UNIT-3 Cyber Security Tools & Techniques

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Understand the most effective cyber security tools and techniques ✓ Discuss the importance of proactive cyber security ✓ Set secure passwords with confidence

Unit 3

Cyber Security Tools & Techniques

Prevention and Defence

It is possible to protect electronic devices from cyber-attacks in a variety of ways. In this unit, we will be discussing some of the most effective ways of combating cyber security attacks and defending computer systems.

Authentication

Authentication refers to the process of ensuring that a person attempting to gain access to a system is the person they claim to be. The most common example of authentication with computer systems being the requirement to enter a username and password.

There are also some systems and organizations that take things a step further, using 'two-factor' authentication to bolster the security of their systems. Examples of additional security checks within a two-step authentication process include fingerprint scanners, voice recognition software and additional personal information that must be entered manually. A physical token (such as an access card) may also be required to authenticate the user.

The greater the extent to which businesses worldwide operate using centralised servers and connected technology, the greater the importance of effective authentication. Today, the vast majority of employers are required to connect to one or more internal and/or external networks, in order to go about their daily business. In doing so, it is essential that they confirm they are the person they claim to be, rather than an unauthorized user. It is just as important for an individual to verify their identity when accessing an in-house intranet as it is a remote worker logging on from an external location.

Each user will typically be provided with an initial username and password by the organization itself, after which they will have the opportunity to change it to something they're able to remember.

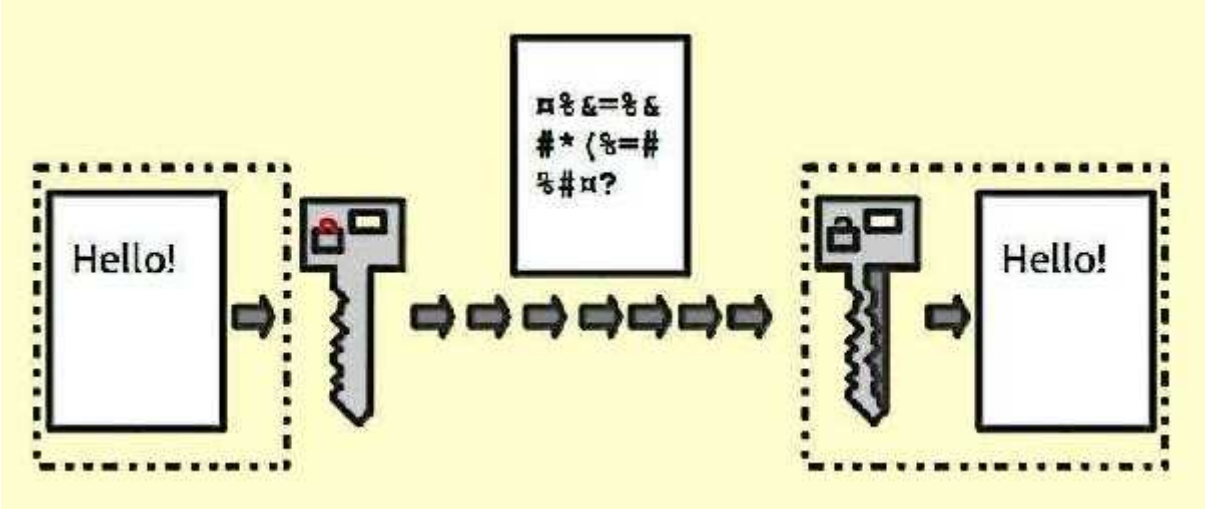
This is where the importance of choosing strong passwords becomes evident. In the event that a single individual chooses a weak password, the security of the entire organisation is compromised. Precisely why the vast majority of proactive businesses make it mandatory for every member of the workforce to change their password on a regular basis. Not to mention, choose a strong password in the first place - usually a password that consists of at least 12 characters, featuring at least one number and one uppercase and lowercase letter.

It may also be strictly prohibited for members of the workforce to use things like dates of birth or pets'

names in their passwords, which are too easy for hackers to guess.

Encryption

The term 'encryption' refers to the process of transforming data into an unintelligible format during transit. Roughly translated, the data is translated into an unreadable language prior to being transmitted, only to then be unencrypted when delivered to the intended recipient. It is something of a lock and key technique - only the authorized recipient has the key to translate the code back into a readable form. Complex mathematical algorithms are used to encrypt and decrypt the data, which happens automatically. At the highest level, encrypted data cannot be unencrypted manually - it could even take an automated algorithm several years to crack the code. These days, the vast majority of sensitive data (such as payment information) transmitted online is safeguarded using encryption.



Source Wikipedia: Figure 3.1: Encryption

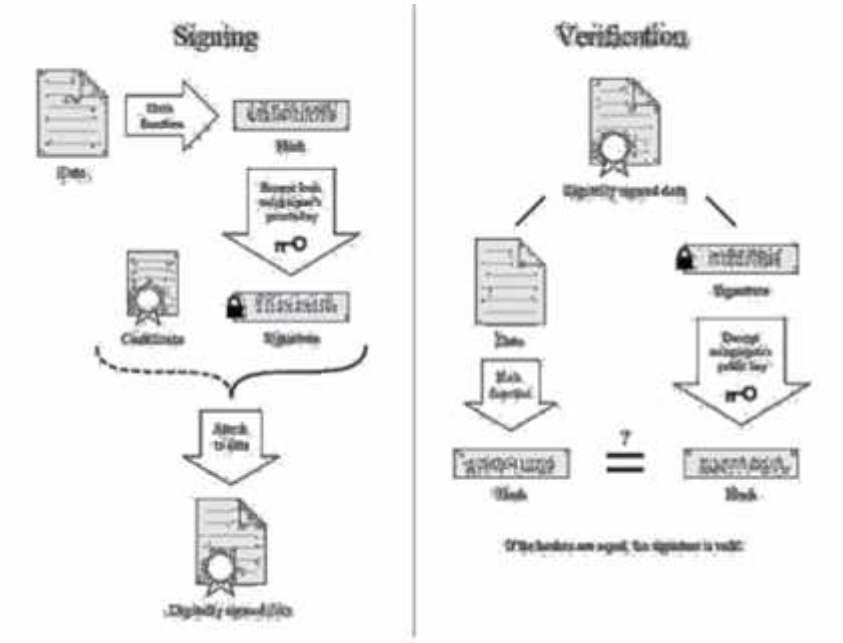
Digital Signatures

This is a technique for validation of data. Validation is the process of certifying the content of a document. The digital signatures not only validate the data, but are also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender.

