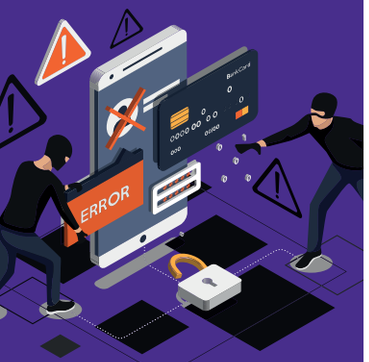
COMMON CYBER THREATS



Many cyber attacks are basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked.

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

INSIDER THREATS
Employees may accidentally or purposefully cause damage to devices, your network, or data.

MALWARE (E.G. VIRUS)
Malware is a piece of software that is specifically designed to disrupt, damage, or gain unauthorised access to your computer.

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

WATCH OUT FOR WEAK POINTS

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

This diagram highlights key weaknesses that you as a business owner 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 Business Hub' on our website.

CLOUD SERVICES & ONLINE ACCOUNTS
Businesses often use virtual 'cloud' services to back up or store files. These can be targets for cyber criminals due to the sensitive business data held within them. Business applications such as accounting, HR, or email services may also be provided over the Internet, and access to these should also be tightly controlled.

SEE TIPS: 5 8 9

SUPPLY CHAIN
If a supplier suffers a security breach you could be attacked through them if their systems and methods of connecting to your network are not secure. Enquire from your suppliers how they secure their services and support to you.

Bogus invoice scams are also common – ensure you and your employees know how to check a supplier invoice is genuine.

SEE TIPS: 8 9

VISITORS
Visitors to your workspace (authorised or unauthorised) might have an opportunity to view confidential data (e.g on an unattended laptop), or they might find a way to tamper with devices or networking equipment.

SEE TIPS: 1 2 8

EMPLOYEES
Employees can present risks to your business through inappropriate use of devices, or not being aware of common cyber threats like phishing emails.

A rogue employee could take advantage of their access to sensitive business information or financial information and assist a cyber criminal to launch an attack (an insider attack).

SEE TIPS: 5 7 8 9 10

REMOTE WORKING
Working remotely from home, traveling, or in a public place can bring additional security risks.

Any portable personal or business-owned device like a laptop, tablet or mobile phone can be easily lost or stolen, which means the data stored on them could be at risk. If you use an unsecure Wi-Fi connection in a public building cyber criminals could access the device and steal the data held on it.

SEE TIPS: 3 5 7 8 10

WI-FI
Cyber criminals can attempt to intercept and gain access to your private business data, login credentials, or actively view data being communicated across your Wi-Fi network.

SEE TIPS: 3 5

SMART DEVICES
Many workplaces have smart devices like smart speakers and security systems. As these are connected to the Internet, there is a risk of cyber criminals using the devices to spy on you, gain access to your network, or steal passwords.

SEE TIPS: 3 4 5 6

SOFTWARE
Your business will most likely use software to process sensitive or confidential data. Cyber criminals will try to get hold of data like customer contact details or bank accounts, so they can then use these to make money. Cyber criminals can gain access through known vulnerabilities in software programs.

SEE TIPS: 6 8

DEVICES
Devices like PC's, laptops and printers, hold and process a lot of data and must be protected from unauthorised use and viruses (malware).

Mobile devices also need to be setup securely because they're portable and can easily be lost or stolen.

SEE TIPS: 4 5 6 7 8

WHY SECURE YOUR BUSINESS?

Cyber security should not be a daunting challenge for business owners. Following the steps outlined in this guide could save time, money and even your business' reputation by reducing the risks of a cyber attack. More details are provided on our Secure Your Business information hub on our website.

If you want to improve your cyber security further, then you can also seek certification under the NCSC Cyber Essentials scheme.

CYBER ESSENTIALS

CYBER ESSENTIALS

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

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

Version 1 - June 2021

1.PHYSICAL SECURITY

• Secure laptops and PCs to desks using lock cables.

• Use device encryption technology like Bitlocker to protect data on devices.

• Turn on a 'Find My Device' service so that lost or stolen devices can be located, and data can be wiped remotely if necessary.

• Restrict and control the movement of visitors in your building by installing key card entry systems on doors for example. This will help control access to equipment or devices.

• Ensure private areas and equipment are secured e.g. network equipment and cabling.

2. KNOW YOUR NETWORK

• Change the default username and password on your Internet Service Provider's modem and other network devices, such as routers and switches.

• Know what devices are connected to your Wi-Fi and wired network - this will help identify unauthorised devices being used.

