Un Llais Cymru
One Voice Wales

Community & Town Councils Digital Guidance

Digital Security Tips for Community and Town Councils in Wales

January 2025

Contents

Introduction 3
Device Security 3
Always Enable Password Protection 3
Track, Lock, or Wipe Lost Devices 3
Update All Devices Regularly 3
Keep Apps Updated 3
Avoid Insecure Wi-Fi 4
Backing Up Your Data 4
Use Caution with Unknown Files 5
Using Passwords and PINs to Protect Your Data 5
Avoiding Phishing Attacks 6
Version History 7

Introduction

As Community and Town councils in Wales increasingly rely on digital technology to manage their affairs, it becomes essential to protect your data and Information Technology (IT) systems from cyber threats. This guide provides simple advice to help you safeguard your council's information, assets, and reputation from common cyber attacks.

Device Security

Mobile devices require specific consideration. Here are some tips:

Always Enable Password Protection

Use complex passwords or PINs for access to devices. Enable fingerprint or camera recognition if available but note that face recognition may not be as secure as other methods.

Track, Lock, or Wipe Lost Devices

Modern operating systems such as Android, Apple IoS and Windows 11 provide inbuilt tools to track devices. These often provide the ability to lock the device remotely or to erase everything if the device is lost or stolen.

Update All Devices Regularly

All mobile devices must be kept up to date with the latest security patches. This is typically the default behaviour for all reasonably current devices. Support and updates may cease for devices after 3-7 years. Devices which are no longer provided with security updates and patches should be replaced.

Keep Apps Updated

Regularly update all installed apps. Monitor installed applications to ensure they are receiving regular updates. Old applications which are no longer supported by their providers are at risk of security compromise and should be removed and an alternative found.

Avoid Insecure Wi-Fi

Any use of Wi-Fi Services in public locations such as cafes, public Transport or community buildings should be secured via a Virtual Private Network (VPN). A VPN is a tool that helps keep your internet connection safe and private. When you use a VPN, your online activities are hidden from others, making it harder for anyone to see what you are doing or steal your information.

You can use a VPN on different devices like mobile phones, tablets, and laptops. Here's how:

- Mobile Phones: You can download and install a VPN app from your app store. Once installed, you can turn it on, and it will protect your internet connection.
- Tablets: Just like on mobile phones, you can find a VPN app in the app store, download it, and turn it on to keep your browsing safe.
- Laptops: For laptops, you can install a VPN program from the internet. After installation, you can connect to the VPN to secure your online activities.

Using a VPN is a simple way to make sure your internet use remains private and protected when you are using public Wi-Fi.

Backing Up Your Data

Ensuring the continuity of your council's operations requires regular data backups. Here are five key considerations:

Identify Critical Data

Determine which data is essential for your council’s functions. This typically includes legal documents and correspondence.

Separate Backup Storage

Keep backups on separate devices and in a different location. This can prevent loss from ransomware or other attacks but also from events such as fire or floods.

Use Cloud Storage

Cloud storage keeps your data safe offsite and offers high availability, often at minimal cost. Refer to separate One Voice Wales guidance on Cloud Storage

Automate Backups

Automated backups save time and ensure your most recent data is always safe.

Protecting Your Organization from Malware

Malware, short for "malicious software," refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware can take various forms. It infiltrates systems to steal, encrypt, or delete data, alter or hijack core functions, and monitor users' activities without their knowledge.

To prevent malware damage, follow these steps:

Install Antivirus Software

Ensure all computers have antivirus software installed and enabled.

Control Use of USB Drives

Limit the use of USB drives to prevent malware infections. Encourage file transfer via email or cloud storage.

Use Caution with Unknown Files

Be cautious with any files which are sent to you via email, especially if they are not from a known and trusted source

Using Passwords and PINs to Protect Your Data

Passwords are crucial for protecting your devices and data:

Enable Password Protection

Set screen lock passwords or other authentication methods on all devices.

Use Two-Factor Authentication

Two-factor authentication (2FA) is a way to add an extra layer of security to your online accounts. It requires not only a password but also a second form of verification, such as a code sent to your phone or an authentication app. This makes it significantly harder for unauthorized users to gain access, even if they have your password.

Enable two-factor authentication where it is available.

Avoid Predictable Passwords

Choose passwords that are easy to remember but hard to guess. Avoid common passwords.

Manage Passwords

Consider using password managers. Password managers are tools that store all your passwords in one place. They help you keep your passwords safe and organize

them easily. When you need a password, the manager will fill it in for you, so you don't have to remember all of them. It can also create strong passwords for you, making it harder for others to guess them.

Change Default Passwords

Always change default passwords on any new devices before distributing them to staff.

Avoiding Phishing Attacks

Phishing is a type of scam where someone tries to trick you into sharing personal information, such as passwords or bank details. This usually happens through fake emails or messages that look like they come from a trusted source. The goal is to get you to click on a link or open an attachment, which can then lead to your information being stolen. It's important to be cautious and verify the source before responding to such requests.

Phishing attacks can trick users into revealing sensitive information. Here are some precautions:

Restrict Access

Give staff the lowest level of access to any sensitive information which is necessary to perform their roles.

Understand Normal Operations

Ensure staff recognize usual procedures to spot unusual requests.

Check for Phishing Signs

Provide training for staff to recognize typical indicators of phishing attacks, such as grammatical errors or requests that convey a sense of urgency.

Report Attacks

Report suspected phishing attacks immediately and avoid feeling guilty or upset for falling victim.

Conclusion

By implementing these practical and cost-effective cyber security measures, community councils in Wales can significantly reduce their risk of falling victim to cyber attacks.

These tips are based on guidance from the National Cyber Security Centre. For more detailed guidance, visit the National Cyber Security Centre's website www.ncsc.gov.uk.

Version History

	Date	Issuer	Reason	Review Date
V1	15/02/25	Justin Horrell	Initial Version	15/02/26

Ariennir gan
Lywodraeth Cymru
Funded by
Welsh Government