Now, the decrypted message is compared with the original message. If both are same, it signifies that the data has not been tampered with and that the authenticity of the sender is verified as someone with the private key (which is known to the owner only) that can encrypt the data which was then decrypted by their public key. If the data is tampered with during transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the message cannot be re-encrypted after tampering as the

private key, which is possessed only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are becoming an essential part of legal and financial transmissions. It not only provides the authentication of a person and the validation of the document, but it also prevents denial or agreement at a later stage. Suppose a shareholder instructs a broker via email to sell the share at the current price. After the completion of the transaction, for some reason, the shareholder reclaims the shares by claiming the email to be forged or fraudulent. To prevent these kinds of situations, digital signatures are used.



Source Wikipedia: Figure 3.2: Digital signature

Antivirus

The prevalence of malicious software (spyware, viruses, Trojans etc.) is growing all the time. As is the threat posed by the most sophisticated forms of these malicious codes. One of the most effective ways of protecting a computer system against such threats is to use an equally sophisticated anti-virus suite. As the name suggests, anti-virus software is designed to identify malicious code upon detection and prevent it from causing damage to the computer system in general. The idea being that before it has chance to wreak havoc on the computer or the network, it is detected, removed or 'quarantined' safely. The user (or network manager) is notified that a suspected malicious file has been detected, after which they can decide what to do with it and determine what action needs to be taken, if any. Antivirus software must be updated regularly to keep up with the growing sophistication of cyber criminals.

Figure 3.3: Different antivirus suites available on the market

Firewall

In the simplest terms, a firewall is any hardware or software (or combination thereof) that builds a virtual 'wall' between a computer system or network and the Internet. It is designed to provide robust protection from anyone and anything that doesn't have the authorisation to bypass the firewall.

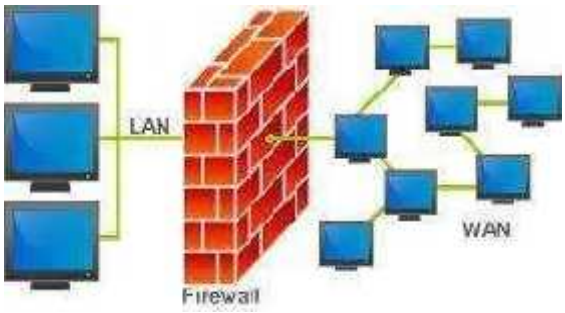


Figure 3.4: Firewall

In every organisation, there are two types of traffic - inbound traffic and outbound traffic. With the latest firewall technology, all data moving in both directions can be monitored and managed accordingly. Any information that hasn't been flagged as 'trusted' by the organization will be automatically detected by the firewall and blocked accordingly. Once again, this will also result in a notification being delivered to the relevant party, in order for them to determine what action needs to be taken.

Businesses use both software firewalls and hardware firewalls to protect their systems, or in some cases a combination of the two.

- **Hardware Firewalls:** Common examples of hardware firewalls include protected routers that prevent unauthorized access to the organization's computers and network systems.
- **Software Firewalls:** These are the 'virtual' firewalls installed on computers and servers to protect from unauthorized access. Operating systems like Microsoft Windows also feature their own in-built software firewalls.

When an operating system like Microsoft Windows ships with its own built-in firewall, it is automatically activated and ready to use. However, the user or the organization will need to configure the firewall, in order to suit their requirements. This will mean tailoring the 'permissions' of the firewall to meet the policies and rules of the organization, effectively determining what kind of information can and cannot pass through the firewall.

The following filters will need to be configured to suit the requirements of the organization:

- **Proxy:** all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- **Packet Filtering:** based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. Examples of such characteristics include IP address, domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- **Stateful Inspection:** rather than going through all the fields of a packet, key features are defined. The outgoing/incoming packets are assessed based on these defined characteristics only.

The firewall represents one of the most important parts of the modern organisation's cybersecurity differences. An effective firewall can significantly reduce the likelihood of falling victim to attack.

Steganography

This is a technique that involves sending hidden messages in files, which could be programs, image files, document files or anything else. The image is invisible and completely undetectable, until

retrieved and viewed by the authorized user. It can be particularly effective, as nobody other than the sender and receiver know that the hidden message even exists in the first place.

Generating Secure Passwords

Guideline for setting secure Password

As previously touched upon, nothing matters more in most organisational settings than setting a secure password. In addition, passwords should be changed on a regular basis for added security. Unfortunately, evidence suggests that a surprising proportion of people continue to choose passwords that are nowhere near secure enough. Always follow the guidelines below when choosing or allocating passwords:

Basics

- All passwords should be a minimum of eight characters long, though should ideally consist of 12 characters or more. The longer the better, as long as the user can remember it.
- A variety of different types of characters and symbols should be used. Every password should contain at least one uppercase and one lowercase character, along with one number and one symbol.
- Under no circumstances should any standard word be used that appears in any dictionary, irrespective of the language chosen.
- Using the same password twice should be strictly prohibited in all instances.

