**Cyber Security Awareness – Advice for Individuals and Businesses**

(notes to accompany the PowerPoint presentation)

**Slide 2: Presentation Contents**

This presentation will show you the importance of Cyber Security.

The aim is to provide you with information about some of the common threats; give you tips and advice on how to stay safe and secure online and make you aware of how you can protect your privacy, while making the most of the benefits the internet has to offer.

**Slide 3: Why is Cyber Awareness Important?**

* 50% of all crime is linked to the internet, although it’s not all Cyber Fraud. Both businesses and individuals are affected.
* On average, it has been found that only 13% of employees are trained in Cyber Security Awareness (Summer 2018)
* Employees are a critical line of defence when it comes to protecting against cyber attacks
* By 2030, the aim is that government contracts will only go to Cyber Essentials Customers. The National Cyber Security Centre’s Cyber Essentials website gives advice about cyber security for organisations; shows how to obtain a certificate for cyber security and provides a searchable database of companies who hold a Cyber Essentials Certificate issued in the last 12 months
* It’s **very important** that, if you are a victim of cybercrime, you must report it

**Slide 4: How Cyber Crime affects the UK**

* The **National Fraud & Cyber Crime Reporting Centre’s Action Fraud** website offers 24/7 live cyber reporting for businesses
  + Examples of a live cyber-attack:
    - Cyber criminals have accessed a company network and stolen personal information about their customers and are demanding payment for its safe return. Also known as hacking extortion.
    - Your website is being flooded with traffic – customers are not able to access it as a result. This is called a **distributed denial of service** (DDOS) attack.
  + **Action Fraud** gives advice for protection against cyber fraud and how to report fraud
  + Anyone can report cyber fraud: Individuals, Small Businesses, Large Corporations, Charities, Police Officers…

**Slide 5: Who is doing the hacking?**

Computer hacking is broadly defined as intentionally accessing a computer or computer network without authorization or exceeding authorization.

**Slide 6: Hacking**

* One of the most common and main reasons for hacking is for financial gain. This affects both businesses and individuals.
* Politically motivated hackers: Like to ‘show off’ their skills, they are interested in fame and status, but not financial gain usually. They are often motivated by ideology. Their targets are mostly government sites, but organisations can also be affected.
* A **hacktivist** (hacking activist), combines strong beliefs (political/ethical) and technical knowledge to attack a company or website which represents opposing views. The aim can be to:
  + Disrupt the website service
  + Cause loss of revenue and/or reputation
  + Name & shame individuals who work for the organisation
  + Display a visible and highly controversial message on the website’s home page
* **Pen Testing** (penetration test): Performed by a qualified third party to conduct an authorised, simulated attack on a business’s computer network to evaluate the security of the system. This service enables companies to identify any weaknesses in their cyber security, as well as their strengths. It is like an external audit and is used for assurance, rather than a primary method for identifying vulnerabilities.
* Thousands of Police Officers are receiving specialist cybersecurity training, to enable them to investigate cybercrime. Police have been given power to hack into private computers, with the justification that this type of surveillance is needed for tracking criminal activity on the internet.
* **Insider hacking** is the unauthorised or accidental misuse of the organisation’s systems or data, by employees.
* A business may hack into its competitor’s system to obtain client information, allowing the first company to contact potential new customers. (It is not legal, but it happens).

**Slide 7: Common Threats – Ransomware**

* Ransomware is a form of malware in which the data, or screen, on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.
* Ransomware infects your device, or network, through:
  + Malicious email attachment
  + Malicious link in an email, SMS (text messages), social networking site or other websites
  + Visiting a corrupt site
  + Opening infected files
  + Opening corrupt macros
  + Connecting corrupt USB devices, or inserting corrupt CDs/DVDs. (Beware of inserting a device into your computer if it has been given to you by another person – even a friend – their security may not be as good as yours and the device could contain an unknown virus)
* Ransomware does not usually access data, but it prevents the user gaining access to the information