• Ensure a monitoring system is set up to check for unauthorised activity on your networks.

3. SECURE YOUR WI-FI

• Change the default name of your Wi-Fi network (called the SSID) to something that will not disclose your Internet Service Provider's name which can reveal the hardware you are using.

• Change the default password on your Wi-Fi to something strong and hard to guess. The default password is usually found on a label on your router supplied by your Internet Service Provider.

• If your business provides free Wi-Fi to the public (e.g. you run a café or restaurant), set it up on a separate network from the one you use for business purposes.

• The best encryption standard for wireless security is 'WPA2' (or higher) – check your Wi-Fi settings to ensure this is in place.

• Do not use smart devices such as smart speakers, light bulbs, or power sockets on your business network where important data is held.

• Never set your Wi-Fi network to 'open'.

4. USE ANTI-VIRUS AND FIREWALLS

• Turn on the firewall included on your broadband provider's router as a minimum, or install a dedicated network firewall.

• Install an anti-virus package to secure all devices in your business against malware.

• Choose an anti-virus package with built in firewall.

• Enable automatic updates on your anti-virus software so you are protected against the latest threats.

5. USE STRONG PASSWORDS

• Use strong passwords made up of three random words – don't use easy to guess passwords like a pet's name or favourite football team.

• Don't reuse the same passwords on multiple accounts.

• Allow a password manager or browsers to store passwords.

• Use Two Factor Authentication (2FA) where possible - this is a way of 'doubling up' on security by asking a user to verify their identity using a code sent to their mobile phone, email address, or from an authenticator app.

6. KEEP HARDWARE & SOFTWARE UP TO DATE

• Ensure that software which is preinstalled on a device (called firmware) is always kept up to date.

• Enable automatic updating of 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.

• Create an asset register of the hardware and software your business uses and review it regularly.

• Create a replacement schedule for all hardware. If a device is no longer supported, upgrade to the newest model as soon as possible.

• Make secure backups of data, either on a regular basis or automatically. Follow the '3-2-1' rule; at least 3 copies, on 2 devices, and 1 off-line.

7. SECURE SET-UP

• Disable 'auto-run' on removable media like USB flash drives – so that if someone inserts it into a PC, it won't automatically run anything on it. This will prevent unknown or malicious software being installed on a device.

• Ensure anti-virus software automatically scans new media (e.g. flash drives) when inserted.

• Disable USB ports for all users unless required for business purposes. This will reduce the risk of malware infecting a computer or business data being copied without authorisation.

• Set up 'inactivity time-outs' or a screen lock on all user accounts so the device goes back to the login screen after a few minutes of inactivity.

8. USER MANAGEMENT

• Restrict permissions that users have to install software or access files to the minimum needed for their role.

• Limit the number of 'administrator' accounts in use. Administrator accounts have more access than regular user accounts, which makes them a valuable target for criminals. They should never used for 'everyday' tasks like sending email or web browsing.

• Have a process in place to manage user accounts from creation through to deletion.

• Temporary user accounts should be removed or suspended when no longer required.

• Create and share an 'acceptable use' policy – this usually includes guidance such as not using business devices for social media use or chatrooms.

• Share procedures on how to report lost or stolen devices.

9. SOCIAL ENGINEERING

• Be aware of scam emails (phishing) and text messages (smishing) that appear to be from reputable sources. These are sent by cyber criminals who are trying to encourage the recipient to click on a dangerous website link, download malicious software or give out confidential data.

• If in doubt, do not click on links, download attachments or take any other action if you're unsure about the sender of the email or text.

• Provide regular training for employees and set up a process for them to report phishing and smishing attempts.

10. WORKING FROM HOME

• Create, update and share your business' policies and procedures around safe and secure use of devices, software and accounts - e.g,using social media accounts, safe use of Internet etc.

• Ensure employees know what to do if there's a cyber incident.

• Check employees are aware not to let family members use business owned devices for personal use.

• Discourage the use of public Wi-Fi hotspots - these can be found in cafes or public spaces and are risky because they could be fake hotspots set up by a criminal.

• Consider the use of a VPN (Virtual Private Network) service for extra security. A VPN protects information being transmitted between your business device and your premises by using encryption technology.

Pocket Guide to

A CYBER SECURE BUSINESS

Practical steps to help secure your business against a cyber attack

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 BUSINESS HUB FOR GUIDANCE AND TUTORIALS

SCAN ME

nicybersecuritycentre.gov.uk/business-hub