360 ASSURANCE

The Ultimate Guide to Cyber Crime

Contents

Report concerns to 360assurance.counterfraud@nhs.net

or use the QR below to find our online reporting form.

Follow @NHSCounterFraud

This document has been designed to raise awareness of cyber crime. We have packed it full of useful information about the most common types of cyber crime and have offered real life examples of large scale cyber attacks to demonstrate the impact that these crimes can have on businesses and individuals alike.

Useful Contacts:

Your Counter Fraud Specialist is specially trained to handle NHS fraud related queries. If you have a concern about NHS Fraud then please contact your organisation's Counter Fraud Specialist (details on the left of this page). Alternatively you can contact the NHS Counter Fraud Authority on 0800 028 40 60 or report online here.

Whether an NHS Health Informatics Service or a private sector service, your organisation's IT service provider will be able to react to reports of scam emails. Stolen NHS equipment should be reported to the police and the IT service provider immediately.

You can report and get advice about cyber crime and fraud affecting your personal IT security from the UK's national fraud and cyber reporting centre, Action Fraud. You can call Action Fraud on 0300 123 2040. You can also report frauds and cyber incidents online here.

Glossary of Terms

Biometrics: At the most basic level, biometrics can be best explained by breaking down the word: bio, as in biological, and metric, as in measurement. That is to say biometrics are biological measurements. Biometric authentication is used in computer science as a form of identification and access control. Examples include fingerprint scanning and facial recognition.

Bitcoin: A type of digital currency that can be sent from user to user without the need for intermediaries (e.g. banks). There are no physical bitcoins, only balances kept on a public ledger that everyone has transparent access to.

Brute Force Attack: A type of cyber attack that is equivalent to trying every key on your key ring to unlock the door and eventually finding the right one. They are simple and reliable. Attackers let the computer do the work—trying different combinations of usernames and passwords until they find one that works.

Code: A set of rules or instructions. It is made up of words and numbers and when you put them in the right order it will tell your computer what you want it to do.

Dark Web: The dark web (also known as the dark net) refers to encrypted online content that is not accessed by conventional search engines. It has gained a reputation as a haven for illegal activities.

Data Breach: A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. This includes breaches that are the result of both accidental and deliberate causes.

Domain: A domain is the address of a website that you type in the browser search bar. In simple terms, if a website was a house, then the domain name would be the address.

Hotspot: A hotspot is a physical location where internet access is provided via Wi-Fi.

IP Address: IP address stands for internet protocol address. It is an identifying number that is associated with a specific computer. When connected to the internet, the IP address allows the computers to send and receive information.

Operating System: In it's most general sense an operating system is software that allows a user to run other applications on a computing device.

Patch (or Security Patch): A patch is a set of changes to a computer program or it's supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes.

Software: The programs and other operating information used by a computer.

Spear Phishing: An email or electronic communications scam targeted towards a specific individual, organisation or business. This is different to phishing emails that are sent to a more wide audience.

Terabyte: A terabyte, much like a byte, megabyte or gigabyte, is a unit of measurement of digital information.

Traffic: Website traffic refers to web users who visit a website. Traffic is measured in visits, sometimes called sessions.

URL: A URL incorporates the domain name, along with other detailed information, to create a web address to direct a specific internet browser to a specific webpage online.

Virtual Private Network: A virtual private network (or VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPN services establish secure encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

CYBER CRIME OFFENCES

The majority of cyber crime offences will fall under the remit of the Computer Misuse Act 1990. The Act is a key piece of legislation that criminalises the act of accessing or modifying data stored on a computer system without appropriate consent or permission. The maximum penalty for offences under the Computer Misuse Act is five years imprisonment.

Hacking is the unauthorised use of, or access into, computers or networks by using security vulnerabilities or bypassing usual security steps to gain access. Criminals may hack systems or networks to steal money or information, or simply to disrupt business.

Malicious Software (malware) can be spread between computers and interfere with the operations of computers. It can be destructive, causing system crashes or deleting files, or used to steal personal data.

Invasion of privacy is the act of someone attempting to intrude on a person’s personal life. This includes hacking into a person’s computer, reading their emails or monitoring online activities.

SOCIAL MEDIA OFFENCES

Trolling is a form of baiting online which involves sending abusive and hurtful comments across all social media platforms. This can be prosecuted under the Malicious Communications Act 1988 and the Communications Act 2003.

Online harassment can include repeated attempts to impose unwanted communications or contact in a manner that could be expected to cause distress or fear.

Disclosure of private sexual images without consent also known as “revenge porn”, this is a broad term covering a range of activities usually involving an ex-partner, often involving the upload of intimate images of the victim to the internet, to cause the victim humiliation or embarrassment.