**Slide 8: Ransomware** – *this slide shows an example of a ransomware attack*

* Payment is requested/collected in digital or virtual currency (*e.g. Bitcoin*)
* Bitcoin is a virtual cryptocurrency based on a secure digital ledger system called a ‘blockchain’. Transactions are made between digital wallets stored on computers and are anonymous so cannot be traced to individuals. It is also not controlled by any central bank or organisation. There are lots of types of cryptocurrency, bitcoin is just one.
* You will be given a limited time to pay (this increases your anxiety and desire to rectify the situation, so it may affect the actions you take).
* It is estimated that 1 in 5 companies/individuals don’t get their information back (this is probably a conservative estimate), or they only get part of the data back and must pay more to get the rest.

**Slide 9: How to tackle Ransomware**

* Always ensure you back-up (copy) your data to a separate device, which is kept separate from your computer, so you can recover it without paying the criminals. Large businesses and organisations often keep their backed-up data at a totally separate site, away from the business premises
* Regularly update your Anti-Virus software, to make sure you have the most recent tools to tackle or prevent new viruses from attacking your computer or network. You can often set this to be done automatically. Download security updates from all your software vendors and Microsoft for your operating system continually; again, this can often be set to update automatically.
* Always take care when opening attachments or clicking on links in emails or SMS (text messages). Even if the email has come from a person known to you; attachments can be added during transit without the sender knowing. If you are unsure, contact the sender to ask if they have sent an attachment before opening it (using a new email, or by phone).

**Slide 10: Phishing** – *the slide shows an example*

**Phishing**:

* Via email

**Smishing**:

* Via SMS (text messages)

**Vishing**

* Via phone calls

All of these are used to manipulate people into disclosing information or taking various actions which lead to the victim being defrauded.

**Examples of phishing**:

* Your bank, emailing or phoning to inform you there is a problem or irregularity with your account and asking you to click on a link (or ring a specified number) to contact them
* A retailer, offering ‘vouchers or gift cards’
* A technology provider asking you to ‘validate your account’
* HMRC (Inland Revenue) informing you that you are ‘due a tax refund’

Things phishing messages have in common:

* They may instruct you to follow a link to a website, or ring a specified number
* They play on human emotions and/or needs: trust, safety, fear of losing money, getting something for nothing etc.
* There is generally an implication that your response is urgent, to avoid an issue or to take advantage of an offer.

**Look at the image on the slide for things to look out for and be aware of**.

**Please Note**: Banks and Credit Card Companies will not pay out if you have given information to the wrong company, through phishing of any kind. (Summer 2018: *Financial institutions are looking at changing these rules, but critics say the new measures may not be enough*)

**Slide 11: What to look out for when shopping on the internet?**

* Be aware: **https://** shows the web page is secure & your information will be encrypted, but it **doesn’t** prove the website is authentic.
* Using a credit card or Pay Pal to pay will provide extra protection for your money

**Slide 12: Online Banking**

Banking online is convenient and safe, providing you protect your password and personal details

**Safe Banking**:

* Don’t be tricked by phishing emails or vishing phone calls into disclosing passwords/pins/other confidential details
  + Banks will never ask for this information by email or on the phone
  + Any communication from banks or other financial institutions will use your name (not Sir or Madam; or Dear Customer); they will usually contain another verification, such as part of your account number or card number
  + If you use internet banking, some banks will now send you an email advising you to log in to your account to see a new message (they will not include a link to the internet banking site)
* Don’t follow links in an email or text message to financial websites
  + Always enter the URL in the browser or use a bookmark you have saved yourself, to access your bank account, and look for https:// and the padlock symbol in the address bar
* Hover the mouse over a link in a message, to display the URL for the website it will connect you to
* Always use a **secure** internet connection to connect to your bank
* Always use a unique & strong password for each financial institution and not the same for any other website you visit
* Ensure you have effective and up to date antivirus and antispyware software and firewall running
  + Protects against identity theft through viruses or spyware
  + Protects against malware on your device impersonating you and sending information to your bank which is not correct e.g. changing the recipient of a payment
* Switch off paper statements and check your online statements regularly
* Get the latest Windows updates from Microsoft (this can be automated).