Things to avoid

- Do not take a simple word and add a single number to the end of it - e.g. "apple1"
- Never simply write the same basic word twice - e.g. "appleapple"
- Don't take an everyday word and spell it backwards - e.g. "elppa"
- Likewise, don't use an everyday word and take away the vowels. - e.g. "ppl"
- All standardised and predictable character sequences should be avoided - e.g. "qwerty"
- Never code letters by their position in the alphabet - e.g. 123 = ABC etc.

Tips

- Your password needs to be too complex and specific for anyone else to guess, but you should be able to remember it so that you don't have to write it down. Under no circumstances should you ever keep a written copy of your username or password.
- Ideally, you should also be able to type your password quickly and fluently. This will limit the chance of somebody guessing your password by watching you type it in.

Bad Passwords

- All passwords that are based on general personal information are considered weak and should be avoided. Examples of which include names of pets, names of spouses, nicknames, dates of birth, towns and cities, car registrations, social security numbers and so on.
- Do not set a password based on anything within sight at the time (printer, scanner, photocopier etc.) as these are far too easy for hackers to guess.
- Avoid the temptation to use the kinds of passwords that are already used by millions - Password1234, Letmein9876 etc.
- Do not include any information in your password that refers to your e-mail address, your computer name, your account name, your username or any of your credentials in general.

Choosing a password

- Using quality password generator software can be a great way of creating a near impenetrable password.
- Think of a song or poem you like, then use the first letter from each word of a sentence to create a unique password.
- Alternate between uppercase and lowercase in a random way only you will remember - e.g. “FaRsigHTdrIVEr3728”.
- Connect two or more words with one or more symbols - e.g."seat%tree"

Changing your password

- Once again, the importance of changing your password on a regular basis cannot be overstated. The same password should never be used for more than a month, though in some cases should probably be changed at least every two weeks.
- If you have even the slightest suspicion that anyone else may know your password, it is your responsibility to ensure it is changed immediately. The same applies if you write your password down at any time and leave it out in the open for even a few seconds.
- Never reuse any password you have used at any time in the past, or a variation thereof.

Protecting your password

- Unless it is appropriately encrypted, you must never store any of your login credentials on a computer. This includes using the ‘save password’ or ‘keep me logged in’ options, which are to be avoided at all costs.
- Under no circumstances should you ever tell anyone else your password - or even a colleague
- Do not send your credentials via email, or any other online channel.
- If you absolutely need to write your password down, it needs to be kept confidential and out of sight at all times. If anyone has the chance to glance at it, your password needs to be changed.
- Never enter your password when you may be in view of someone else at the time.

Remembering your password

The more complex and difficult to guess a password is, the trickier it becomes to memorise it. However, there are things you can do to ensure you don't forget your password, such as:

- Use a secure password manager.
- Repeat each new password to yourself several times when assigning it.
- Choose passwords that mean something important to you, but mean nothing to anyone else.

Bad Examples

Each of the following represents a password a hacker could easily guess:

- "fred8" - Based on the user's name, also too short.
- "christine" - The name of the user's girlfriend, easy to guess
- "kciredref" - The user's name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Adding random capitals alone doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

A good password isn't difficult to assign. It's simply a case of coming up with something you'll remember that nobody else would be able to guess, such as the following:

- "IwAwfF2C5885" - I wait all week for Friday to come, followed by four numbers.

How would a potential hacker get hold of my password?

For the professional cybercriminal, getting hold of a password isn't particularly difficult. The four most common ways of doing so being as follows:

1. **Steal it.** It's important to remember that you really never know who might be looking over your shoulder at the time. It's also worth remembering that cyber criminals these days are often armed with devices with enormous zoom functions, meaning they could be watching every key you press when you're entering your username and password.
2. **Guess it.** You'd be surprised how easy it is for professional cyber criminals to simply *guess* other people's passwords. This is because there are common trends among certain age groups, demographics, locations and so on - hence the criticality of 100% unique passwords.
3. **A brute force attack.** This refers to instances where software is used to repeatedly attempt to

gain entry to a system by trying different passwords, over and over again. Often, hundreds of thousands of attempts per minute.

4. **A dictionary attack.** Similar to a brute force attack, this is where specialist dictionaries containing hundreds of thousands of words, technical terms, foreign language words and so on are used to automatically force entry to a system. Again, it's simply a case of bombarding the system with entries, until the correct password is found.

Using a Password Manager

The idea of a password manager is that rather than struggling to continuously assign, remember, change and memorise secure passwords on a regular basis, the software takes care of everything on your behalf. Effective password management software makes it quick and easy to store, back up and generally manage all your passwords.

What's more, it encrypts all your other passwords, which can only be accessed using a master password. Hence, you only need to remember this one master password, in order to gain access to the rest of your passwords.

What is a password manager?

A password manager can simplify the process of securing your computer, your network and your personal information in general. Just as long as you assign an effective master password, you can securely store all of your passwords for later retrieval at the touch of a button.

Why you should use it?

Password managers are particularly useful for those who find it difficult to remember every password they assign. If you use are the same password for more than one website or account, you're putting yourself at unnecessary risk of attack. In which case, using a password manager could be the answer.

How does it work?

Once again, it's simply a case of using a software package to store and safeguard your passwords. The password manager could be stored directly on your machine, or accessed remotely on the cloud. Either way, all you have to do is enter a master password, in order to gain access to your various credentials.

Of course, a password manager is only safe to use when the software itself is up to par. In addition, you also need to ensure that your master password is as robust as it can possibly be. In an organisational setting, it is not uncommon for two-factor authentication to be used to allow users access to password management systems.

Guidelines For Safe Internet Browsing

Safe Browsing

For all the advances in Internet security made over recent years, hackers are only ever one step behind. In fact, they sometimes find ways of pre-empting the efforts of cybersecurity experts. The term 'safe browsing' effectively means ensuring that the connection between the website and the computer/device accessing it is secured. By secured, we mean a safe connection that makes it impossible for cyber criminals to access and steal personal information, which may include payment information or personally-identifiable information that could be used for identity theft. When a secure connection is made, "https" can be seen in the URL instead of just http. Depending on the web browser, you may also see a small padlock icon, or a similar visual indicator of safety.

