Cyber Awareness

A Practical Guide for Individuals

Learn how to protect yourself online with straightforward tips and practical advice to enhance your safety and security.

DORSET POLICE

A safe county for everyone

Dorset Police Cyber Crime Unit

Contents

Foreword

In today's digital landscape, the internet presents countless opportunities for connection, learning, and entertainment. However, navigating this expansive online environment can often feel daunting.

This booklet is crafted to equip you with the knowledge and tools necessary to navigate the internet safely and with confidence.
Within these pages, you will discover clear tips and practical advice designed to meet your needs. From recognising common scams to safeguarding your personal information, our goal is to help you harness the benefits of technology while minimising potential risks.

While this guide cannot guarantee complete protection from all cyber threats, it highlights straightforward methods to enhance your online safety and secure your personal information.

As you delve into this booklet, remember that you are not alone. Numerous resources and communities are available to support you on your online journey. By staying informed and vigilant, you can engage with the digital world securely and comfortably.

For additional information, please refer to the 'Find Out More' section at the end of the booklet.

Hannah Bird
Cyber Crime Protect and Prevention Officer
Dorset Police Digital Capabilities Unit

Understanding and Recognising Cyber Threats

In an increasingly connected world, understanding cyber threats is essential for everyone. Cyber threats come in many forms and can impact individuals, businesses, and organisations alike. By recognising these threats and understanding how they operate, you can take proactive steps to protect yourself and your information.

This section will explore common types of cyber threats and provide practical tips for safeguarding your online presence.

Tip 1: **Be Aware of Phishing Attempts**

Phishing is a common cyber threat where attackers attempt to trick you into revealing personal information through emails, text messages, or phone calls that seem to come from trustworthy sources, such as banks or government agencies.

These messages often ask for sensitive details or prompt you to click on harmful links.

To protect yourself:

- Carefully check the sender's email address for any inconsistencies.
- Look for signs of poor grammar or unusual wording in the message.
- Avoid clicking on links or downloading attachments unless you are certain they are safe. Instead, navigate to official websites directly.

Tip 2: **Understand Malware and its Risks**

Malware is a term for software specifically designed to harm your devices or steal your data. This includes viruses and spyware. Once malware infiltrates your system, it can lead to data breaches, file corruption, or loss of access to your device.

To defend against malware:

- Install reputable antivirus software and keep it updated to detect and remove threats.
- Be cautious about downloading software from the internet; always use trusted sources.
- Refrain from clicking on pop-up ads or unfamiliar links, as these can often lead to malware infections.

Using passwords to protect your data

Your smartphones, tablets, and computers hold a lot of important personal information, such as photos, messages, and details of your online accounts. It's essential to keep this information safe from anyone who shouldn't have access.

When used correctly, passwords help ensure that only you can access your information, keeping it secure and private.

Tip 1:
Use three random words

A good way to make your password difficult to crack is by combining three random words (for example apple.nemo.hotel). To make the password stronger consider adding numbers, uppercase letters, and special characters.

Avoid using easily guessed information like pets' names, birthdays, or common words. Instead, consider using a passphrase made up of three random words to create a strong and memorable password.

Tip 2:
Don't use the same password everywhere

It's important to have a unique password for each of your accounts. If someone gains access to one password, they could potentially use it to access your other accounts as well. By creating different passwords, you help ensure that if one account is compromised, your other personal information remains safe. This practice adds an extra layer of security, protecting your sensitive data from unauthorised access.

Tip 3:
Use a Password Manager

A password manager stores passwords safely for you, meaning that you can have unique passwords for each service as you won't need to remember them.

Most password managers are designed to be user-friendly. Tutorials and customer support are available to help new users get started, so even if you haven't thought about using one before, you should try it.

Understanding Two-Step Verification (2SV)

Two-Step Verification, or Two-Factor Authentication is an important security feature that adds an extra layer of protection to your online accounts. By requiring two forms of verification before allowing access, 2SV helps keep your personal information safe, even if someone gets hold of your password.

How does Two-Step Verification work?

When you enable 2SV on an account, you'll need to provide two types of information to log in:

1. **Something You Know**: This is usually your password.
2. **Something You Have**: This could be a code sent to your mobile phone, a code generated by an authentication app, or even a physical security key.

This means that even if someone else knows your password, they still cannot access your account without the second form of verification.

Ensure that the phone number or email address associated with your account is current. If you need to recover access, having up-to-date information is crucial.

Tip 1:
Enable 2SV on all important accounts

Turn on 2SV for your email, banking, and any other accounts that hold sensitive information. This adds an extra layer of security to your most valuable accounts. 2SV if often enabled in the Security or Privacy Settings.

