# Cyber Security Toolkit

Illustration:
Charli, age 16 - Inspiralba

breeze_digital

www.breezedigital.uk

# Introduction

**Anyone can fall victim to a cyber scam or attack and suffer worrisome consequences including identity theft and financial loss. The positive news is there are steps you can take to help protect yourself and manage the risks.**

If you use a smartphone, laptop, tablet or computer and access services online, such as mobile banking, email and social media, your devices and online accounts hold your personal information, and you should take steps to protect it.

This toolkit is a starter guide to help individuals recognise common cyber risks and provides a simple checklist to work through to increase your cyber safety.

# Password Protection

Using a strong password is essential because it helps protect your personal and sensitive information from unauthorised access. Hackers and cybercriminals use various methods to crack weak passwords and access your personal information for their own gain.

Use Strong Passwords – The most common reason for use of a simple password and password reuse is that they are easy to remember so you don't get locked out of your accounts. This is the easiest win for hackers who can try a variety of common passwords to gain access to your device or online accounts.

The first proactive step you can take is to find a password manager to remember the passwords for you. The main advantage is that you only have to remember one strong password to access all your accounts.[1]

**How to create a strong password checklist:**

- Create passwords with a mix of upper and lowercase letters, numbers, and symbols.
- Longer Is Better - Longer passwords are more secure; aim for at least 12 characters.
- Unique for Each Account - Never reuse passwords a cross different accounts or services.
- Passphrases Are Effective - Consider using random word combinations for easy-to-remember yet strong passphrases.
- Avoid Common Choices - Stay away from easily guessable passwords like ***"password"*** or ***"123456."***
- Regularly Update Passwords - Change passwords periodically, especially for critical accounts.
- Struggling to think of as unique password that meets the above criteria? Let your password manager generate a secure password for you.

1. For further information on password managers visit https://ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

# Password Protection (Continued)

**Enable Multi-Factor Authentication (MFA)**

What is Multi-Factor Authentication? Multi-factor authentication (MFA) is an additional layer of security that can be added to your personal accounts and devices. There are various options including security questions, passcodes and verifying your identity via a different device. For example, you are logging into your internet banking on your laptop and are asked to confirm your identity by entering a pin sent by text message to your mobile device.[2]

2 For further information visit: https://ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email

# Beware of Phishing

Phishing is simply an attempt to trick you into doing the wrong thing. It is a fraudulent practice by scammers to obtain personal information such as credit card details. They may pose as a relative, manager in your workplace or a reputable company.

If a link in an email, text or on social media looks suspicious, **DON'T** click on it.

**How to spot a Phishing Email?**

- Always check the email address that the email is coming from. As phishing scams become more sophisticated, emails can look like they are from a legitimate source and display a name that is recognisable to you.
- Beware of unexpected emails, text messages or phone calls with seemingly urgent requests or payment demands. In a work setting this might look like the CEO asking you to do an urgent task for them. In a personal capacity, it may look like your bank has contacted you about money leaving your account. As a general rule, take your time to check a source is legitimate by contacting your trusted suppliers.

Remember, you should never be ashamed or blamed for falling victim to an attack. If you click a link and are worried something may be wrong, speak to a trusted person and seek advice. These scams are deliberately set up to catch you out and anyone can become a victim.[3]

3. For further information on reporting a scam, please visit: https://ncsc.gov.uk/collection/phishing-scams

# Malware

Malware is software that is specifically designed to disrupt, damage, or gain access to your computer system. Cyber criminals use this to deceive a victim into providing personal information for identity theft, take your financial details, control your devices and to infect your devices to use them for mining cryptocurrencies.

## How to protect myself against Malware?

**Device Protection Steps:**

- Make sure your operating system and applications are updated as Cybercriminals look for weaknesses in outdated or old software. Ensure you install updates as soon as they become available.
- Always ensure your Anti-Virus is up-to-date and perform regular security checks by running a scan using the security software you have installed on your device.
- Restrict the number of applications on your device. Only install applications on your device that you need and use regularly use.
- Make sure all your software is licenced from a legitimate source.