How do I know if a website is secure?

We're gradually reaching a point in time where the latest versions of the world's most popular web browsers provide warnings of unsafe websites. These days, it's likely that a upon attempting to enter an unsafe website, you will be informed by the browser and advised *not* to proceed. If you wish to proceed, you will need to specify this and override the in-built security protocols. Other than this, it's simply a case of checking the security status of the website as outlined above.

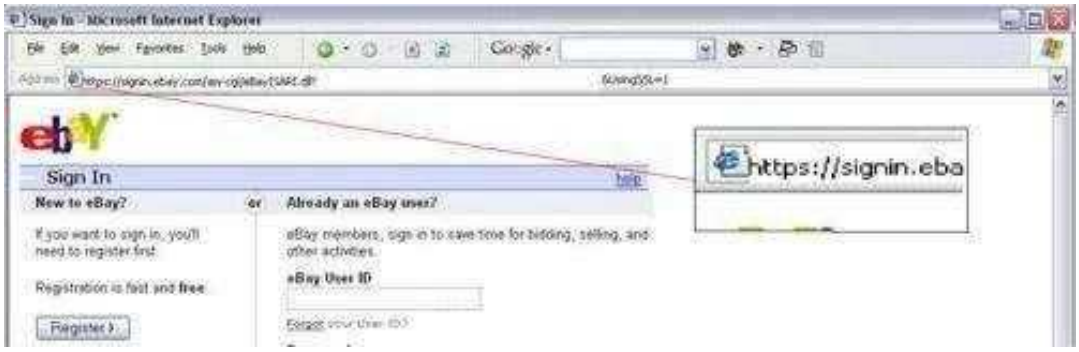


Fig. 3.5

Tips For Buying Online

Online retail is fast becoming the new standard for a new generation of consumers worldwide. Lured by the appeal of cheaper prices, limitless product availability and the convenience of shopping from home, millions are now shopping primarily or even *exclusively* online. Nevertheless, shopping online means submitting personal information and payment information, which will always carry risks. Risks that can be mitigated by following the guidelines below:

I. **Pay securely**: Don't make any payment unless:
   - You are on a secure website, and
   - The website encrypts and protects payment information

Once again, you will see one or more indicators on the page to indicate that it is a safe and secure website. As a reminder, these indicators are as follows:

- The URL begins with „https://", not „http://"
- The browser displays an image of a closed padlock or a similar icon

Unless there is complete verification of the security of the website, you should never submit any of your personal information or attempt to make a payment online. It is a risk not worth taking.

II. **Know the business:** If in any doubt whatsoever, establish and verify the reputation of the online business in question. Conduct as much research as necessary and check customer reviews to check whether or not they can be trusted and are worth doing business with.

III. **Know the product:** Make sure you check whether:

- The product is legal
- The product is suitable for your requirements
- All guarantees and warranties are valid in your country
- Some kind of warranty is provided
- The company offers a fair returns policy
- You understand all published terms and conditions
- You've carefully considered the privacy policy
- Customer feedback is generally positive
- The business clearly prioritises safety and security

IV. **Check additional costs**: The price you see isn't always the price you pay - added fees include:

- currency conversions
- local and national taxes
- postage and delivery fees
- insurance (where applicable)

Shopping online could save you money, but not *all* products and services sold online are as cheap as they appear to be at first glance.

V. **Protect your privacy**:

As mentioned above, you absolutely must check the seller's privacy policy and their terms and conditions document in full. By making a purchase, you agree to comply with all terms, conditions and policies published - you need to know what you're signing up for.

VI. **Keep records**: Always retain information about the company and other key documents such as:

- Confirmation of the order placed as soon as it is displayed
- Receipts generated automatically or sent to you by e-mail

You also need to ensure you have been charged the right amount by checking your:

- Credit card statement
- Merchant account statement (such as PayPal)
- Bank statement.

Don't forget that where currency conversion applies, you will be charged in accordance with the seller's conversion rate at the time.

VII. **Dispute auction issues**: If you run into an issue while shopping via a marketplace like eBay, it's essential to open a dispute immediately in the event that:

- The item you purchase doesn't arrive
- The item you sold isn't paid for
- The item you receive differs from the description
- The seller/buyer cuts off contact with you

Wireless Security

In this section, we will be discussing several important security best practices when using a wireless network.

What Is Wireless Lan?

The Wireless LAN or WLAN has taken over as the new standard for the vast majority of homes and businesses worldwide. As the name suggests, a Wireless LAN or WLAN is a wireless network, wherein any number of computers and devices are able to connect and interact with one another wirelessly. Wireless systems are as swift, seamless and simple to use as traditional wired systems, only with the convenience of eliminating cables from the equation.

The benefits of Wireless LAN or WLAN systems include the following:

1. No requirement for physical connections via cables for maximum convenience and versatility.
2. Freedom to position devices and computer systems in any location around the home or

office.

3. Outstanding value for money - Wireless LAN or WLAN has become the new standard for 21st century computing and is comprehensibly affordable.
4. Surprisingly easy to set up and operate, with little to no experience necessary.
5. The potential to be every bit as a secure a as a traditional wired network, if not more so.

Figure 3.6: A typical Wireless network

Major Issues with WLAN

Of course, it's not to say that the WLAN is by any means a flawless system. Across the board, all networks and computer systems are open to a wide variety of attacks. In fact, a typical WLAN may be significantly easier to penetrate than a comparable wired system. This applies only in instances where a WLAN is not properly configured, or hasn't been sufficiently safeguarded by those using or managing it. Some of the most common attacks directed at WLANs include Sniffing, Key cracking, DoS (Denial of Service), De-authentication attacks, War driving etc.