Grooming refers to the actions of an individual who builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation.

Stalking online is a form of harassment which can involve persistent and frequent unwanted contact, or inference in someone’s life.

Virtual mobbing takes place when a number of individuals use social media or messaging to make comments to or about another individual, usually because they are opposed to that person’s opinions. The volume of messages may amount to a campaign of harassment.

PHISHING

WHAT IS PHISHING?

Phishing is one of the most prevalent scam types. Phishing occurs when fraudsters attempt to trick their victims into doing the wrong thing, such as clicking a bad link in an email that will download malware or direct them to a rogue website.

Phishing can be conducted via a text message, social media or by phone, but the term is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly and hide among the huge number of ordinary emails that busy users receive. Attacks can install viruses, sabotage systems, or steal intellectual property or money.

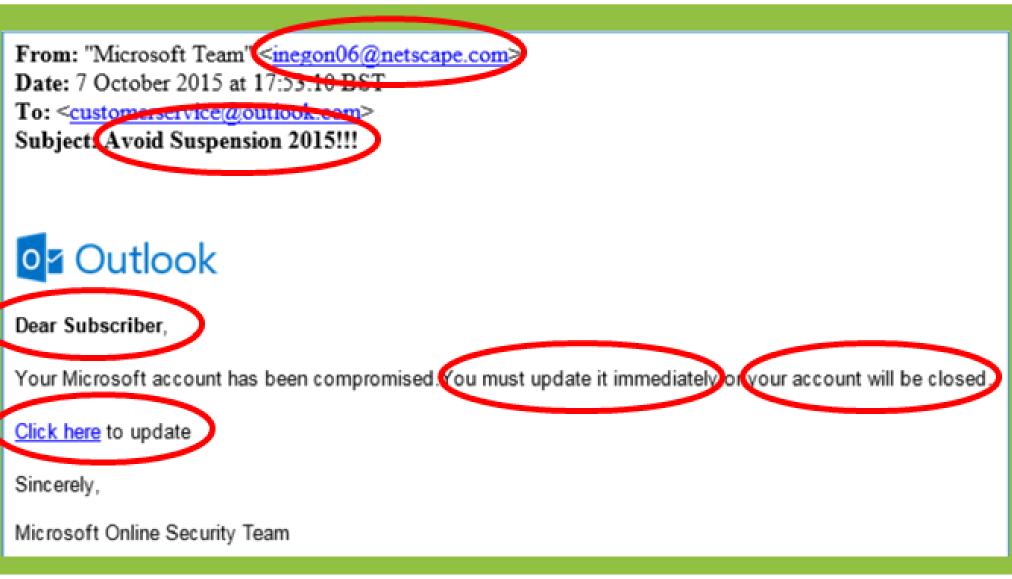
90%	£1.3m	76%	1.5m
of all data breaches result from a phishing attack.	The average financial cost of a data breach through phishing.	The percentage of businesses that have been affected by phishing attacks.	The number of new phishing sites that are launched each month.

PHISHING SCAMMERS JAILED FOR ATTEMPTED £59M FRAUD

An estimate £59m worth of fraud was prevented in the UK after three men were convicted for launching a sophisticated phishing scam to access the accounts of bank customers in 14 countries. The Met Police Central e-Crime Unit (PCeU), the Serious Organised Crime Agency (SOCA) and the US Secret Service acted on intelligence of more than 2,600 phishing pages that mimicked banking websites. The fake pages were designed to dupe victims into logging on to them and providing their banking credentials. The trio were gathering data and stealing money from counties all over the world including the UK, USA, China, Russia and Australia.

The men behind the scam were traced to the UK, staying in a luxury hotel in London and caught red-handed using laptops to log into servers storing compromised banking data. Following the arrests, officers discovered servers containing details of 30,000 bank customers - 12,500 of which were in the UK - and 70 million customer email addresses to be used in phishing attacks.

A PERFECT EXAMPLE OF A PHISHING EMAIL:



From: "Microsoft Team" <inegon06@netscape.com>
Date: 7 October 2015 at 17:53:10 BST
To: <customerservice@outlook.com>
Subject: Avoid Suspension 2015!!!

Dear Subscriber,

Your Microsoft account has been compromised. You must update it immediately or your account will be closed.

Click here to update

Sincerely,

Microsoft Online Security Team

THINK BEFORE YOU CLICK: WHAT TO LOOK OUT FOR

Who is the email from?

Most legitimate organisations will have their own email domain in the same way that many NHS email users will have a @nhs.net email account. If the name of the sender and the email address do not match up it is probably a scam.