Tip 2:
Choose a method that works for you

When setting up 2SV, you'll usually have a few options for how to receive your verification codes. You can choose to get codes via text message, an email, or an authentication app. Pick the method that you find easiest to use and remember.

Tip 3:
Beware of phishing/scam attempts

Be aware of emails or messages that ask for your 2SV codes. Legitimate companies will never ask for this information directly. If you receive such a request, do not respond and report it.

Scam Messages & Calls - Phishing

Scam messages and calls are deceptive attempts to trick you into giving away personal information or money. These can come in the form of emails, texts, or phone calls that look and sound legitimate.

These scam messages are often referred to as phishing. Phishing is when someone pretends to be a trustworthy source in order to steal your information. If you are unsure who is contacting you, do not give out any personal information. It's always better to be safe!

Tip 1:
Look out for urgent language

Beware of urgent language: Scammers often try to create a sense of urgency to prompt you to act quickly without thinking. If you feel pressured such as with a specific deadline, the language used, or are made to feel anxious, take a step back and verify the sender/caller before proceeding.

It is really important to slow down and take your time when you receive unexpected messages/calls. Question what the sender/caller is asking for, and why they are contacting you.

Tip 2:
Verify requests with trusted sources

If you get a message or call asking for personal information, it's a good idea to hang up or ignore the message. Then, contact the organisation directly using a trusted phone number to confirm if it's real.

Tip 3:
Avoid clicking unknown links or attachments

If you receive a message with links or attachments you weren't expecting, it's best to avoid clicking on them. Instead, you can visit the official website directly to check.

Tip 4:
Check the sender's information

Take a moment to look at the sender's email address or phone number. Scammers often use addresses or numbers that look similar to real companies but may have small differences.

Also be aware of generic greetings. Legitimate organisations usually personalise their messages.

Protecting yourself on Social Media

Social media is a great way to connect with friends and family, share experiences, and stay informed. However, it's important to remember that not everyone online has good intentions. Protecting your personal information and privacy on social media can help you enjoy these platforms safely. Here are some simple tips to keep your accounts secure.

Tip 1:
Adjust your privacy settings

Review the privacy settings on your social media accounts. Make sure you limit who can see your posts and personal information. You can often choose to share your profile only with friends or specific groups, which helps keep your information more secure.

You can usually adjust your privacy settings by navigating to the "**Settings**" or "**Privacy**" section on your social media account.

Tip 2:
Be careful what information you share

Think twice before posting personal information, such as your address, phone number, or details about your daily routine. Scammers can use this information to target you. Instead, share general updates that don't give away too much about your location or personal life.

Tip 3:
Verify friend requests

Only accept friend requests from people you know personally. Scammers often create fake profiles to connect with unsuspecting users. If you receive a request from someone you don't recognise, it's best to ignore or block it.

Tip 4:
Watch out for suspicious messages

Be wary of messages from friends or connections that seem unusual, especially if they ask for money or personal information. It's possible that their account has been hacked. If you receive a strange message, consider contacting the person through a different method to verify.

Safe Online Banking

Online banking makes managing your finances easier than ever, but it's important to stay vigilant to protect your personal information. With the rise of cyber threats, knowing how to bank safely online can help you safeguard your money and account details. Here are some simple tips to keep your online banking experience secure.

Tip 1:
Use strong & complex passwords

Create strong passwords that combine upper- and lower-case letters, numbers, and special characters. Avoid using the same password for multiple accounts. A unique password for your banking account adds an extra layer of security.

Tip 2:
Monitor your bank accounts regularly

Regularly check your bank statements and online account activity for any suspicious transactions. If you notice anything unusual, report it to your bank immediately. Prompt reporting can help minimise potential losses.

Tip 3:
Enable Two-Step Verification

Whenever possible, enable Two-Step Verification (2SV) on your banking accounts. This is an extra security step that helps protect your account. With 2SV, after you enter your password, you'll also need to provide a second piece of information to log in. This usually comes in the form of a code sent to your mobile phone via text message or generated by a special app.

For example, once you enter your password, you might receive a text with a code that you need to type in to gain access. This means that even if someone else gets your password, they won't be able to access your account without that code. It adds an important layer of protection and helps ensure that only you can access your banking information.

Tip 4:
Log out when you are finished

Always log out of your online banking session when you're finished, especially if you're using a shared or public computer. This helps prevent unauthorised access to your account.

Making Purchases Online

Shopping online offers convenience, but it also comes with potential risks. Understanding how to protect your financial information while making purchases is essential. Here are some top tips to help you shop safely online:

Tip 1:
Use a credit card for payments

Use a credit card for payments (if you have one). Many of these protect online purchases as part of the Consumer Credit Act.
Debit card payments offer less protection, but you might be able to make a claim for a refund under a voluntary scheme called 'chargeback'.
If you use payment services such as PayPal, Apple Pay or Google Pay, check their 'terms & conditions' to see what cover they provide. Never pay by direct bank transfer.

