Cyber Security: Top Tips

Passwords

If a website is compromised and the passwords stolen then criminals will try the email address and password against other websites. If you have used the same password on multiple sites, you have a problem!

You also need to avoid the most commonly used passwords, as they are too easy for attackers to guess.

It is humanly impossible to remember lots of different complicated passwords, so you need password manager software. Password managers will generate really complicated (genuinely random) passwords for you, store them securely, and automatically enter them into website login screens (but just as helpfully will not automatically enter them into fake ‘phishing’ login screens).

- Use a different password on every website or web service: do not reuse them
- Use complicated – ideally truly random – passwords
- Using password manager software makes both feasible: it will generate passwords and store them for you

Two-step authentication

Many web services now allow a ‘two step’ login process. Either a code is read from a phone app, or (most commonly) is sent by text message to your phone. The code is only valid for a short period of time, meaning if it gets into the wrong hands it can’t be used.

Both Google and Microsoft Office 365 make this available.

- Turn on two-step authentication where it is offered.

Anti-malware software

Probably the best known defence.

- Install anti-malware software from a reputable source on all your devices. Keep it up-to-date.

Website blacklists

Many security software (anti-malware) software packages block known dangerous or fake websites. On a bigger scale, systems for filtering website access are available for networks.

- Use website blocking software, or a network service to avoid access to dangerous sites.

Software updates

Software is very complex, and it is possible to give it a particular set of input conditions that can cause it to fail. In even more specific circumstances, this ‘failure’ can flow in a particular direction, leaving the computer insecure and causing software code carried alongside the attack to run. This is another way hackers install ‘ransomware’ software onto computers.

- Install security updates without delay.

Awareness and training

Awareness of the risks amongst staff makes it more likely that they will avoid being tricked or accidentally do the wrong thing.

- Security is everyone’s job.
- Make sure staff know the importance of looking after information.
- Share awareness of the latest security threats.

Secure configurations

Software tends not come configured in the most secure way. For example, it is a good idea not to use an account with ‘administrator’ capabilities for day-to-day use on Windows. There are online guides to configuring software securely: see NCSC End User Device Guidance, for example.

https://www.ncsc.gov.uk/guidance/end-user-device-security

You should also disable or uninstall software that you don’t need, to avoid being impacted by security problems with it. As an example, some of the bundled software with Lenovo laptops had serious security issues.

- Uninstall software you don’t need.
- Configure software securely.

Blocking inbound connections

Network firewalls and personal firewall software to ensure that devices on your network cannot be ‘seen’ or contacted by anyone outside. Most broadband routers have firewall settings: as default they tend to block inbound connections, but it is a good idea to check that no inward routes have been opened you don’t need.

- Ensure network firewalls are operating and don’t have unnecessary ‘holes’.