Is there poor spelling/grammar/vocabulary?

You should check the email for poor spelling, grammar or vocabulary. In the above example the triple '!' is informal and indicated a scam.

Is it personal?

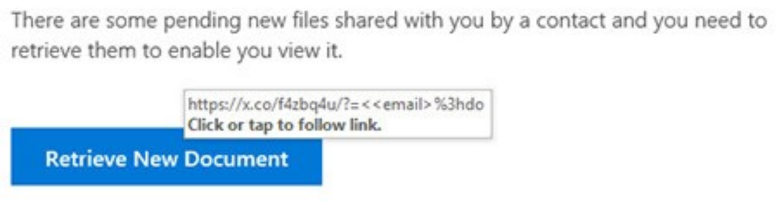
Phishing emails will often use generic terms when addressing you as they send the emails out to hundreds of people. "Dear Subscriber", as shown in the example above, is a common one.

Does it create a sense of urgency or make threats?

The most successful phishing emails create a sense of urgency as it does not give the recipient time to think. The above example instructs the recipient to act immediately otherwise their account will be closed. This is a tell-tale sign of a phishing scam.

Does the email provide a link or URL?

Clicking a link in an email is a common request. To check the legitimacy of a link you can hover your mouse over the link or address to see the linked sites true address. Misspelt URLs or unfamiliar domain names can often highlight that an email is not genuine. See the example below from a spoofed Microsoft email. If this link was genuine then the hyperlink displayed would reflect a Microsoft website.



There are some pending new files shared with you by a contact and you need to retrieve them to enable you view it.

https://x.co/f4zbq4u/?=<<email>%3hdo
Click or tap to follow link.

UPDATES

You are probably no stranger to those little pop-up windows that tell you software updates are available for your computer, laptop, tablet or mobile device. You might be tempted to click on that “remind me later” button. Do not do it, or at least, do not put off updating your software for long. Why are software updates so important? There are a lot of reasons. Here are five that show you why it is important to update your software regularly:

1 **Software updates do a lot of things.** This might include repairing security holes that have been discovered and fixing or removing computer bugs. Updates can add new features to your devices and remove outdated ones. While you are at it, it is a good idea to make sure your operating system is running the latest version.

2 **Updates help patch security flaws.** Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software program or operating system. Hackers can take advantage of weaknesses by writing code to target the vulnerability. The code is packaged into malware (malicious software).

3 **Software updates help protect your data.** You probably keep a lot of documents and personal information on your devices. Your personally identifiable information - from emails to bank account information - is valuable to cybercriminals. They can use it to commit crimes in your name or sell it on the dark web to enable others to commit crime.

4 **It’s not all about you.** Ok, cyber security is mostly about you, but you’ve got other people to think about to. If your device gets a virus, you could pass it on to your friends, family and business associates. That is why you want to keep your software and systems updated. Trusted security programs and anti-virus protection can help prevent from malware.

5 **You deserve the latest and greatest.** Updates not only patch security holes, they can also add new features and improve existing ones. You don’t want to fall behind the times! In that way, software updates really are all about you. Your software program may get a new shot of stability—no more crashing!

For information on updating your Windows software click here.
For information on updating your iOS software click here.
For information on updating your Android software click here.

CASE EXAMPLE: WANNACRY RANSONWARE ATTACK

What was WannaCry?

The WannaCry ransomware attack was a global cyber-epidemic that took place in May 2017. This ransomware attack spread through computers operating Microsoft Windows. Users' files were held hostage and a Bitcoin ransom was demanded for their return. Were it not for the continued use of outdated computer systems and poor education around the need to update software, the damage caused by this attack could have been avoided.

How did the WannaCry attack work?

The cybercriminals responsible for the attack took advantage of a weakness in the Microsoft Windows operating system using a hack that was allegedly developed by a national security agency. Known as Eternal Blue, this hack was made public by a group of hackers called the Shadow Brokers before the WannaCry attack.

Microsoft released a security patch which protected users' systems against this exploit almost two months before the WannaCry ransomware attack began. Unfortunately, many individuals and organisations do not regularly update their operating systems and so were left exposed to the attack. Those that had not run the Microsoft update before the attack did not benefit from the patch and were left open to attack.

What happened if the WannaCry ransom was not paid?

The hackers demanded $300 worth of bitcoins and then later increased the ransom demand to $600 work of bitcoins. If victims did not pay the ransom within three days, victims were told their files would be permanently deleted.

What impact did the WannaCry attack have?