**Bank Mandate Fraud**:

Serious organised crime groups are profiting from fraudulent schemes that target organisations and individuals.

Bank mandate fraud is frequently used by these groups as it carries low risk and potentially high rewards.

Examples of bank mandate fraud:

* **Online Bank Account**: Hacked into by a fraudster and monthly payment details are altered, so the money is transferred to the fraudster's account not the correct recipient
* **Individual Contact**: Someone contacts you, pretending to be from an organisation you have a standing order with, requesting that you change the standing order to reflect a change in their banking. The funds will go to the fraudster, instead of the genuine recipient. (Always contact the company, using a known email address or telephone number to check the request is genuine. You can advise them of the contact/information you have received if it has not come from them)
* **Business Contact**: Someone, pretending to be one of your suppliers, informs you they have changed their bank details and request a corresponding change to an existing direct debit. As a result, the bank mandate is amended to send funds to the fraudster's account provided. (See the point above for how you can protect against this)

All banks have online security information on their websites, including information about known frauds. They constantly review their security to protect you during online banking processes.

**Slide 13**

The URL (website address) reveals it is not the NatWest website

* Often the URL will be like what you might expect to see, but there may be a spelling mistake

**Slide 14: SMS from Banks**

* Financial institutions will **not** ask you to log in via a link
* Always access your online banking in the usual way (typing the URL in yourself, or using a bookmark you created), to see if there are any messages on your account
* Banks often have sites or email addresses where you can report SPAM.
* Don’t just delete a SPAM email; mark it as SPAM so your email provider will block future emails from the same sender.

**Slide 15**

* Here you can see the top 2 messages are authentic, because they are only advising the statement is ready to view – there isn’t a link to access the site. They also displayed the last 4 digits of the card as extra verification.
* The third message is fake, because there is a ‘link to your online banking’. Financial institutions don’t send messages like this one.

This is a ‘spoof’. Fraudsters use specialist software which alters the sender ID, so that it appears with the name of a bank (or another selected sender). Consequently, the text may be included within an existing text message thread on the recipient’s phone - making it seem genuine.

**Slide 16: Public Wi-Fi**

* Unauthorised people can intercept anything you are doing online if the connection is not encrypted, including:
  + Capture passwords and/or usernames
  + Read emails and intercept the data you send across the unencrypted Wi-Fi connection
* Someone may set up a spoof hotspot (fake Wi-Fi), to fool you into thinking that it is a legitimate one. So, they can see everything you are doing on the internet
* With an encrypted connection, you will be required to enter a ‘**key**’
* If you are not asked for a key and you can just log in, the operator will know you are online in the café, hotel or pub and there will probably not be any encryption.
  + Hotels may share your information with others
  + **Never** send or receive any personal information on a Public Wi-Fi connection
  + **Don’t** do online banking or shopping
  + Business people, wishing to access their corporate network should use a secure, encrypted Virtual Private Network (**VPN**)

A VPN is a secure encrypted connection between a computer and network on the internet, for example: an employee working from home and connecting securely to a company network.

* **Lock down Social Media**
  + Social networking is good for personal users (allowing people to stay in touch with friends and relatives) and valuable for businesses, but there are risks. To safeguard against these:
    - Use strong and unique passwords
    - Your username should not include personal information e.g. joe\_glasgow or jane\_Liverpool
    - Limit the personal information you include in your profile or in posts
    - Keep your profile closed
    - Set up a separate email account to register/receive emails. So, if you close your social media page, you can stop using the email too without having to inform your other contacts
    - Be **very wary** of publishing pictures of yourself or others; particularly children
    - Be aware of what friends post about you or reply to your posts…. their privacy settings may not be so tight as yours, or they may have accepted or extended invitations to people you don’t know
    - Don’t post holiday dates or photos while you are away. Burglars research social networking sites to gain this information. Insurance companies will not pay out, if you have advertised online that you are away
    - New job? Remember, many companies routinely view current or prospective employees’ social networking pages, so be careful what you post and what your friends say
    - Learn how to use the privacy features, to restrict strangers, and be guarded about who you allow to join your network
    - Be on your guard about phishing scams, fake friends and posts inviting you to visit other pages or sites; they may not be authentic sites, or you may pick up a virus
    - Ensure you have effective and updated antivirus and antispyware software and firewall running before you go online.
  + **Chatrooms**
    - Chatting online is fun, but do you know who you are talking to?
    - Visit the **ThinkuKnow** site, or the online safety pages for the social networking site you are using