Rather than focusing on attacks specifically, it is more productive to consider the various ways a WLAN can be *protected* from the most common threats.

Secure WLAN

The security of any wireless network will always come down to three simple things:

- Whether or not the data being transferred is encrypted
- How the user or organisation looks for and reports suspicious activities
- The general education and awareness of the user

It is important to view WLAN security as a shared responsibility, which each and every user across the board contributes to in some way. It is not enough to simply expect the network manager or administrator to ensure the safety of the network on behalf of everyone else.

Wi-Fi at home

Wi-Fi has become a standard feature in the homes of hundreds of millions of people worldwide. To such an extent that the vast majority of us now take Wi-Fi for granted as an important (or even mandatory) part of our everyday lives. Unfortunately, research suggests that the vast majority of people also take the security of their home Wi-Fi technology for granted. Wi-Fi serves an important role, but does so in a silent and invisible manner.

Hence, how can you effectively protect and secure something you cannot see?

Protecting your wireless network at home is just as important as protecting your network in the workplace. The difference in this instance being that when you're provided with the basic hardware and software needed to set up a Wi-Fi system at home, it will initially only be safeguarded by the vendor's most basic security settings and protocols.

Subsequently, it is up to *you* to ensure that all the necessary safeguards are in place to protect your personal information, your identity and your financial data.

Unfortunately, there is no silver-bullet answer for the cybersecurity question at home. Instead, it's a case of using your own common sense, along with relevant countermeasures to ensure you are protected from attacks. Examples of which include the following:

Use a Firewall:

Your operating system will include some kind of built-in firewall as standard. However, it is up to you to take a look at the firewall in your system's Internet settings and ensure the necessary restrictions and allowances are in place.

Don't use Default Credentials:

Your router will most likely be installed with its factory-specified credentials in place. This means a username and password that are not only generic and not specified by you personally, but could even be indicated on the router itself. It's not uncommon for a router's original password to be printed on a label on the bottom of the router, which for obvious reasons constitutes a security threat. Always ensure that your router is protected with a strong username and password that cannot be guessed by anyone else.

Disable Auto-Connect:

It's also a good idea to be mindful about keeping your computers and devices connected to your Wi-Fi networks at all times. It can be tempting to use the "connect automatically" feature for convenience, but doing so could put your devices in harm's way.

Avoid Unknown Networks:

Believe it or not, it's not uncommon for households (and mobile device users) to attempt to connect to unknown Wi-Fi networks, in the event that their primary connection becomes unavailable. Irrespective of how much you need to get online and how legit any given network may appear, you should never connect to any unknown Wi-Fi source at any time. Do so and cyber criminals could watch and log everything you do from start to finish.

Safe Browsing Guidelines For Social Networking Sites

Contrary to popular belief, the concept of social networking is nothing new. To one extent or another, online communities have been around since the Internet itself first came into existence. From bulletin boards to online forums to email lists and so on, people have always used the Internet to connect with communities from around the world. It's just that today, the social networks we've come to rely on are significantly more sophisticated and user-friendly. Not to mention, accessible 24/7 via the devices we all carry in our pockets.

The thing that most people forget when using social media is the fact that every social network is an online business. The reason social networks are free to use is because the businesses behind them collect your personal information and use it to make money. Some of it is sold to third party businesses, some of it is used to target you with relevant advertising materials. Upon entering any social network whatsoever, you are immediately bound by the terms, conditions and privacy policies of the business in question. Your personal information may be hidden from public view, but is nonetheless provided for the social network itself to do with as it pleases.

As with all websites, therefore, it is essential to ensure you understand the extent to which you are both providing and permitting the use of your personal information. Social media privacy policies and terms and conditions documents are long and complex for a reason. It's technically mandatory for each and every user to consult these terms before using the services on offer, but evidence would suggest that fewer than one in every 100,000 users actually does so.

However you use social media, it is important to understand how to safeguard yourself from harm. Simply by understanding the basics, you'll be in a better position to protect yourself online.

General Tips on using Social Networking platforms safely

Social media is no less than an everyday essential for hundreds of millions of people worldwide. The problem being that much of the information we share on social media can be used by hackers to carry out criminal acts.

Detailed below are a few important tips and guidelines for staying safe with social media:

Always ask the questions:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me is being shared by my contacts?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone I'm connected with?

Additional guidelines to follow at all times include:

- Regularly consider the safety and security of the credentials you use to log on. If there's any chance anyone else might know your password, you should think about changing it.
- In any case, all your social media passwords should be changed every few weeks.
- Review the default security settings established by the social network itself, making adjustments as necessary in accordance with your preferences and requirements.
- Under no circumstances should you ever use the same password across multiple social media platforms, or any accounts you hold online.
- If you intend to access your social accounts in public places, do so only via a private connection and ensure nobody is looking over your shoulder at the time.
- Always remember that any information you share on your social pages is public and can be accessed by anyone. Even if you select the 'friends only' option or equivalent, it is still comparatively easy to access by today's sophisticated cyber criminals.
- Keep an eye out for suspicious activity and notify the social network of anything unusual immediately. For example, if anything appears on your post you didn't publish yourself.
- Never stay logged in when you aren't using your device, or use password 'auto-fill'. Should you lose your device, whoever finds it could gain immediate access to your accounts.
- Carefully check the terms, conditions and privacy policies of the social networks you use, in order to ensure you are willing and able to comply with all terms set out.

Posting Personal Details

There's a direct connection between the explosive popularity of social networking and the growing threat of identity theft. When signing up with a social network in the first place, it is usually a requirement to share a fair amount of personal information. Examples of which may include your date of birth, a contact telephone number and perhaps your home address. Nevertheless, this is all the kind of information that should never be shared publicly online. It's worth remembering that when a platform like Facebook automatically publishes a congratulatory message on your birthday, everyone in the world now knows your name *and* your date of birth.