The WannaCry ransomware attack hit around 230,000 computers globally. One of the first companies affected was the Spanish mobile company, Telefonica. By 12th May 2017, thousands of NHS hospitals and surgeries across the UK were affected.

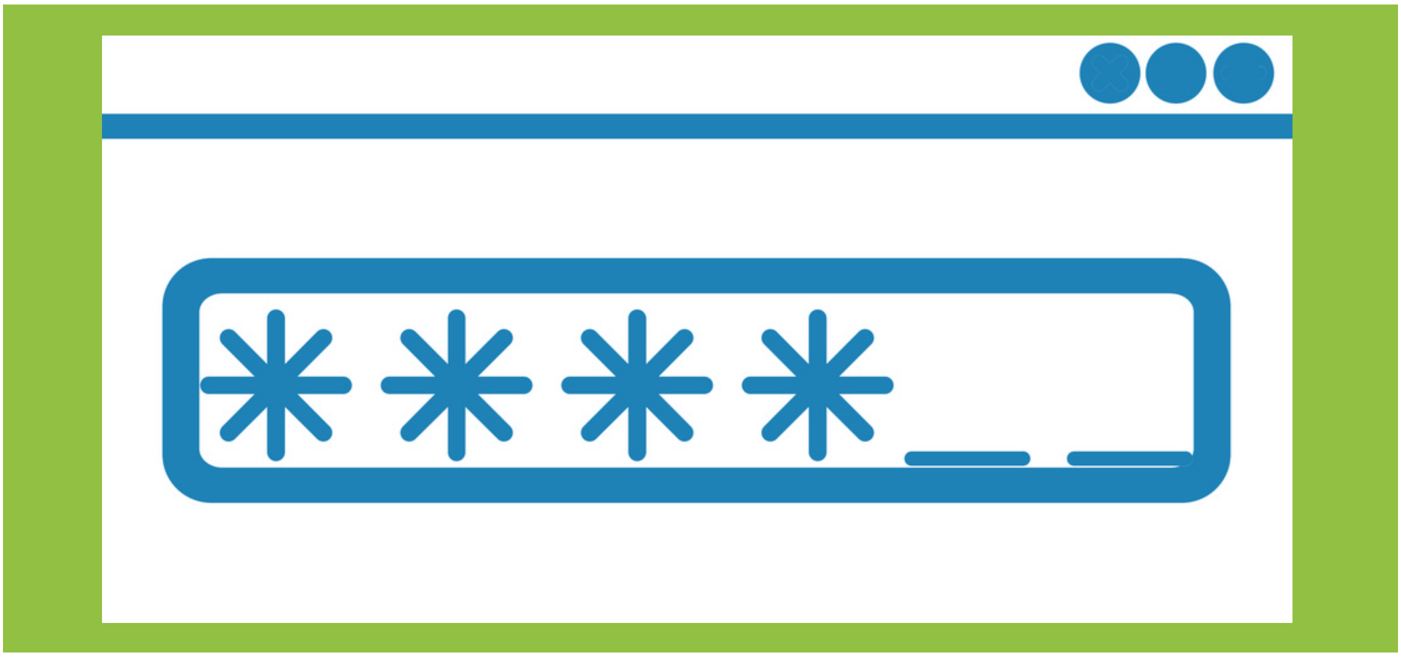
A third of NHS hospital Trusts were affected by the attack. Ambulances were rerouted, leaving people in need of urgent care. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were cancelled as a result of the attack.

There are a number of websites you can visit to learn more about Cyber Crime:

1. National Crime Agency
2. National Cyber Security Centre
3. Get Safe Online
4. Cyber Aware
5. Action Fraud
6. Take 5
7. Friends against Scams
8. National Trading Standards Scams Team
9. The Met Police
10. Europol
11. Interpol
12. Crown Prosecution Service

PASSWORDS

Weak passwords risk breaches in patient confidentiality. The easiest way to protect yourself from cyber threats is to have strong and varied passwords. Passwords are the best form of defence we have to prevent unauthorised access, so make sure you keep them private and out of sight of others.



MASSIVE BRUTE-FORCE ATTACK ON ALIBABA AFFECTS MILLIONS

Alibaba's e-commerce site TaoBao was the victim of an attack that reused stolen account credentials, such as passwords and usernames from third party sites.

A report claims that the hackers used a database of 99 million usernames and passwords, which they entered into Alibaba's cloud network in a brute force attack. It is believed that 20.6 million accounts and passwords were successful, which allowed the hackers to buy products and post fake reviews. TaoBao, like eBay, is a reputation based seller-to-seller market place where reputation counts very highly so boosting an accounts reputation via fake reviews can be a big bonus.

