instead.

## Mobile devices:

* Keep screen lock on. User strong passwords.
* Select a device with anti-theft features.
* Turn off Bluetooth when it’s not needed.
* Regularly update the operating system and apps to get the latest security patches.
* Securely back up your data.
* Do not click on ads when surfing the internet.
* Do not “jail break” your mobile phones.
* Only install the apps that you really need.
* Disable location services for apps that don’t need it.
* Do not connect apps to other resources unless it is necessary.
* Reset these devices to factory setting, or “wipe” them, before selling, gifting, exchanging, or disposing of these devices. Remember to take out the SIM card.

## Public wi-fi / hot spots:

* Disable ad hoc networking.
* Turn off auto-connect to non-preferred networks.
* Turn off file sharing.
* Consider using your phone’s mobile network instead.
* Do not use / avoid public wi-fi.
* Do not use public wi-fi to enter personal credentials.

## Home networks:

* Create one network for you, and another one for guests.
* Change your router’s name and password.
* Change the password to your wireless network.
* Turn on router’s WPA2 encryption and firewall.
* Do not use default user names and passwords.
* Do not broadcast your home network.

## Social engineering:

* Make a phone call to contact the person who sent the email to confirm the authenticity if you suspect that it may be fraudulent.
* Limit the amount of personal information you give out.
* Use privacy settings online wherever possible.
* Do not respond to requests for personal and financial information via email.
* Do not open an attachment from someone you know if you’re not expecting it. Call to confirm before clicking.
* Do not assume that every email you receive is authentic.

How to choose services, software and equipment?

## Email providers

Email is one of the most essential online services used today. If your email is compromised, your personal information (accounts, communications, phone numbers, addresses, etc.) can be stolen.

Features to look for:

1. Authentication. A high quality email service will provide secure authentication to prevent spam and spoofing.
2. Virus scanning. Email is scanned for malicious content by the provider.
3. Anti-spam: reputable email service providers filter spam from your inbox.
4. Phishing protection. Some service providers will identify potential phishing emails.
5. Look for a provider that offers enough storage to meet your needs, good IMAP and POP sync, options for your mobile device, and intuitive interface.

## Password protection

Weaknesses are a result of how users choose and manage passwords, and it can make it very easy for hackers to access them and break into individual accounts. Password management tools help users store and organize passwords, and can even provide additional features, such as form filling and password generation and audit.

Features to look for:

1. Synchronization. A good password manager will allow access from anywhere and synchronize across devices.
2. Password generator. Automatically generates strong, complex passwords.
3. Encryption. Passwords are stored encrypted, and the master password is not retrievable.
4. Multi-factor support. Better management tools will support complex multi-factor passwords.
5. Look for password management tool that supports all types of browsers, operating systems and mobile devices that you use.

## Virus and malware protection

If you use a computer for banking, web browsing, shopping, email, instant messaging and don’t have proper protection, you are at a high risk of being victimized. Running real-time anti-virus products and keeping them up-to-date is an essential step to reduce risk from malware, and can reduce infection by more than 80%.

Features to look for:

1. Detection. High-quality software detects existing and new variations of malicious software.
2. Cleaning. Effectively quarantines or removes malicious software from an infected device.
3. Protection. Helps maintain a healthy system by proactively preventing malicious infection.
4. Performance. Good anti-virus software will not slow down your system.
5. Parental controls. Optional feature that will secure your system when used by children.
6. Backups. Many applications provide optional back-up protection in case of system failure.
7. Consider the number of devices that each vendor will allow the software to be installed on per license subscription purchase.

## Wireless routers

A wireless router allows you to connect devices to the internet and communicate with other devices on your network. Routers are computers, with their own operating system, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log key strokes and access your accounts.

Features to look for:

1. Distributed Denial of Service (DDoS) protection. Prevents high-volume malicious attacks on your home network.
2. Firewall. Secures your network from intrusion.
3. Gust network. Allows for separate network and credentials for temporary access.
4. Look for a router with a range that fits the size of your home and supports the number of devices you want to connect to it.

## Internet of Things (IoT) devices

New IoT devices are coming in every day. An IoT device is any nonstandard computing device that connects wirelessly to a network and has the ability to transmit data. Examples of IoT devices include thermostats, light bulbs, door locks, fridges, cars, fitness trackers, implants for RFID and pacemakers.

Features to look for:

1. Software/firmware update capability. Every network-connected device should have a means for authorized operators to update the device’s software and firmware. Ideally, the updating process will be highly automated while still providing cryptographic checks to allow updates from an authorized source.
2. System reset. Every device should include a way to reset it to its original manufactured clean state.
3. No default password. Rather than permitting an easy-to-hack default password, each device should require the user to define a unique and reasonably secure password for access from a network interface.
4. No ancillary services. A device should not offer any services to the network that it does not require to support its core functions.
5. No backdoors. A device should not have hidden or known entry points that can be easily exploited by the device vendor or others.
6. Availability of privacy options. A device should allow you to configure privacy options, limit the amount of information it shares.
7. Device support. Device makers should provide online access to operators’ manuals, access to updates, and updated instructions. Support information should include a clear explanation of the product’s support lifecycle.
8. Contact information and support forum. Vendors should provide contact details or a support forum to which organizations can report any problems with the device or its software.
9. Basic support label. Each device should carry a label that helps the authorized operator identify it and find support information.