**Here are the things to look out for:**

- Your device is running slower than usual.
- Your web browser takes you to a site you did not want to visit.
- Infection warnings – frequently accompanied pop-ups offering to buy something to fix them.
- Problems shutting down or starting up your device.
- Frequent pop-up ads

**Guidance on what to do if your device is infected with Malware:** https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take
**How to report Cyber Crime:** https://www.ncsc.gov.uk/section/information-for/individuals-families#section_5
**Resources:** https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
https://www.ncsc.gov.uk/guidance/securing-your-devices

**Be aware online:**

- Do not click a link on a pop-up as it may download Malware on your device Close the pop-up by using the "X" and navigate away from the website that produced the pop-up.
- If you have received an unknown link in an email, social media, or text message that you don't recognise, don't click the link.
- Make sure the website your accessing has https at the beginning of the website address/ Uniform Resource Locator (URL) to ensure it is a legitimate company site.
- Only purchase applications from official app stores as malicious software can be contained in these applications which bypasses your in-built security systems for your devices and gives an unauthorised person all your personal data.

**I think my computer has been infected with Malware. What should I do?**

1. Go offline!
2. Conduct a full system scan of your device using a legitimate anti-virus software.
3. Restore your computer to an earlier back-up
4. Delete all temporary files found in the Temporary Files folder.
5. Go into Safe mode
6. Reinstall your Windows or iOS operating system – these vendors allow you to do this free of charge.

# Firewalls

A firewall is a security program that helps protect your internet network by filtering unknown traffic and blocking outsiders from gaining access to your personal data. It is designed to allow only authorised traffic to talk to your computer systems.

## The Two Types of Firewalls

**Boundary Firewall** – This protects your whole network by restricting inbound and outbound traffic on a network of computers or devices. This is commonly used within organisations combating cyber-attacks by implementing restrictions / Firewall rules that allow or block traffic according to its source.

**Host based Firewall** – It works in the same way as a Boundary Firewall but is installed on one device and protects that alone. The main benefit of host-based firewalls is that they stay active even when switching networks, so they are prominently used for portable devices. This would be the perfect solution if you're working from home, in a coffee shop, traveling for work etc.

**How to make sure your Firewall is secure?**

- Always change the default password on your Firewall.
- **Restrict Access** – Make sure to set up rules to ensure that only certain people can access your firewall, this will keep your data safer.
- **Block all unauthorised access** – Create a whitelist, this is a list of devices, email addresses, IP addresses, domain names or applications that your firewall knows and trusts.
- **Laptops/Home working** – consider adding a Host based firewall to laptops that are used outside of your normal working location, this will help keep your data secure.
- **Virtual Private Network (VPN)** – this is establishing a protected network connection when using public internet connections which hides your website traffic from outside users. Consider using this when you go online to ensure your data is protected without it your online usage can be monitored and taken advantage of.

# Backups

It is critically important that you ensure that your files on your device e.g., pictures, bank statements, mortgage agreements etc are protected. To keep your files secure, create a backup copy of your valuable files to protect them against virus attacks, hardware failure or human error.

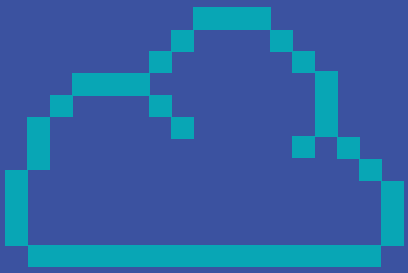
## Back up checklist

**Frequency** - Backups should be performed as often as possible, leaving too long between backups means more data lost in the event of an incident.

**Location** - Think about storing backups on the cloud or on removable media that is stored elsewhere such as a hard drive or a server

## 321 back up rule[4]

3: Create one primary back-up and two copies of your data
2: Save your backups on two different types of media
1: Keep at least one back up file stored off site.



