Cyber Fundamentals

BOXPHISH

Three of the most common cyber-attacks a business may encounter:

1. **Phishing** – most commonly conducted via email, trying to get the target to click on a malicious link or share their confidential information

2. **Social Engineering** – using manipulative, emotive behaviour to trick the target into sharing confidential information

3. **Ransomware** – a type of malware that infects the targets device and encrypts data, forcing them to pay a ransom to get their information back

Remember:

- Think before you share on social media
- Carefully check email domains
- Never click or download anything you're unsure about
- Use strong and unique passwords and passphrases, plus two-factor authentication where possible

Best Practises:

Protect your Data

Be Cautious with Emails

Strengthen your Accounts

Social Engineering

BOXPHISH

What: an attack that takes advantage of *human vulnerability* – often playing on the victim's emotions.

Why: tricking targets into handing over account credentials, personal information, company data or even direct payments.

Attacks often try to appeal to:

- ➜ Fear
- ➜ Curiosity
- ➜ Greed
- ➜ Sympathy

Best Practises for Prevention:

1. **Slow down** – assess the content carefully before reacting
2. **Ask questions first** – analyse the important details of the message before anything else
3. **Always navigate manually** – avoid links and visit websites independently if needed
4. **Beware of hackers** – try reaching out to the sender through another platform to verify their identity/message
5. **Second-guess unbelievable rewards** – if something sounds too good to be true, it probably is

Malware

BOXPHISH

There are several ways malware can be downloaded onto a victim's device:

1. **Phishing** – attackers aim to trick targets into opening an attachment loaded with malware, or into visiting an infected website
2. **Remote Desktop Protocol**– hackers brute-force passwords to gain access as an admin
3. **Drive-By Downloads** – downloads which take place without the victim's knowledge upon visiting an infected website
4. **USB & Removable Media** – cybercriminals load a USB with malware, leave it lying in plain sight and wait for a victim to pick it up and use

Malware can::

- ➜ Lock a device or render it completely unusable
- ➜ Tamper with data or take control of accounts
- ➜ Spy on your daily activities through keylogging

What should you do?

1. Disconnect infected devices
2. Disconnect from the Internet
3. Reset your credentials
4. Wipe infected devices
5. Ensure backups are free from malware before restoring
6. Connect devices to a clean network
7. Install, update and run anti-virus software
8. Reconnect to your network

Ransomware

BOXPHISH

What: ransomware is a form of malicious software which encrypts data on a device or network

Why: victims can only regain access to their files by paying a ransom to the criminals behind the ransomware

Always avoid:

1. Email attachments or hyperlinks
2. Compromised websites
3. Pop-up adverts
4. Physical devices

Over 50% of all organisations globally have been victims of ransomware attacks

Every 39 seconds an organisation is attacked

Safe Home Working

BOXPHISH

To ensure you are maintaining security when working from home, follow our highlighted best practices:

1. **Have you devices authorised by your IT department** – this should ensure anti-virus software is properly installed & you have a secure VPN in place
2. **Avoid sharing devices with housemates**– in order to limit the risk of human error
3. **Stay on top of your software updates** – un-patched vulnerabilities could lead to unauthorised criminal access and contamination or theft of cloud hosted data
4. **Maintain a connection with your IT team** – necessary in case you need to raise any security questions or concerns

Credit Card Fraud

BOXPHISH

There are 5 main ways you can become a victim of credit card fraud:

- ➜ Phishing
- ➜ Card Theft
- ➜ ID Theft
- ➜ Card Skimming
- ➜ Social Engineering

How you can stay vigilant:

1. **Never leave your card unattended**
2. **Regularly check your bank statements for unfamiliar payments**
3. **Never share your card details or PIN with anyone**
4. **Only communicate with your bank through official, secure channels**
5. **If in doubt, act with caution and withhold payments**

Physical Devices

BOXPHISH

Physical devices can be a serious threat to our online security:

1. **USB Drop Attacks** – attackers leave a malicious device in a public place, hoping that someone will pick it up and use it, hence downloading the malware onto their device
2. **Printer Breaches** – if your printer is linked to an unsecured network, hackers can view and access your confidential files
3. **Security Cameras** – hacking security cameras allows cybercriminals to spy on your daily activities
4. **Access Cards** – these are very easy to clone and can allow criminals to gain entry to secure locations

What should you do?

- ➜ Strengthen the security of internet connected devices
- ➜ Encrypt web traffic
- ➜ Upgrade your access controls
- ➜ Show caution with USBs

Mobile Devices

BOXPHISH

Mobile devices can be a serious threat to our online security:

1. **Device vulnerabilities** – this typically refers to loss, theft or physical infiltration, often linked to insecure PIN numbers on mobile devices
2. **Application Threats** – occurring through users failing to update apps or installing insecure/unauthorised apps
3. **Phishing Attacks** – when delivered through mobile devices these are known as smishing (SMS phishing) and vishing (voicemail phishing) attacks
4. **Insecure Networks** – linked to people working in a more hybrid world, the risk of insecure networks has increased as public Wi-Fi is rarely protected

What should you do?