The massive brute-force attack took place without Alibaba's security team noticing these millions of failed login attempts. However, these attacks are most likely to have gone undetected due to the vast amount of traffic that TaoBao receives in a day.

SEVEN TIPS TO MAKE YOUR PASSWORDS AS STRONG AS POSSIBLE

1. Make your password long. Hackers use multiple methods for trying to get into your accounts. The most basic way is to personally target you and manually type in letters, numbers and symbols to guess your password. The more advanced method is to use what is known as a 'brute force attack'. In this technique, a computer programme runs through every possible combination of letters, number and symbols as fast as possible to crack your password. The longer and more complex your password is, the longer the process takes. Passwords that are three characters long take less than a second to crack.

2. Make your password a nonsense phrase. Long passwords are good; long passwords that include random words and phrases are better. If your letter combinations are not in the dictionary then they will be harder to crack. Also, do not use characters that are sequential on a keyboard, such as number in order or the widely used "qwerty".

3. Includes numbers, symbols, and uppercase and lowercase letters. Randomly mix up symbols and numbers with letters. You could substitute a zero for the letter O or @ for the letter A, for example. If your password is a phrase, consider capitalising the first letter of each new work, which will be easier for you to remember. For example, if your phrase is: "My First House Was At Number 12 Bond Street" your password could be "Mfhw@n12BS".

4. Avoid using obvious personal information. If there is information about you that is easily discoverable, such as your birthday, anniversary, relatives or pets names, do not include them in your password. These only make your password easier to guess. On that note, if you are required to choose security questions and answers when creating an online account, select ones that are not obvious to someone browsing your social media accounts.

5. Do not reuse passwords. When hackers complete large-scale hacks, as they have previously done with popular email servers, lists of compromised email addresses and passwords are often leaked online. If your account is compromised and you use this email address and password combination across multiple sites, your information can be easily used to get into any of these other accounts. Use unique passwords for everything.

6. Start using a password manager. Password managers are services that auto-generate and store strong passwords on your behalf. These passwords are kept in encrypted, centralised locations, which you can access with a master password. Many services are free to use and come with optional features such as syncing new passwords across multiple devices and auditing your password behaviour to ensure you are not using the same one in too many locations.

7. Keep your password under wraps. Don't give your passwords to anyone else. Don't type your password into your device if you are in plain sight of other people. Do not plaster your password on a sticky note on your work computer!

You can check how quickly your password could be hacked using the following website: https://howsecureismypassword.net/ The link will explain in a quantifiable way how long it would take for a computer to crack your password.

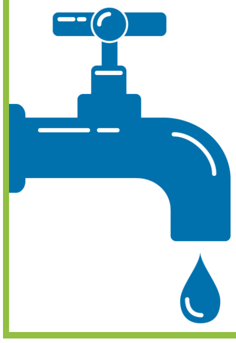
TWO FACTOR AUTHENTICATION

WHAT IS TWO FACTOR AUTHENTICATION

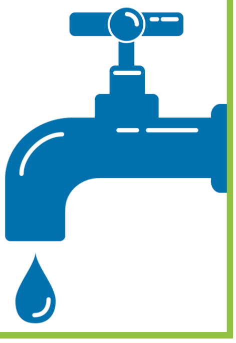
Two factor authentication, sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves. This process is done to better protect both the users credentials and the resources the user can access. Two factor authentication provides a higher level of security than authentication methods that depend on single factor authentication, in which the user only provides one factor - typically a password or passcode. Two factor authentication methods rely on a user providing a password, as well as a second factor, usually either a security token or a biometric factor, such as a fingerprint or facial scan.

SETTING UP TWO FACTOR AUTHENTICATION IS EASY….

You can find useful guides for setting up two factor authentication on some of your accounts by clicking the following logos:



PROTECTING YOUR PERSONAL DATA



The information you post online can be a treasure trove for a cyber criminal. Social media sites are used by millions of people every day, and many people have online accounts where a significant amount of information is detailed about them, their employment and their education.

In the same way, a criminal may see that you are on holiday through a social media post and burgle your house, a cyber criminal may use a work contact email address or details of a conference you are attending, which you have posted online, to assist in a cyber attack against you.

It is very easy for a cyber criminal to create a spear phishing email from the information that can be found online using simple searches via a search engine. This is called open source information and is available on the internet without requiring access to secure areas on any website.

For example, a simple tweet about a visit to a restaurant could be used to create a spear phishing email that appears to come from the restaurant. This email may offer you the opportunity to enter a competition or claim a discount on your next visit by completing a form attached to the email. This form may contain malicious software and on opening it the malware can spread on to your computer.