[4]Government Help: https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

# Common Scams to look out for!

**1. "Hi Mum"**

Receiving a text message saying ***"Hi Mum, I lost my phone. Please reply to me on this number: 07xxxxxx".*** Replying to this message will lead to hearing about your child losing or breaking their phone and their friend loaning them the money to pay for a new phone.

The next message will be ***"Can you pay my friend back until I get internet banking set-up on my new mobile. I really need the money"***

**How to combat it?**

Always be suspicious of unexpected requests from relatives. If you think this accident might have occurred call your friend or relative to confirm its really them texting you with this request.

**2. Online Marketplace Scams**

Online Marketplaces such as Facebook Marketplace, eBay etc are becoming more popular to obtain the best deal on high value items. Scammers will copy a legitimate advert and post it on another marketplace. An individual will enquire if the item is available and you will receive a reply that the item is available but for some reason the person selling the item is away. They will ask for an up-front payment to secure the item. The seller may even send you an invoice. However, as soon as you make the payment, the post disappears, and all contact is lost.

**How to combat this?**

Don't ever buy an expensive item that you have not seen in person. Research the seller to ensure that they are legitimate through looking at previous reviews.

**3. Pig Butchering Scams**

This starts with a message on social media or a dating website and develops into a friendship or a romance. Over time, the new friend will give you compliments and share intimate information about their lives and asks you to do the same. Once this new friend gains your trust, they will say that they have been investing money into a new cryptocurrency platform and it's been doing really well.

The individual will suggest that you invest your money into the scheme. If you decide to invest, you may see it working for you and the profits go into your account on the new platform. You and your friend celebrate this and invest more and more money into the platform. Suddenly you log in and find your friends profile is gone and the cryptocurrency platform site does not exist.

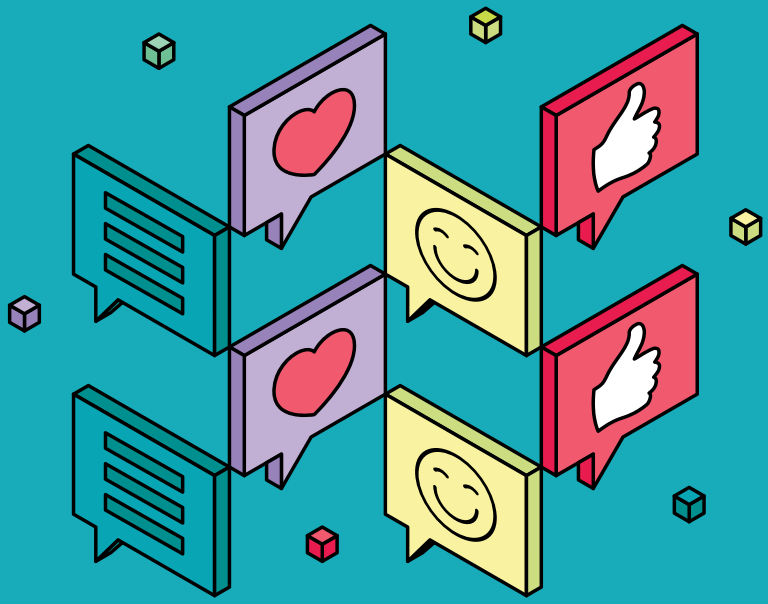
**How to combat this?**

The advice here is to be very careful where you invest your savings. Only take financial advice from sources which are regulated by the Financial Conduct Authority, and never from someone who, ultimately, is no more than a stranger online.[5]

[5] For more scams and further information on the scams discussed, please visit the below source. Source: "Five Scams to watch out for right now" By Nick Stapleton (BBC Scam Interceptors) Link: https://www.bbc.co.uk/programmes/articles/3M1LPtdbXrWFyqTyyNrCzT9/five-scams-to-watch-out-for-right-now

## Useful Resources:

For more information and live links sources used in this document please visit breezedigital.uk/url



## Contact Us

01506 862 227
info@breezedigital.uk