COMMON CYBER THREATS

SOCIAL ENGINEERING

Attackers attempt to trick you into doing 'the wrong thing', such as clicking a bad link that will download malware or direct you to a malicious website.

MALWARE

Malicious software or file that can infect a device and be a security risk to the user.

RANSOMWARE

Locks the user out of their files or their device, then demands an anonymous online payment to restore access.

SPYWARE

Unwanted software that infiltrates your device, stealing your Internet usage data and sensitive information.

MALICIOUS WEBSITES & APPS

Websites or Apps that contain malware or malicious content that compromise your data and device.

UNSECURED WI-FI

Hackers can steal unencrypted data from users' devices accessing the Internet through unsecured public Wi-Fi.

DEVICE THEFT

Criminals steal your device, then use it to commit criminal acts online.

CYBER CRIMINALS WILL LOOK FOR WEAK POINTS IN YOUR HOME TO GET THEIR HANDS ON FINANCES OR SENSITIVE DATA THAT THEY CAN USE FOR THEIR OWN GAIN.

This diagram highlights key weaknesses in the home that you should be aware of.

We have included practical tips (found overleaf) that you can refer to, to help you secure these weaknesses and further guidance can be found on our 'Secure Your Home Information Hub' on our website.

www.nicybersecuritycentre.gov.uk/home-security

ROUTER – YOUR GATEWAY TO THE INTERNET

Your broadband router is the gateway to the Internet and your first line of defence from cyber criminals being able to access your home network or other devices. Learn how to use its security features such as turning on a built in firewall and changing the default login password.

SEE TIPS 2 3 4 5

WI-FI

Don't make your Wi-Fi network on your broadband router easy for cyber criminals to access.
All the data that transmits wirelessly around your home needs to be protected. Learn how to secure it correctly and change the default password.

SEE TIPS 3 5

TVS AND GAMES CONSOLES

Most TVs and games consoles can connect to the Internet, which makes them vulnerable to cyber security breaches if they're not securely set up and kept up to date by enabling automatic software updates.

SEE TIPS 8 10 11

COMPUTERS & LAPTOPS

These devices hold and process a lot of your personal data.
It is important to properly protect them from unauthorised use and from viruses (also called malware). Learn the basics of securing your devices and be sure to install anti-virus software.

SEE TIPS 1 4 5 6 7

SMART PHONES & TABLETS

Mobile devices carry as much data as a PC or laptop. Because they are portable, they can be easily lost or stolen. Learn how to secure them correctly.

SEE TIPS 1 5 6 8 9 10

HOME OFFICE

When working from home it's important to keep your devices secure against cyber criminals and unauthorised access by family and friends. Portable devices can be lost or stolen more easily, which means the data on them could be at risk. Make sure you know how to report any problems to your IT department.

SEE TIPS 4 8 9 12

SMART TOYS

'Smart' or 'connected' toys are interactive and can be used by children from as young as three. They can be connected via Bluetooth or a Wi-Fi connection. As with any smart devices, you should check that the Internet connection it links to is securely set up, and that any apps it links to on your phone or tablet are securely configured.

SEE TIPS 5 6 8 10

SMART SECURITY DEVICES

Internet-connected security devices such as CCTV cameras, baby monitors, locks and doorbells are open to the same risks as other smart home devices, except cyber criminals can access live footage and possibly control your door locks. Learn how to set up smart security devices properly to protect your home.

SEE TIPS 3 5 8 10

SMART DEVICES

Smart home devices such as smart speakers and appliances (sometimes called Internet of Things or IOT) contain miniature computers that connect to your home network.

Cyber criminals can use these devices to spy on you or to commit other crimes.

Ensure security is part of your buying criteria when purchasing 'smart devices' and learn how to keep them updated and secure.

SEE TIPS 3 5 8 10

ONLINE ACCOUNTS & CLOUD SERVICES

Services you use online like shopping, social media, email, media streaming, and cloud services (e.g. photo/file backup sites) can be targets for cyber criminals, due to the personal data and financial information stored on them. Strong passwords and enabling 2 Factor Authentication can help protect your data.

SEE TIPS 5 6 7 10

A CYBER SECURE HOME

HAVE CONFIDENCE IN YOUR HOME SECURITY

A connected home is set up so that Internet-enabled appliances and devices like central heating, lighting, security cameras, baby monitors, TV's and kitchen appliances can be controlled remotely using a networked device such as a smart phone.

While a connected home is efficient and makes life a lot easier, there are security risks. If these 'smart' appliances and devices are not correctly set up and secured, cyber criminals could gain acess to them and potentially steal personal & private data and financial information that you store or access through your smart devices.

NI Cyber Security Centre

We work to make Northern Ireland cyber safe, secure and resilient for its citizens and businesses.