Tip 2:
Only give required details on checkout

When making your payment, only fill in the mandatory details (often marked with an asterisk) such as your address. There's often an option to 'check out as a guest', which means you don't need to create an account to complete the payment.

Tip 3:
Check the shop is legitimate

You can research online shops to check they're legitimate, particularly if it's a store you've not used before. Use consumer websites, or reviews from people (or organisations) that you trust.

If you're unsure about a link you receive, don't click on it. Instead you can:

- Type the official website address of the organisation (if you know it) directly into the browser's address bar
- Search for the organisation, and then take time to read the entries on the results page (don't just click the top item)

Tip 4:
If something goes wrong, report it

If you've been tricked into making a payment, tell your bank and report it as a crime to Report Fraud.

If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it. Always contact your bank directly using the official website or phone number.

Safe Online Browsing

In an increasingly digital world, safe online browsing is essential to protect your personal information and maintain your privacy. With various threats lurking on the internet, such as malware, phishing attacks, and data breaches, adopting secure browsing habits is crucial. Here are some top tips to help you browse the web safely and securely.

Tip 1:
Beware of public Wi-Fi

Public Wi-Fi networks can be convenient, but they often lack proper security, making it easier for cybercriminals to intercept your data. Avoid accessing sensitive information, such as online banking, while connected to public networks. If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your connection and protect your data from prying eyes.

Tip 2:
Be cautious with pop-ups

Avoid clicking on pop-up ads or links that seem suspicious. Many pop-ups can lead to malicious websites or install malware on your device. Use a pop-up blocker to enhance your security.

Information:
Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) encrypts your internet connection, making it more secure and protecting your data from prying eyes.

This is especially important when using public Wi-Fi networks, as a VPN can help safeguard your personal information from cybercriminals.

By masking your IP address, a VPN protects your data from hackers, particularly on public Wi-Fi networks where security risks are higher. This encryption also keeps your browsing activities private, preventing third parties from tracking your online behaviour.

When selecting a VPN, choose a reputable provider that prioritises user privacy and offers robust security features. Using a VPN is an effective way to ensure safer and more secure browsing, giving you peace of mind while online.

Avoiding Romance Fraud

Dating fraud is when someone uses a fake identity to build a relationship with you, often with the intention of stealing money or personal information. These fraudsters can be very convincing, making it important to know how to recognise the signs and protect yourself while dating online or even in person.

Tip 1:

Be aware of the warning signs

Being aware of the warning signs of romance fraud can protect you from falling victim:

Reluctance to meet face-to-face or video call - Because they are using a fake online identity they often refuse to meet face-to-face or on a video call. They will create excuses to avoid doing so.

They ask for money - For professional scammers their main objective will be getting you to give them money - this may be a one off payment or a number of smaller payments.

They get serious, fast - Often the relationship gets romantic very quickly. The individual falls hard for you and they want to move quickly.

They want the relationship to remain a secret - They will want to isolate their victim, to prevent them discussing the relationship with others, as other people may see warning signs the victim cannot.

Tip 2:

Avoid sharing personal information too soon

Keep sensitive information like your address or financial details private until you know the person well. Scammers may use this information to manipulate you, so be cautious about what you disclose.

Tip 3:

Look for inconsistencies

Pay attention to details in conversations. If someone's story changes or doesn't add up, it could be a sign they're not truthful. Trust your instincts—if something feels off, ask questions.

Tip 4:

Trust your instincts

If something feels off or makes you uncomfortable, listen to your gut. Your instincts can help protect you. If you have doubts, it's okay to end the conversation or block the person.

Data Protection & Privacy

In our digital age, protecting personal data is more crucial than ever. Personal data includes any information that can identify you, such as your name, address, phone number, email, and even financial details. With increasing cyber threats, it's essential to understand how to safeguard this information to maintain your privacy and security online. Here are some top tips to help you protect your data:

Tip 1: **Install Anti-Virus Software**

Antivirus software is essential for protecting your devices from malware, including viruses, worms, and ransomware. It works by scanning files and applications in real-time to block threats before they can cause harm.

Look for reputable antivirus programs that offer features like scheduled scans, automatic updates, and additional security measures such as firewalls and phishing protection. Investing in reliable antivirus software helps safeguard your personal data and reduces the risk of falling victim to cyber threats. Remember, even if you use a Mac, it's important to have antivirus protection, as no system is completely immune to attacks.

Tip 2: **Enable your Firewall**

Firewalls act as a barrier between your device and potential threats from the internet. Ensure that your device's firewall is enabled and configured correctly. This helps block unauthorised access and protects your data from external attacks.