Exactly the kind of information that makes identity theft much easier.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

Friends, Followers and Contacts

What's interesting about social media is the way in which people have a tendency to become far more trusting than they would be in real life. For some, it's simply a case of building the biggest possible database of 'friends' or 'followers', despite the fact that they don't actually know 99% of these people in the real world. They also have no real way of knowing whether the vast majority of these people can be trusted.

The more people you connect with online that you don't really know, the are more likely you are to fall victim to a cyber-crime. Your friends, followers and contacts might not launch an attack on you personally, but what about *their* friends, followers and contacts?

Status Updates

Social networks are routinely used by enormous audiences worldwide to effectively 'show off' whatever they're doing at the time. It's not unusual for people to post status updates several times per day, providing the world with insights as to where they are and what they are doing. Unfortunately, it can be difficult (or even impossible) to keep this information private. When you let your friends and contacts know what you are doing, you could be broadcasting this information to the rest of the world.

This is why you need to think very carefully about what you are saying and who you are saying it to. Is there a chance your current status update could put you in physical danger? Could it get you in trouble with one or more parties, if seen by the wrong people? Could it be used to blackmail you, if the information fell into the wrong hands?

Status updates are a fun way of keeping in touch, though have resulted in countless people losing their jobs, or the demise of their relationships. It's always worth remembering that on social media, there really isn't such a thing as 100% 'private' information. It all has the potential to go public at any time.

Revealing your Location

As touched upon, it's up to you to determine whether or not it's a good idea to share your location online. Even if you don't share your location, there's a good chance the social network is tracking your every move. It's pretty much the norm these days for social networks to make use of GPS-enabled devices, in order to track the movements of their subscribers and use the information to their advantage. Not in any malicious way - more for marketing and promotional purposes.

Nevertheless, this still means that a log is being kept somewhere of your movements, whenever you are online and using a GPS-connected device. If you'd prefer not to be tracked, you can always deactivate your device's GPS, or turn 'location settings' off.

Sharing Videos and Photos

The average social media user these days shares any number of photos on a daily basis. The problem being that many do not realise just how much information a single photo can contain. Along with the individuals present in the picture, a photograph can make it clear where you are at the time. With geotagging, even a relatively nondescript photograph can be traced back to the location from which it was taken.

For example, take a picture at home, share it online and there's a good chance it could be used to work out where you live. Combined with information like your date of birth, your full name and your e-mail address, this could be all that's needed to hijack your identity. For obvious reasons, you should never post a photograph of anyone else on any social platform, without first gaining their consent.

Instant Chats

A growing number of social platforms now provide their users with instant chat facilities, which allow individuals and groups thereof to communicate in real-time. Instant chat facilities can be both convenient and enjoyable to use, but must nonetheless be approached with caution. Just like social media in general, you need to be mindful of who may be monitoring your actions and communications at the time.

Most major social networks are predominantly safe, but the same cannot necessarily be said for your Internet connection. For example, if you are using a public Wi-Fi network and a chat facility, there's a chance your conversation could be monitored by someone else. One of many reasons why it is important to avoid using public shared Wi-Fi connections where possible - especially when sharing private information.

In addition, it is inadvisable to share any sensitive information on an instant chat facility, with any individual you do not know well enough to trust.

Joining and Creating Groups, Events and Communities

When you join a group or community on social media, you have the opportunity to make invaluable connections with like-minded people. The same also goes for organizing events - particularly when you invite people to sign up who aren't already within your network. One of the biggest points of appeal with social media being the ability to *extend* your network and meet new people.

Unfortunately, joining a group or community inherently means entering into a 'collective' with people you don't know. More often than not, there's nothing particularly risky about joining groups or communities. Nevertheless, there's still a chance that one or more people within the group might not be who they appear to be. Whichever way you look at it, you are effectively communicating with strangers for the time being, and should therefore take precautions accordingly.

Until you are completely confident in *every* member of the group or community, it is inadvisable to share any sensitive information. Would you normally hand pictures of yourself and your personal information to strangers you encounter when walking down the street? It's exactly the same with social media, only for some reason people tend to be far more liberal with the information they distribute online.

Once again, it's a case of protecting your identity and not putting yourself at unnecessary risk. While the chances of being targeted are relatively slim, it's important to remember that cybercriminals are opportunists. If they find an easy target - i.e. someone publicly broadcasting their private information to the world - they'll take advantage.

Email Security Tips

Most people receive an astonishing amount of 'spam' on a daily basis. Most of which is filtered, though some will always find its way into your inbox. The good news being that the vast majority of spam content received is technically harmless, if somewhat irritating. Nevertheless, there are several essentially email security guidelines to be aware of, in order to avoid falling victim to cybercriminals.

Examples of which include the following:

1. If you receive an e-mail attachment you were not expecting, under no circumstances should you open it. The same also applies to any email attachments that come from sources you are not familiar with. Never open an attachment or download any files to your computer, unless you know where they came from and are sure they are safe.

2. Ensure your anti-virus software is active, up to date and configured to block malware transmitted by email. In addition, it's also important to use a reliable and reputable e-mail service like Gmail, which automatically scans emails for viruses upon their arrival. If any warnings or alerts are generated, they should be taken seriously.

3. The best way to avoid being targeted by spam and erroneous emails in general is to stop sharing your e-mail address so liberally. It's worth remembering that each time you enter your e-mail address online for any reason, it is probably shared with hundreds or even thousands of sources. Guard your email and share it only when absolutely necessary.

4. Ensure that any spam messages that make it to your inbox are flagged as spam and reported where appropriate. If you come across an e-mail that is remotely suspicious, it is *your* responsibility to report it to your ISP and e-mail service provider as quickly as possible.