HOW TO PROTECT YOURSELF FROM DATA LEAKAGE

1. **Be wary of what you post online.** Does the information have to be in the public domain? Don't reveal sensitive information i.e. home address, financial information or phone number. You can also limit details about work history as this information can be used to hack into your account.
2. **Know what information can be found about you online.** Complete a simple open source internet search to see what data is available about you. There may be information posted by others that you are not aware of, or information you did not know was posted in the public domain.
3. **Separate business information from personal information and who can see which.** Don't have personal contact details on business websites and vice versa. Keep work and personal life separate.
4. **High security settings on social media sites.** Don't let everyone see everything. Make sure that personal information and details you only want friends or colleagues to see are kept private by using the security settings on social media sites. Set them to ensure that only the people you want to see your information can see it, and encourage your friends and family to do the same. In addition, be wary of people that want to follow or friend you. Consider what interest they have in you and whether they are suitable to see personal information about you.

SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions.

To access a computer network, the typical hacker might look for a software vulnerability. However, a social engineer could pose as a technical support person to trick an employee into divulging their login credentials. The fraudster is hoping to appeal to the employee's desire to help a colleague and would perhaps act first and think later.

5 TIPS TO HELP YOU AVOID BEING A SOCIAL ENGINEERING VICTIM

1. **Consider the Source.** A found USB stick isn't necessarily a good find. It could be loaded with malware just waiting to infect a computer. And a text or email seemingly from your bank may not be from your bank. Spoofing a trusted source is relatively easy. Don't click on links or open attachments from suspicious sources. No matter how legitimate the email looks, it is safer to type a URL into your web browser instead of clicking on a link.
2. **Slow down.** Social engineers often count on their targets to move quickly, without considering the possibility that a scammer may be behind the email, phone call, or face to face request on which they are acting.
3. **If it sounds too odd to be true…** How likely is it that a foreign prince would reach out to you for help? Or on the flip side, that a relative is texting you to post bail while travelling? Investigate any requests for money, personal information, or any item of value before handing it over.
4. **Install an antivirus software or a security suite** and keep that software up to date. Also, make sure that your devices are running the latest versions of their operating software. If possible, set the operating systems to update automatically. Having the latest versions of these software applications on your devices will help ensure they are prepared for the most recent security threats.
5. **Your email software can help you.** Most email programs can help filter out junk mail, including scams. If you think yours isn't doing enough, do a quick online search to find out how to change it's settings. The goal is to set your spam filters to high to weed out as much junk mail as possible.

5 TYPES OF SOCIAL ENGINEERING ATTACKS

Baiting: This type of social engineering depends upon the victim taking bait, not unlike a fish reacting to a worm on a hook. The person dangling the bait wants to entice the target into taking action.

Example: A cybercriminal might leave a USB stick, loaded with malware, in a place where the target will see it. In addition, the criminal might label the device in a compelling way - ”Confidential” for example. A target who takes the bait will pick up the device and plug it in to a computer to see what is on it. The malware will then automatically infect the computer.

Phishing: A well known way to grab information from an unwitting victim. Despite its notoriety, it remains quite successful.

Example: A fraudster might send an email that appears to come from a source trusted by the would-be victim. That source might be a bank asking email recipients to click on a link and log into their accounts. Those who click on the link are taken to a fake website that, like the email, appears to be legitimate. If they log in to that fake site, they are essentially handing over their login credentials and giving the crook access to their bank accounts.

Email Hacking and Contact Spamming: It is in our nature to pay attention to messages from people we know. Some criminals try to take advantage of this by commandeering email accounts and spamming account contact lists.

Example: If your friend sent you an email with the subject “Check out this site I found, it is totally cool!” you might not think twice before opening it. By taking over someone’s email account, a fraudster can make those on the contact list believe they are receiving an email from someone they know. The primary objectives include spreading malware and tricking people out of their data.

Quid Pro Quo: This scam involves an exchange - I give you this, and you give me that. Fraudsters make the victim believe it is a fair exchange, but that is far from the case, as the cheat always comes out on top.

Example: A scammer may call a target, pretending to be an IT support technician. The victim might hand over the login credentials to their computer, thinking they’re receiving technical support in return. Instead, the scammer can now take control of the victim’s computer, loading it with malware or, perhaps, stealing personal information from the computer to commit identity theft.

Vishing: Vishing is the voice version of phishing. The “V” stands for voice, but otherwise the scam attempt is the same. The criminal uses the phone to trick a victim into handing over valuable information.

Example: A criminal might call an employee, posing as a co-worked. The criminal might ask the victim to provide login credentials or other information that could be used to target the company or it’s employees.