*The following 3 slides show examples of cyber fraud*:

**Slide 17**

A first-time buyer transferred more than £74,000 to a fraudster, believing it to be his solicitor’s account. At the time of the report, the buyer had only received £7,837 back.

**Slide 18**

This couple thought they were sending money to their solicitor, but the bank details had been changed and they transferred the money to a criminal.

**Slide 19**

Hackers trick buyers into sending their deposits to rogue accounts

You can check if you’ve had information taken or your email account has been compromised on the following website: **https://haveibeenpwned.com/**

**Slide 20: Passwords Advice**

Passwords are the most common way to prove your identity to access internet websites, email accounts, Personal Computers etc. **A strong password is essential**.

* Make sure all your email accounts have unique passwords
* All your financial accounts should have unique passwords
* Don’t use the same password for multiple sites
* Choose passwords that are easy for **you** to remember, but others won’t associate with you
* The current recommendation is to create a password from three random words (of 6 characters, or more, each preferably); use numbers and symbols too if the website requires it, or to make the password even stronger
* Pick a phrase or song lyric and use the initial letter for each word to make up your password
* When asked to ‘give your mother’s maiden name’, as extra security, choose another name you will remember. (The same can apply for ‘Favourite Teacher’, ‘First Friend’ or ‘Place of Birth’ etc)
* Password changes where numbers are incremented, or dates appended, are easy to crack; especially if you are using a dictionary word, or name.

There is a view now that, if you keep changing your password (or as an employee you are required to change your password frequently), the password will get progressively weaker. It is best to start with a very strong password and stick to it.

**Risks of using weaker passwords:**

People impersonating you to commit fraud or other crimes:

* Hackers accessing your bank account
* Fraudsters purchasing items online with your money
* Criminals impersonating you on social networking and dating sites
* Fraudsters sending emails in your name
* Hackers accessing the information on your personal computer

You can check the strength of your existing passwords on the following website: **https://howsecureismypassword.net/**

**Password Managers**

A password manager is a software application that is used to store and manage the passwords that a user has for various online accounts and security features.

Password managers store the passwords in an encrypted format and provide secure access to all the password information with the help of **one master password**

* A password manager helps to generate and retrieve complex passwords, so you don’t have to. The manager will automatically enter your login details when you visit a known website.
* A password manager will use the maximum numbers of characters and/or symbols
* Passwords are stored on an encrypted database or some calculate them on demand. Some password managers provide locally installed software
* Password Managers are good to use; **you must remember one login password only**
* To choose a Password Manager, look at the reviews/stars given by current users and technology sites, who do not have a vested interest. (***LastPass*** *is an example of a Password Manager;* ***Dashlane*** *has a free version*)

**Please note**: **Tamworth Borough Council cannot recommend a Password Manager for you to use. The examples above are well known suppliers of the service.**

**Slide 21: Advice – Looking at items in your home**

**Router**:

* If it is older than 3 years, consider replacing it
* Always update the router; many aren’t automatically updated. Check your router manufacturer’s website for instructions
  + - Updating the firmware of your router will provide security fixes and, sometimes, its overall performance
* Change the network name on your router from the default name. The default name gives away what type of router it is, and hackers know the easiest ways to access each manufacturer’s hardware.
* Change the default password to a strong password of your own

**The Internet of Things** (IOT):

**IOT** are everyday objects that are connected to the internet to receive controls and provide usage data to their owners or third parties: manufacturers or utility providers.

