

## Cyber Security Fundamentals for South Petherton Parish Council

### Why is it important?

Cyber security is the protection of physical technologies and devices, as well as online data, networks, applications and processes against criminal interference.

Strong cyber security practices work to reduce the risk and impact of cyber-attacks and prevent any external or internal damage to organisational assets.

*The techniques used by cyber attackers are developing at an alarming rate, resulting in growing concerns around the topic.*

Previously the most dangerous cyber attacks involved a more direct method of hacking into networks. Now, for the modern hacker it is more lucrative and often far simpler for criminals to take advantage of email communications and data held in the cloud.

To provide a better understanding of the types of cyber attacks an organisation may encounter, and the impact they can create, there are three common tactics;

**Phishing** Phishing attacks are most frequently conducted via an email, and will often involve impersonating a trusted source, such as a service provider. Phishing attacks often use urgency in their language to get the target to quickly click on a link, download an attachment or fill in login details – potentially resulting in account takeover, financial theft, data loss or compromised devices.

**Social engineering** Social engineering is a common technique used to gather confidential information. This can often be confused with phishing as it is frequently conducted via email and can involve impersonation of someone you are familiar with. However, the key difference is that social engineering attacks don't have to rely on malicious links or attachments, instead relying on manipulative behavioural tactics to trick the target into willingly sharing the desired information.

**Ransomware** Ransomware is a type of malware that infects a target's device and encrypts the data stored within it, making all of the user's data and documents completely unusable. Ransomware authors will leave a message to a target, offering them the unique decryption code in return for a ransom payment – however, it is not unheard of for organisations to pay this ransom and still never gain access back to their data.

Both social engineering and ransomware tactics were used in the M&S attacks in April 2025. Those responsible gained access to internal systems and obtained admin credentials by posing as known members of their IT helpdesk services. They proceeded to steal customer data and then successfully deploy their ransomware; encrypting their data. M&S have since revealed that as a result, this attack was costing an estimated £3.8m per day.

**Shoulder surfing** Shoulder surfing happens when someone watches you enter sensitive information, such as passwords or PINS, or credit card numbers. It can occur in public places like cafes, airports or even at work. Always be mindful of your surroundings and shield your screen or keypad when entering private information.

**Leaving devices unlocked** Leaving your computer or phone unlocked, even for a short time, gives anyone nearby the chance to access your data, email or work systems. Always lock your device when stepping away, no matter how briefly. A strong password, PIN, or biometric lock helps protect your information.

**Plugging in unknown USB's** Unknown USB drives can contain harmful software designed to steal data or damage your system. Even if one looks harmless or was found in the office, you should never plug it into your device unless you are certain of its source and safety.

**Letting someone use your device when logged in** Allowing someone to use your device while you're logged in puts your accounts, files and data at risk. Even trusted colleagues or friends could accidentally access sensitive information or install harmful software. If someone needs access, log out first or provide an alternative.

To understand how poor cyber security practices can rapidly escalate from seemingly harmless actions, lets think of a hypothetical case that could involve a Cllr. The role affords Cllrs access to highly confidential data making them a prime target for cyber criminals. A convincing email arrives in their inbox appearing to be from their clerk. The email informs them that updates have been made to the council Cllrs page of the website and instructs them to click through a link to see the updates. Interested in viewing the updates, the link is clicked and followed, leading to nothing but a blank page. The Cllr makes a mental note to tell the clerk the next time they speak. What they haven't realised though, is that simply clicking the link was enough for keylogger malware to be silently installed on their computer, allowing the attacker to monitor everything they type – including login details. If they had read the senders email address carefully, they would have noticed a misspelling or inaccuracy in the domain name, which would indicate the email was not legitimate.

### What does good cyber security look like?

Cyber security best practices are often thought to only involve an organisations IT department – for example by implementing virus protections for all users' devices and overseeing backup solutions for data. However, modern cyber attacks are more

frequently being targeted at individuals rather than the networks and because of this there are a range of cyber security best practices that should be followed by all users. Below are some best practices to keep in mind in your daily activities.

**Protect your data** Data protection is much more than just creating copies of important files and preventing hacking attempts. Even something as simple as sharing a photo on social media, not realising that a computer screen with an open file can be seen in the background could be enough to result in a damaging data breach.

**Be cautious with emails** Email attacks can be extremely subtle and hard to spot in today's threat landscape. The most important things to keep in mind are; carefully check email domains, never open attachments from new senders, and avoid clicking unknown website links. If you are ever unsure of whether a link or email domain is trusted or not, contact someone before taking any actions.

**Strengthen your accounts** Account takeover is a rising threat due to the amount of data now stored in cloud applications. To avoid falling victim, make sure to set strong and unique passwords for all of your accounts, and set up two-factor authentication wherever possible.