USING PUBLIC WIFI

WHAT IS PUBLIC WI-FI?

Public Wi-Fi can be found in popular places like airports, coffee shops, shopping centres, restaurants and hotels—and it allows you to access the Internet for free. These 'hotspots' are so widespread and common that people frequently connect to them without thinking twice. Although it sounds harmless to log on and check your email or you bank account, everyday activities like these require a login and could be risks on public Wi-Fi.

The problem with public Wi-Fi is that there are a tremendous number of risks that go along with these networks. While business owners may believe they're providing a valuable service to their customers, chances are the security on these networks is lax or non-existent.

MAN IN THE MIDDLE ATTACKS

One of the most common threats on public Wi-Fi networks is called Man-in-the-Middle (MitM) attacks. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and read them. So what you thought was private no longer is.

Other threats from using public Wi-Fi networks include:

- **Malware Distribution:** Due to software vulnerabilities, attackers can slip malware onto your computer without you even knowing.
- **Snooping and Sniffing:** Cybercriminals can buy special software kits and even devices that can assist them with eavesdropping on Wi-Fi signals. This allows hackers to access everything that you are doing online.
- **Malicious Hotspots:** These hotspots trick victims into connecting to what they think is a legitimate network because the name sounds reputable, when in fact, it could be a rogue access point. Connecting to these networks allow cybercriminals to view your sensitive information.

HOW TO STAY SAFE ON PUBLIC WI-FI

The best way to know your information is safe while using public Wi-Fi is to use a virtual private network (VPN) when surfing on your computer. To learn about VPN's watch this video.

If you must use public Wi-Fi, follow these tips to protect your information:

DON'T:

- Allow your Wi-Fi to auto-connect to networks.
- Log into any account via an app that contains sensitive information.
- Leave your Wi-Fi or Bluetooth on if you are not using them.
- Access websites that hold sensitive information, such as healthcare accounts.
- Log onto a network that isn't password protected.

DO:

- Disable file sharing.
- Only visit sites using HTTPS.
- Log out of accounts when done using them.
- Use a VPN (virtual private network) to make your public Wi-Fi connections are made private.

WHAT IS HTTPS?

HTTPS, the lock icon in the address bar, an encrypted website connection—it is known as many things. While it was once reserved primarily for passwords and other sensitive data, the entire web is gradually leaving HTTP behind and is switching to HTTPS. The 'S' in HTTPS stands for 'secure'. It is the secure version of the standard 'hypertext transfer protocol' your web browser uses when communicating with websites.

When you connect to a website with regular HTTP your browser looks up the IP address that corresponds to that website and connects to that IP address. Data is sent over the connection in clear text. An eavesdropper on a Wi-Fi network can see the webpages you are visiting and the data you are transferring back and forth. This is why passwords and other sensitive information should never be sent over a HTTP connection as an eavesdropper could easily steal them, instead always check for HTTPS.

MALWARE

WHAT IS MALWARE?

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of computer code developed by cybercriminals, designed to cause extensive damage to data and systems or to gain unauthorised access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

Virus: Possibly the most common type of malware, viruses attach their malicious code to clean code and wait for an unsuspecting user or an automated process to execute them. Like a biological virus, they can spread quickly and widely, causing damage to the core functionality of systems, corrupting files and locking users out of their computers.

Worms: Worms get their name from the way they infect systems. Starting from one infected machine, they weave their way through the network, connecting to consecutive machines in order to continue the spread of infection. This type of malware can infect entire networks of devices very quickly.

Spyware: As the name suggests, spyware is designed to spy on what a user is doing. Hiding in the background on a computer, this type of malware will collect information without the user knowing, such as credit care details, passwords and other sensitive information.

Trojans: Just like Greek soldiers hiding in a giant horse to deliver their attack, this type of malware hides within or disguises itself as legitimate software. Acting discreetly, it will breach security by creating backdoors that give other malware variants easy access.

Ransomware: Also known as scareware, ransomware comes with a heavy price. Able to lockdown networks and lock out users until a ransom is paid, ransomware has targeted some of the biggest organisations in the world today - with expensive results.

Adware: Adware is a type of malware that, once downloaded, will unexpectedly show advertisement on the victim's computer. Adware doesn't tend to steal data like other forms of malware, but it can be extremely frustrating as the user is forced to see ads they would prefer not to. The ads range from small banner ads to invasive pop-up windows that can't be closed down.

Botnet: A bot is a device that has been infected with malicious software to do something harmful without the user's knowledge. Botnets are networks of these infected devices that work together under the control of an attacker. Botnets can be used to conduct phishing campaigns, send out spam or used to carry out Distributed Denial of Service Attacks (DDOS).