Contact us
info@nicybersecuritycentre.gov.uk

Visit our website
www.nicybersecuritycentre.gov.uk

Follow us on Twitter
@NICyberSC

In association with :-

scamwiseNI PARTNERSHIP

Version 1 - October 2021

1.PHYSICAL SECURITY

- Store devices out of sight in safe places when not in use e.g. car or home
- Turn on a 'Find My Device' service so that lost or stolen devices can be located, and data can be wiped remotely if necessary.
- Regularly make a secure backup of your data separate from your computer, offline, and stored in a safe place.

2. KNOW YOUR NETWORK

- Change the default username and password on your Internet Service Provider's router and any other network devices you may have. Your provider should give you instructions on how to do this.
- Be aware of what is connected to your wired network and Wi-Fi using tools like the 'Fing' app. Some routers also have this feature built in. This will help identify any devices that should not be using your network.

3. SECURE YOUR WI-FI

- Never set your Wi-Fi network to 'Open'. Your Internet Service Provider should give you instructions on how to secure your Wi-Fi with 'WPA2' or 'WPA3' encryption standard.
- Change the default name of your Wi-Fi network (called the SSID) to something that won't disclose your Internet Service Provider's name (which can reveal the hardware you are using to cyber criminals).
- Change the default Wi-Fi password to something strong and hard to guess, and only share it with people you trust.
- Set up smart devices (e.g. your smart speaker) on a 'Guest' Wi-Fi network so that they are kept separate from devices that store private data, such as your PC or laptop. This reduces the risk of a hacker getting access to your main network through one of these devices. More information on how to do this can be found on our website information hub.

4. USE ANTI-VIRUS AND FIREWALLS

- Firewalls help stop unwanted Internet traffic and malicious apps using your network.
- Turn on the firewall included on your Internet Service Provider's router.
- Install an anti-virus package with built in firewall to secure each device against malware.

5. USE STRONG PASSWORDS

- Set strong passwords using three random words - longer is stonger.
- Ensure you have a strong password for your primary email because criminals could use this email account to get access to your other accounts using the 'Forgot Password' feature.
- Don't reuse passwords on multiple accounts.
- Use a password manager or your browser to store your passwords.

6. ENABLE 2 FACTOR AUTHENTICATION

- Use Two Factor Authentication (2FA) - this is essential and a way of 'doubling up' on security by verifying your identity using a code sent to your mobile phone, email address, or from an authenticator app.

7. SURF THE INTERNET SECURELY

- Use an up to date web browser such as Microsoft Edge, or Google Chrome.
- Check the address bar to make sure you are on the proper website you intended to visit.
- Only use reputable websites for shopping.
- Don't give more information that is needed to carry out a transaction.
- Consider more secure payment options – e.g. payment services like PayPal, or a credit card that provides additional buyer protection.

8. SECURE YOUR SOFTWARE

- Enable automatic updates for operating systems (e.g. Windows), apps, and anti-virus software - this will allow the latest versions to always be in place, minimising the risk of cyber attacks due to using out of date software.
- Only purchase and download software from reputable and trusted sources.
- Only buy devices from reputable retailers to ensure they adhere to safety and security guidelines
- If a device is no longer supported by the manufacturer, replace it with one that is.

9. BEWARE OF FAKE EMAILS AND TEXTS

- Scam emails (phishing) and text messages (smishing) that appear to be from reputable sources are known as social engineering. These are sent by cyber criminals trying to encourage the recipient to click on a dangerous website link, download malicious software or give out confidential data.
- Don't click on links, download attachments or take any other action if you're unsure about the sender of the email or text.
- Send suspicious texts to 7726 and phishing emails to report@phishing.gov.uk

10. SET UP PRIVACY CONTROLS

- Only allow necessary cookies for websites when you visit.
- Review privacy settings for apps on your devices and for services that you use online.
- Don't give more information than what is required to create an account or use a service.
- Make sure your social media accounts are set to private so that your information is not widely shared.

11. TURN ON PARENTAL CONTROLS

- Make sure there is a password or PIN for you to verify payments your children want to make, for example, in-game, or app purchases, otherwise they might purchase things above their age group.
- Set up content filters on devices that will block inappropriate websites.
- Talk to children about Internet safety. Useful resources on this can be found on our website information hub.

12. WORK FROM HOME SECURELY

- Be aware of your organisation's policies and procedures.
- Know how to report cyber incidents.
- Don't let family members use your work device.
- Accept software updates as soon as they appear on your device.

Pocket Guide to

A CYBER SECURE HOME

Practical steps to help secure your connected home.

NI Cyber Security Centre

ALWAYS REPORT CYBERCRIME, ESPECIALLY IF YOU HAVE BECOME A VICTIM

PSNI

T:101 (Non Emergency)
W: www.psni.police.uk

ACTION FRAUD

T: 0300 123 2040
W: www.actionfraud.police.uk

If you are in immediate danger and need assistance dial 999

VISIT OUR HOME SECURITY HUB FOR GUIDANCE AND TUTORIALS

SCAN ME

nicybersecuritycentre.gov.uk/home-security