Cyber Hygiene Top Tips

PASSWORDS

All passwords you use should be strong and unique. For example, don’t use the same password across any personal and work-related sites that require you to login.

Use a password manager as these can create strong passwords that can be stored securely. There are free ones available such as LastPass or KeePass.

Wherever possible, ensure you turn on two-factor authentication (2FA).

Never store passwords in your web browser, as its not as secure as a dedicated password manager and are weak to local attacks.

UPDATE EVERYTHING

From the operating system to the apps you use, ensure everything is up to date to reduce the chance of an exploit.

When downloading apps to mobile devices ensure you download them from trustworthy sources. Get rid of old apps you don’t use to reduce the attack surface.

Don’t jailbreak your mobile phone, as you make the kernel available to attackers.

Make sure you have endpoint protection on all your devices to detect and remove viruses and malicious code.

DON’T TRUST PUBLIC WI-FI

Don’t access personal or financial data with public Wi-fi as you don’t know if this is a spoof access point and open Wi-fi’s are not safe connections as others can see the data you are posting.

APP PERMISSIONS

When downloading an app for the first time check the permissions that the app is requesting are appropriate to the permissions it needs.

Turn off location services unless using an app that requires this service.

If using business apps on your mobile phone, ensure those are installed into a separate container or workspace so when removed you don’t lose all your data.

ENCRYPT EVERYTHING

Encrypting files can reduce the chances of your data being compromised if you lose your device or are hacked.

You can turn on Apple’s FileVault or Windows BitLocker encryption to encrypt the hard drives on a laptop or desktop.

Both iPhones and Android devices are encrypted by default, however it is still good to make sure you are making regular backups and do a check to ensure you are backing up what you think you are backing up.

SOCIAL MEDIA

Assume everything is public and check your privacy and visibility settings on social media sites to ensure that only contacts you know can see what are sharing rather than a public audience. Also ensure that any personal information like email address, date of birth and home address is not shared at all.

Don't post geotagged photos on social media sites – remove geolocation tagging from the photos you post online as its easy for an attacker to see where you are especially if you are on holiday. Wait to post your holiday pictures on your return that way you are not advertising that no one is at home!

Message companies privately rather than posting on the company's social media pages as this information is publicly available to an attacker and they will use it against you and try and call up as you to get your information from companies that are less likely to do rigorous checks on your data like a bank and could divulge it to a hacker.

FRAUDULENT WEBSITES

Check the website starts with https:// and the site has a padlock icon in front of the website name in your browser as it shows the site is encrypted so your browsing and payments can't be intercepted.

Check the website address via Google's Safe Browsing search or similar.

Never pay via bank transfer if credit card payment options are not available.

Check for online reviews of the website and check that the reviews are not all by one person or are very new.

If something is that much of a bargain it's probably too good to be true. Check the returns policy and delivery information as fraudulent websites will not offer information on how and where to return a faulty item.

EMAILS

With the rise on phishing emails, often the email will be requesting you send them money, click a link, or divulge your password or bank information, stop! Take your time to check who is sending the message – does it look legitimate?

Never click on a link in an email, send money in a hurry or divulge your pin or personal information to an incoming call regardless of who they say they are. Ensure you call your bank or organisation back via their main number by looking them up on the internet.

TEXT MESSAGES

Smishing messages are text messages with a link in them. Do not click the link. If the text message is from your bank or HMRC find the legitimate number on their website and give them a call if you are concerned.

PHONE CALLS

Assume everyone in the room can also hear your private calls, so be cautious about the information you are disclosing in public places.

Be cautious if you receive a call asking you for a payment, pin number or password urgently. Always call the company back by checking the telephone number on their website so you know you are calling a legitimate number and not a hacker before disclosing any personal information.

If there is a sense of urgency, money requested, links to click on or personal information is being requested or you don't think something is quite right, don't do it!