- ➜ Protect your mobile devices with strong and unique PINs
- ➜ Use mobile apps carefully
- ➜ Show caution with mobile communications
- ➜ Stick to secure networks

51% of organisations have suffered a data breach through employee mobile devices

Account Takeover

BOXPHISH

This is a type of fraud where a cyber criminal gains access to a user's online account to access confidential data or steal financial information. This can be done in one of three main ways:

1. **Phishing** – most commonly this occurs through brand impersonation or CEO fraud to trick the user into revealing their account credentials

2. **Credential Stuffing** – login details which have previously been stolen are obtained and then used against a variety of websites in the hopes of finding a match

3. **Brute Force** – a form of hacking where the attacker creates an automated script that runs through potential password combinations until the correct sequence is found

Best Practises:

Set up Multi-Factor Authentication (MFA)

Look out for suspicious emails

Use strong & unique passwords

Social Media

BOXPHISH

There are two main ways social media can become a significant security risk, either as a source for criminals to **gather data** or as a platform for criminals to **contact you.**

Be cautious when posting about:

- ✖ Your holiday or vacation plans
- ✖ Your birthday or special dates
- ✖ Your address
- ✖ Any photos which might have confidential information in the background

Best Practices:

1. **Make privacy a priority** – consider who might have access to your information
2. **Strengthen your access security** – set secure passwords and use Multi-Factor Authentication (MFA) where possible
3. **Avoid over sharing** – don't give away any information that might give a hacker an advantage
4. **Show caution with direct messages** – remember anyone can be hacked, so be cautious with suspicious messages no matter who they're sent by
5. **Update your settings regularly** – ensure these remain up to date

Safe Internet Usage

BOXPHISH

When browsing the internet, it's vital that you stay aware of what you're browsing and what you're clicking on. You should be particularly cautious of:

- Unknown links
- Attachments
- Pop-up adverts

Clicking on any of these could result in malicious software being downloaded onto your device.

Remember:

- ➜ Think before you share on social media
- ➜ Don't accept friend requests from strangers
- ➜ Set your profile to private
- ➜ Be cautious about any suspicious messages or requests

Best Practises:

Weigh the potential risks before posting personal or work-related information

Configure your privacy settings across social media

Avoid clicking on suspicious links, attachments or adverts online

Passphrases

BOXPHISH

The most important thing when it comes to setting a strong password is **uniqueness.** In order to guarantee a truly unique password, a passphrase is the recommended option.

A passphrase is a combination of **three random words** creating a password that is both **long enough and strong enough** to protect your accounts.

You should evaluate your passwords if they include things like:

- ➜ Your family or pet's names
- ➜ Your school/workplace/hometown
- ➜ Any familiar dates
- ➜ Phrases like *password* or *qwerty*

What makes a good passphrase:

- **Use three or more random and unrelated words**
- **Aim for at least 14 characters**
- **Include a number between each word**
- **Don't repeat your passphrases across multiple accounts**
- **Don't use personal words or details which can easily be found online**
- **Never write your passphrases down or share them with anyone**
- **Consider the use of a reputable password manager**
- **Ensure Multi-Factor Authentication (MFA) is enabled where possible**

Workplace Security

BOXPHISH

Protecting your devices

Be careful what you're clicking on and watch out for suspicious download requests or attachments.

- Lock your devices when they are not in use
- Never walk away from your computer with confidential files or emails visible on screen
- Be aware what is on your screen when sharing on calls

Restricting physical access

Watch out for tailgating – a physical security breach where an unauthorised person will try to follow someone into a secure area

- Keep your key card or access fob stored safely on your person and don't lend it to anyone
- Question anyone unfamiliar you see trying to gain entry

Managing your files and data

Be cautious when you are accepting file transfers or downloads, as they could be infected with malware.

- Keep your work area free of papers and documents
- Avoid taking confidential files home
- Lock private information away at the end of the working day
- Shred documents when they re no longer required
- Never leave confidential files in a printer

Identity Theft

BOXPHISH

Identity theft often begins with a phishing message, leading you to a fraudulent website where your data is stolen. In these cases, ask yourself if it could be a SCAM:

SENDER	Who is the message coming from? Are you sure it's really them?
CONTENTS	Is it asking for details you wouldn't normally share? Anything suspicious?
ADDRESS	Is the address correct for your organisation? Are there any spelling mistakes?
MISTRUST	Is there anything about the email that rings alarm bells? Are you sure you can trust it?

Best Practises:

Ensure your devices & cards are protected

Always be cautious

Strengthen your passwords

Spear Phishing

BOXPHISH

Spear phishing is a targeted attack on a specific employee. These can be identified through:

- **Sense of urgency**: don't ever be rushed into doing anything online
- **Requests to click on links or open attachments**: beware of links in email even if they look genuine
- **Appeal to human greed or fear**: if it sounds too good to be true, it likely is
- **Requests for sensitive data**: don't give out sensitive information unless you have verified the identity of the person requesting

Key phrases to look out for:

- ➜ Urgent action required
- ➜ Updates required immediately
- ➜ Suspicious payments
- ➜ Your accounts will be deleted

Data Breaches

BOXPHISH

A data breach is a security violation that usually occurs in one of three main ways:

1. **Physical** – the physical theft of your private information, e.g., card receipts, physical files or hard drives
2. **Electronic** – information can be hacked electronically if it is not properly protected, encrypted or if you're using an unsecure network
3. **Skimming** – these data breaches occur when card payments are taken, capturing the card data via the magnetic stripe on the reverse

"data spills"

"data leaks"

What should you do?