What is a Distributed Denial of Service (DDOS) attack?

They attack websites and online services. The aim is to overwhelm them with more traffic that the server or network can accommodate. The goal is to render the website or service inoperable. The traffic can consist of messages or requests for connections.

HOW TO PROTECT YOURSELF FROM MALWARE

There are a number of ways to protect yourself from Malware, many of which have already been covered within this document (e.g. keeping software updated and being wary of links and attachments in emails). However, you can also protect yourself from malware in the following ways:

1. Don't trust pop-up windows that ask you to download software: When surfing the web, you might come across sites that show pop-up windows, making you believe your computer has been infected and asking you to download some software in order to protect yourself. Don't fall for this trick. Just close the pop up window and make sure that you don't click inside the pop up window.

2. Limit your file sharing: Some sites and applications allow you to easily share files with other users. Many of these sites and applications offer little protection against malware. If you exchange or download files using these file-sharing methods, be on the lookout for malware. Malware can often be described as a popular film, album, game or programme.

3. Use anti-virus software: If you need to download something, you should use an anti-virus programme to scan that download for malware before opening it. Antivirus software also allows you to scan your entire computer for malware. It is a good idea to run regular scans of your computer to catch malware early and prevent it from spreading.

SONY PICTURES HACK

What were the 2014 Sony hacks? In late November 2014, Sony Pictures Entertainment was hacked by a group calling itself the “Guardians of Peace”. The hackers, who are widely believed to be working in at least some capacity with North Korea, stole huge amounts of information off of Sony’s network. They leaked the information to journalists, who wrote embarrassing things that Sony employees had said to each other.

Next, the hackers threatened to commit acts of terrorism against movie theatres, demanding that Sony cancelled the planned release of The Interview, a film about the North Korean Leader Kim Jong Un. The US government say they have strong evidence that North Korea was responsible for the attack, though the North Korean regime has denied it.

What did the hackers do? The attackers took terabytes of private data, deleted the original copies from Sony computers and left messages threatening to release the information if Sony didn’t comply with the attackers demands. Sony’s network was down for days as administrators struggled to repair the damage.

Over the course of several weeks, the hackers posted several waves of files stolen from Sony’s computers. The hackers posted five Sony movies (four unreleased) to file sharing networks. They also leaked thousands of confidential documents - everything from private correspondence among Sony executives to salary performance data about Sony employees.

What are the lessons learned?

The two main lessons learned are that companies should be investing more in network security and companies should make sure they are well-prepared to respond to attacks.

BANK HACKERS STEAL MILLIONS VIA MALWARE

In late 2013, an ATM in Kiev started dispensing cash at seemingly random times of day. No one had put in a card or touched a button. Cameras showed that the piles of money had been swept up by customers who appeared lucky to be there at the right moment. A Russian cyber security firm, Kaspersky Lab, was called to Ukraine to investigate. They discovered that the errant machine was the least of the bank’s problems.

The bank’s internal computers, used by employees who process daily transfers and conduct book keeping, had been penetrated by malware that allowed cyber criminals to record their activity. The malicious software lurked for months, sending back video feeds and images that told a criminal group how the bank conducted it’s daily routines.

Then the group impersonated bank officers, not only turning on various cash machines, but also transferring millions of dollars from banks in Russia, Japan, Switzerland, the USA and the Netherland, into dummy accounts set up in other countries.

It was estimated that around £650 million was stolen from the financial institutions in total.

LOCK YOUR SCREEN

We all store a large number of files containing private information on our computers and studies have concluded that the majority of data theft happens due to insufficient safeguard measures. One easy way to prevent data theft is by locking your computer when you are away from your work station.

Here are some reasons why locking your computer screen is so important:

- **Privacy:** By locking your computer you will prevent unauthorised persons from accessing your PC.
- **It helps prevent unwanted inconvenience:** When your computer is not used for a while the monitor may go dim or go off. However, that does not mean that the computer Is off. If you do not lock your computer screen when you walk away a stranger may come and use a key like delete, enter or space to wake the computer. These buttons can sometimes trigger an action. You could end up losing an important file or some text in a document.
- **It helps to protect confidential communications:** Sometimes somebody may send you confidential information intended for your eyes only. Locking your computer will help protect confidential communications and documents.
- **It prevents data from being altered.** Not locking your computer is like surrendering access to your files, whether personal, confidential or public. This means that anyone can access your computer and modify, remove or even share data from your computer. Locking your computer after use will prevent this type of incident.