Examples of these can include:

* + Security cameras
  + Infant monitors
  + Heating controllers
  + TV set top boxes
  + ‘Smart’ electrical goods (fridges; bathroom scales; programmable lighting)
  + Motor vehicles

All are vulnerable to hacking, because they are connected to the internet.

***Example****: A North American casino installed a smart fish tank as a new attraction. The tank could regulate temperature, salinity and take care of feeding (connected to the internet). Despite the Casino’s efforts to secure their network, the fish tank turned out to be a weakness and hackers were able to exploit that to transfer 10GB of data to a device in Finland, before the breach was detected.*

**Why would they be hacked?**

* Security cameras are hacked so that the hacker can ‘spy’ on the activities of the household; e.g. to find out if the house is empty on a regular basis
* Different items can give access to the privacy and confidentiality of your home and family
* You would not want your baby monitor to be hacked. You may be having a conversation in the room that gives away personal information.

All the connected items in your home will be configured to connect to your router, so **remember**:

* Change the default password
* Ensure the Wi-Fi is secured to WPA2
* Read the manufacturer's instructions **before** connecting the device to the internet

It is often easier to check and change the settings when you are installing the device initially.

**QR Codes**

QR codes are a fast and easy way to reach advertisers’ websites direct from your smartphone or tablet. You can research products while shopping. They are convenient to you and valuable to the vendor or advertiser. However, using them isn’t without risk:

* QR codes can’t be read by a human eye, so there is no way of knowing that the website you are taken to is authentic
* Even where codes have been published in public places, an alternative code can be substituted by fraudsters
* You can be directed to a fraudulent site where you may disclose personal or financial information to fraudsters, or you may be exposed to inappropriate material or pick up a virus.

**Reduce the risk**:

* Ensure that any QR code reader app that you download is from a reputable source
* Where possible, and especially in public places, check for visual indications that a QR code has not been tampered with (for example with an over sticker).
* **Never** enter personal or financial information on a website to which you have been directed from a QR code.
* If you are downloading security software for your smartphone or tablet, choose one which has a built-in QR code scanner.

Some commonly-available QR code readers include the ability to check the authenticity and safety of destination websites.

**Slide 22: Advice**

To help keep your device or network secure:

* **Update**: Reinstall a program using a newer version (free of charge)
* **Upgrade**: Like an update, but not always free
* **Migrate**: Stop using an application, to move to another product on preferential terms

**Firewall**: A barrier between the internet and your devices or networks

* Protects against hackers
* Protects against Worms (a virus that can spread from device to device)
* Prevents some outgoing traffic originating from a virus infection

**A firewall does not protect against SPAM or most malware and spyware**.

**Cyber Insurance**: A product used to protect businesses and individuals from internet-based risks and risks involving Information Technology infrastructure and activities. Insurance does not protect you against attack, but it can offset costs involved with recovery after a cyber-related security breach or similar event.

**Plan**:Businesses should prepare a plan for response and recovery in the event of an incident. The ***plan*** should help employees detect incidents quickly, lessen the impact of the attack and return the business to normal as soon as possible.

It will outline the steps to manage a cyber security incident, for employees responsible for the recovery of data or for closing a breach.

**Slide 23: You are the best defence!**

The number one cause of cyber security breaches is negligence or carelessness. You can prevent cybercrime by being alert to the dangers:

* Never open attachments you are not expecting (even from a known sender)
* Don’t click on links to websites; type the correct URL (website address) into the address bar
* Hover over links included in an email, to reveal the URL
* If you receive a SPAM email; report it as SPAM so the email provider can block future emails from the same sender.

**Slide 24: What support is there for Businesses and the Public?**

**Slide 25 – 30: Resources**

*These slides show useful websites*

**Slide 31: Final Slide.**