5. You also need to familiarise yourself with the warning signs of 'phishing' emails. This is where an e-mail appears to come from a legitimate source - eBay, PayPal, a bank, HMRC etc. - though was actually sent by a cybercriminal. Almost everything about the e-mail looks legit, including the request to "update your personal information". Upon receiving any such e-mail, always telephone the source and verify its authenticity, before going any further.

6. Always carefully check the e-mail address the communication has come from, in order to verify its source. If an e-mail has indeed come from eBay's support team, this should be apparent in the source email address. You can always copy and paste this e-mail address into Google, in order to see if it has been flagged as fraudulent.

Smartphone Security

Introduction

The overwhelming majority of people now carry a pretty sophisticated computer with them in their pockets. Today's smartphones are more powerful and feature-packed than the average PC or laptop was just a few years ago. What's more, smartphones are also connected to the Internet on a 24/7 basis. This means that even while you sleep, your mobile device is getting up to a wide range of activities in your absence.

Mobile phones were once used for making calls and exchanging text messages - they're now the kinds

of lifestyle aids the world has come to rely on.

Almost everything you can do on your home computer is something you can do on your mobile device. But what many (or most) fail to realise is how every smartphone (and mobile device in general) is as open to attack as any home computer. If not, considerably more so. Nevertheless, some people go to extreme lengths to safeguard their computers and wireless networks at home, though do nothing to protect their mobile devices.

As already touched upon, the vast majority of mobile devices have in-built GPS functionality. While this is necessary for things like satellite navigation and mapping, it also provides your service provider with a complete and real-time record of your movements. Each time you take a photograph, additional information like the date, time and location is stored (or even transmitted) automatically.

Deactivating these 'locations settings' is an option, though can have a negative impact on various apps and features.

Smartphone Security Guidelines

Purses, Wallets, Smartphones

It's safe to say that most of us hold our wallets and purses in high regard. Or to put it another way, we're fundamentally aware of the value of their contents and will do whatever we can to take care of them. Nevertheless, evidence would suggest that people aren't nearly as aware of the value of the contents of their mobile devices. We consider losing a wallet or purse to be a disaster, whereas temporarily misplacing a mobile phone is more of an inconvenience.

Something that's often overlooked is the way in which a smartphone is connected to the Internet on a 24/7 basis. To an extent, this also technically means that every bit of data stored on your mobile device is accessible by others. That is, unless you proactively defend your device from attacks - something the majority of people simply aren't doing.

Compare your purse or wallet to your mobile device:

A simple exercise can illustrate the importance of safeguarding your mobile device. If you were to empty the contents of your wallet or purse, you may find two bank cards, two credit cards, a gym membership card, a driving licence, a couple of pictures of your loved ones and a quantity of cash.

By contrast, gain unauthorized access to someone's mobile device and you gain access to the following items:

- Thousands of pictures of friends and family
- Email applications and their passwords
- Access to thousands of emails
- Social networking applications and their passwords

- Banking applications (with access to bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information
- A complete record of your recent movements and activities

The greater the extent to which we rely on our mobile devices, the more dangerous they become. Or at least, dangerous if they are not sufficiently safeguarded. Smartphones collect an extraordinary quantity of information about us, every hour of every day. They also transmit much of this information to the internet and the everyday communication service providers we work with. Worse still, it's comparatively easy for today's sophisticated cybercriminal to hack into this information and do whatever they want with it.

Backing up your information is one thing - ensuring it doesn't fall into the wrong hands is another.

Specific precautions related to common uses of smartphones.

Platforms, Setup and Installation

Platforms and Operating Systems

Right now, the overwhelming majority of mobile devices worldwide are powered by Google's Android or Apple's iOS operating systems. Both of which are considered to be predominantly safe, but offer no guarantees as such. In order to ensure the safety of your device, it is important to ensure that you are running the latest version of your preferred operating system accordingly. In addition, it's worth noting that any alterations made to the backend (coding) of the software could compromise its security.

There's still a relatively robust market for Windows Phone and BlackBerry devices, but they account for only a small proportion of the total global smartphone market.

Feature Phones

Interestingly, 'feature phones' that are not nearly as sophisticated as a typical smartphone can be significantly more secure. It's the classic catch-22 situation - the more sophisticated a device becomes, the easier it becomes for cyber criminals to hack it. It's not to say that feature phones *cannot* be targeted by cyber criminals, but the vast majority tend to focus their efforts on more sophisticated smartphones, tablets and connected mobile devices in general.

General Setup

When you buy a new mobile device, it will ship with its default factory settings. This means you will need to set up the device to suit your preferences and requirements. If you are unfamiliar with the way mobile devices work, it's advisable to go with the general/generic settings using the 'auto' setup feature. However, doing so will usually turn things like location settings and ad targeting on. If you don't want your phone to be tracked for marketing purposes, you'll need to alter the settings manually.

In any case, it's perfectly possible to change all important settings on your device at a later date, if you wish to do so.

Installing and Updating Applications

As already touched upon, it is of the utmost importance to ensure your mobile operating system is kept up to date at all times. However, the same also applies to all mobile applications across the board. Each and every application has its own security flaws and general performance issues. As a result, developers are continuously searching for potential issues with their software, in order to implement 'patches' and fixes before hackers gain the upper-hand.

This is why the vast majority of apps on the average mobile device are updated on such a regular basis. Continuously updating apps to the latest version can be a nuisance, but is nonetheless mandatory for the safety of your device. It's entirely up to you whether you activate or deactivate automatic updates, but it's typically advisable to keep it active. Otherwise, you may miss out on an important update that's needed to protect your device from a potential security risk.

It's equally important to be mindful of the applications you install on your device in the first place. When browsing the world's biggest app libraries, it's hard *not* to take things for granted. You simply assume the apps you come across are safe, downloading them onto your device without a second thought. Nevertheless, if you don't carry out the necessary checks to ensure the safety of the app, you could be headed for disaster.

Use customer ratings, feedback and recommendations as a guide, while carrying out Google searches to verify the quality and authenticity of any unknown apps you intend to download.