To ensure your firewall is enabled, go to your device's settings: for Windows, navigate to "**Control Panel**" > "**System and Security**" > "**Windows Defender Firewall**." On a Mac, go to "**System Preferences**" > "**Security & Privacy**" > "**Firewall**." Make sure the firewall is turned on to help protect your personal data from external attacks.

Tip 3: **Limit personal information you share online**

Limit the amount of personal information you share online, especially on social media platforms. Review your privacy settings and adjust them to restrict who can see your information. Avoid sharing sensitive details unless absolutely necessary.

Device GPS Location Services

Many devices use GPS (Global Positioning Service), a satellite-based service that tracks your location in real time. GPS is essential for navigation, fitness tracking, and finding nearby services. However, being mindful of which apps and services have access to your location helps you maintain control over your privacy and security.

Tip 1:
Review your Phone's Location Settings

Take your time to review and adjust your phone's location settings. Disable GPS when it's not needed to reduce unnecessary location sharing.

Many smartphones also allow you to limit location access to "while using the app", preventing apps from tracking you in the background. This gives you greater control over when and how your location is shared.

Tip 2:
Use Biometrics to Lock your Device

Secure your phone with biometric locks, such as fingerprint or facial recognition, to prevent unauthorised access to your location data if your device is lost or stolen.

Tip 3:
Manage Apps that Share Location

Regularly check the permissions granted to apps. Go to your phone's settings and review which apps can access your location. Revoke permissions for apps that do not need it, and uninstall any that you no longer use.

Some apps, like map apps, may have timeline features that show your recent locations or activity. Check these settings and clear your location history if you do not want is saved.

Choose apps from trusted developers and avoid installing apps from unknown sources that might misuse your data.

Tip 4:
Turn Off Location Sharing with Others

Many devices and apps allow you to share your real-time location with friends and family. Whilst this might be useful, make sure to regularly review who has access. Stop sharing your location if it is no longer necessary, and double-check your settings to ensure old permissions haven't been looked.

Final Recap - Essential Cyber Security Tips

Use strong & complex passwords

Create long passwords that include a mixture of upper and lower case letters, numbers, and special characters. Pets names, dates of birth, and common words don't make for good passwords. We recommend using a passphrase made up of three random words. Also, ensure devices are secured with a password or passcode.

Enable Two-Step Verification

Enhance your account security by enabling 2SV. This requires an additional verification step, such as a code sent to your phone or authentication app, whenever you log in.

Regularly check your privacy settings

Regularly check the privacy settings on your social media and online accounts. Adjust them to ensure that only trusted contacts can view your personal information.

Be mindful of what personal information you share online

Be mindful of the information you share on social media and public forums. Where you go to school, or work, or on holiday... this information is more valuable than some people think.

Backup important data & information

Creating backups of important data (e.g., photos and videos) is crucial. A backup allows you to restore information if a device or account is lost or compromised.

Ensure devices are regularly updated

Make sure you install software updates as soon as they become available. They often contain important security fixes.

Beware of public Wi-Fi

Whilst it's absolutely fine for casual browsing, free Wi-Fi is not secure. Sensitive data like passwords and banking details can be spied upon. Use your mobile data, or a Virtual Private Network (VPN) instead.

Find Out More

Staying safe online can sometimes feel overwhelming, but you don't have to navigate it alone. Below are some useful links and resources that provide additional information and support on various topics related to online safety. Whether you're looking for guidance on protecting your personal information or understanding the latest scams, these resources can help you stay informed and secure.

WWW.DORSET.POLICE.UK/CYBER

The Dorset Police Cyber Crime Unit homepage contains useful information and links to resources to help keep you safe online. You can also request tailored cyber awareness sessions covering a variety of topics.

WWW.NCSC.GOV.UK/CYBERAWARE

The National Cyber Security Centre (NCSC) is part of GCHQ (Government Communications Headquarters), the government's intelligence and security organisation. As such, they are well placed to provide impartial security guidance. Their Cyber Aware campaign gives straightforward advice to help people secure their accounts and defend against some of the more prominent forms of cybercrime.

WWW.REPORTFRAUD.POLICE.UK

Report Fraud is the UK's national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. Should you fall victim, you should report to Report Fraud by visiting their website or by calling 0300 123 2040.

WWW.STOPTHINKFRAUD.CAMPAIGN.GOV.UK

Stop, Think Fraud is a National campaign offering straightforward, impartial advice that helps prevent email, phone-based, and online fraud. Stop, Think Fraud is brought to you by the UK Government in partnership with City of London Police, the National Cyber Security Centre, and the National Crime Agency.

Other Important Contacts:

If you believe you may be a victim of fraud, you can contact your bank on **159**.

You can report phishing scams by forwarding the email to **report@phishing.gov.uk** or by forwarding an SMS to **7726**.