1. Set strong credentials
2. Shred documents that are no longer required
3. Use strong passwords/passphrases
4. Report any lost devices immediately
5. Encrypt confidential information
6. Never allow your card out of your sight when making a payment

Online Self Defence

BOXPHISH

Why: if you spend time online, then you are at risk of a cyber-attack so you need to master the art of self defence to protect yourself

Most cybercriminals want to steal your private information or infect your device with malware. To prevent this, there are a number of things you can do:

- ➜ Set a strong password or passphrase
- ➜ Use Multi-Factor Authentication (MFA)
- ➜ Ensure your devices are up to date
- ➜ Run regular anti-virus scans

What to watch out for:

1. **Fraudulent websites** – check the address bar to ensure the details are genuine
2. **Phishing emails** – this is a very common tactic that cybercriminals use
3. **Pop-up adverts** – be cautious when clicking on things online, this could download malware onto your device

Online Shopping

BOXPHISH

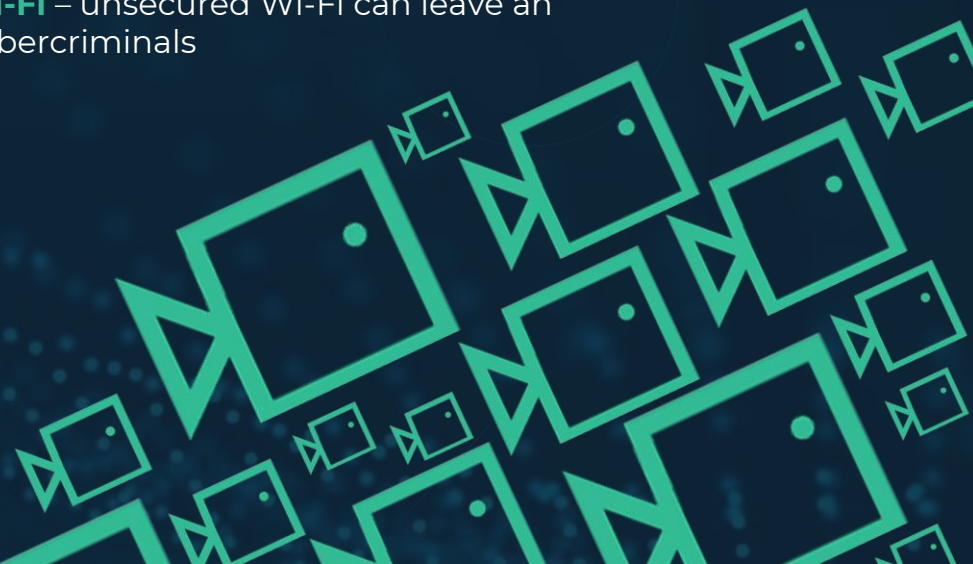
Cybercriminals will try to take advantage of your online shopping habits to trick shoppers out of their money and personal data.

The most common threats to watch out for :

- ✖ Phishing emails
- ✖ Fraudulent websites
- ✖ Spoofed applications

Best Practices:

1. **Watch out for impersonation** – and ensure the account is genuine
2. **Check the security of websites** – look for a padlock in the address bar, along with HTTPS://
3. **Research unknown brands** – check online reviews on third party websites
4. **Be protective of your data** – don't enter any information you think sounds unnecessary or suspicious
5. **Use a secure Wi-Fi** – unsecured Wi-Fi can leave an open door for cybercriminals



CEO Fraud

BOXPHISH

CEO fraud involves the **impersonation** of a senior executive in order **to divert payments** to a fraudulent bank account.

Cybercriminals carry out research online in order to make these attacks as believable as possible.

What to watch out for in emails:

1. **Time pressure and urgency** – e.g., if the sender is trying to get you to send something before the end of the day
2. **Out of office messages** – e.g., if an email comes from someone you're not expecting to hear from
3. **Persistent follow-up emails** – e.g., if the sender harasses you to complete the task in an unexpectedly short timeframe

These attacks cost UK businesses £121 billion each year

Personal Security

BOXPHISH

Why: cybercriminals are constantly looking for new ways to attack, so individuals need to be constantly developing new ways of protection

Remember: if you are online, you are vulnerable. Once a cybercriminal has managed to hack your device, they can see and track everything you do

Attacks can take place through:

- ➜ Your computer
- ➜ Public printers
- ➜ Mobile devices
- ➜ USBs and other removable media

Best Practises for Protection:

1. **Set strong passwords** and use multi-factor authentication (MFA) wherever possible
2. **Watch out for MFA bombing attacks** and treat unfamiliar requests with caution
3. **Keep software up to date** and run regular anti-virus scans
4. **Lock your devices** and your SIM cards to ensure your device is not vulnerable even when it is locked