Communicating Securely (Voice and Messages) with a Smartphone

Secure Voice Communication

Basic telephony

Eavesdropping has become even more commonplace in the era of smartphone technology. These

days, it's perfectly possible for a mobile device to be configured to record, store and transmit the sounds its microphone picks up, even when it is deactivated. Or to put it another way, you think your phone is switched off, but it's actually recording you…or it could be.

Again, the likelihood of falling victim to this kind of invasion of privacy is relatively low. Nevertheless, it represents an ongoing threat that should be both acknowledged and taken seriously. Simple measures to avoid falling victim to eavesdropping include the following:

- Don't let anyone you do not know and don't implicitly trust gain physical access to your device while out of your sight. Installing spyware on a mobile device is surprisingly quick and easy to pull off.
- If you are disclosing private or important information of any kind, you might want to think about turning off your phone and removing the battery. Alternatively, ensure your device is out of reach and therefore cannot pick up anything you say.
- Don't forget that the communication could be intercepted on the *other* side of the conversation. You therefore need to ensure that the other party follows the same basic safety protocols as you.
- In terms of traditional eavesdropping, it's the classic case of being aware and cautious of anyone who may be around you at the time. Where confidential and sensitive information needs to be communicated, it's worth ensuring you're in a secluded and private location.

Even where voice and text communications are encrypted by service providers, general encryption standards are somewhat weak. As a result, it isn't particularly difficult for hackers to intercept everyday communications, decrypt the information and do whatever they want with it. In addition, it's worth remembering that your cellular service provider will have a complete record of *all* of your text and voice communications. None of which is likely to be used for illegal means - more for marketing and security purposes.

There are some Smartphones on the market that are designed to encrypt all communications to a military standard. Nevertheless, they are relatively rare and comparatively expensive. The good news being that the likelihood of your everyday communications via mobile devices being hijacked is relatively minimal. As a result, it's simply a case of taking common sense precautions.

Along with the above, it's sensible to avoid communicating any particularly sensitive information over the phone that doesn't *need* to be communicated. If it's something deeply personal, financially sensitive or has the potential to get you in trouble, you might want to think about who could be listening at the time. It's unlikely anyone will be listening, but just in case - common sense prevails.

Skype

Skype is the world's most popular VoIP platform, used by hundreds of millions of people and businesses worldwide. Initially available exclusively for desktop PCs and laptops, Skype is now a

standard feature on the vast majority of smartphones and tablets. The safety (or otherwise) of Skype remains a topic of some debate, as it is difficult to independently confirm the security of a non-open-source piece of software. Microsoft makes continuous claims regarding the safety of Skype, while others insist it is just as open to eavesdropping and general cyber attacks as any other communication platform.

In any case, Microsoft keeps a complete record of all Skype communications, so it's important to be wary of the information you share on Skype.

SMS

The popularity of traditional SMS communication across many western markets is diminishing all the time. This is due to the growing popularity of applications like WhatsApp, which along with expanding the versatility of text messaging also allow users to communicate for free. Irrespective of whether you use WhatsApp or SMS, however, neither is considered completely safe.

SMS communications are fundamentally unsecure, while WhatsApp (and similar platforms) are as open to attack as any other social network. With WhatsApp, you also need to be mindful of things like geotagging when sending pictures and videos. Again, as there are no guarantees your communications are 100% safe, you need to think carefully about the information you are transmitting by way of text message.

Securing SMS

There are several tools and apps available that can be used to send text messages more securely. One example of which being TextSecure, which securely encrypts messages when they are sent and decrypts them at the point of receipt. In order for the service to be used, both parties need to have the TextSecure tool set up on their device. The communication could still technically be intercepted by a hacker, but it would be near-impossible for them to decrypt the message and access the information therein.

Sending Email from your Smartphone

Using a smartphone to send and receive e-mail can be exceptionally convenient. In fact, millions of people have come to rely on their mobile devices as their primary e-mail communication tools.

However, there are certain risks that accompany sending and receiving e-mails by way of mobile device. The vast majority concerning the way in which what is far easier for a smartphone to be stolen, monitored or hacked into than a traditional computer.

It can be preferable (or even necessary) to use your mobile device to send and receive emails. In which case, it is essential to bear the following precautions in mind:

- Downloading and storing copies of sensitive emails on your mobile device is inadvisable. Should anyone gain unauthorised access to your device at any time, a touch of the screen will be all that's needed to access your inbox and all the information it contains.
- Try to get into the habit of logging out of your inbox when you are not using it. This is particularly important when out and about in public, as you never know who may have their sights set on your mobile device.
- Avoid using public or shared Wi-Fi connections at all costs. Under no circumstances should you ever send or download important email communications via shared connections, which are far too easy for cybercriminals to monitor.
- Take care when entering your username and password in public - there's always the chance you're being watched.

Wi-Fi or Mobile Data?

Realistically, the safest way to communicate any data whatsoever is via your own secured Wi-Fi connection. While it's not to say cellular isn't predominantly safe, it's technically a shared and open connection anyone can use and/or hack into. Secured Wi-Fi connections can never be guaranteed 100% safe, but are nonetheless the safest available option for the time being.

Again, it's impossible to overstate the importance of avoiding shared Wi-Fi connections where possible. Each and every key you press could be tracked, logged and used by hackers for any purpose they see fit. Even if you're not doing anything particularly important or confidential at the time, they could still gain access to your computer, your passwords and your personal information.

Unless it is absolutely necessary, limit your online activities (particularly those of a sensitive nature) to secure Wi-Fi connections you can trust.

Further Reading:

- ✓ ***CYBER SECURITY LAW, CYBER SECURITY LAW, by PAVAN DUGGAL Jan 17, 2019***
- ✓ ***How to Become a Cyber-Security Analyst: Phase 1, Paul Oyelakin, Sep 30***