Topic: 1.4 Security

1.4.1 Importance of Security and Data Integrity.

Data security deals in the area of keeping data safe. It includes preventing unauthorized personnel from retrieving it, moreover preventing it from damage or intentional destruction, infection or corruption. If the data is recovered, stolen, copied, or damaged from these computer systems then it can lead to a serious problems.

Data integrity is the counterbalance of data in both during and after processing.

Data may get:

- Lost or damaged during a system crash - especially if the crash affects the hard disk.
- Corrupted as a result of faulty disks, disk drives, or power failures.
- Lost by accidentally deleting or overwriting files.
- Lost or become corrupted by computer viruses.
- Hacked by unauthorized users and deleted or redact.
- Destroyed by natural disasters, in acts of terrorism, or war
- Deleted or altered by employees wishing to betray the company in order make money or as the act of revenge or Blackmail.

How to keep your data safe from accidental damage, human errors and corruption?

Measures that can be taken to keep data secure include:

- Making regular backups of files (backup copies should be stored in fireproof safes or away from the place of origin e.g. another building)
- Protecting your computer against viruses by running an anti-virus check every once in a while
- Use a password protected computer so that access to data is restricted.
- Safe storage of important files stored on removable disks, e.g. locked away in a fireproof and waterproof safe. How much you invest on secure data storage all depends on how important your data really is.
- Allowing only authorized staff into certain computer areas, e.g. by controlling entry to these areas by means of ID cards, magnetic swipe cards, or biometric scanners.
- Always logging off or turning terminals off when not in use and if possible locking them by means of physical lock.
- Avoiding accidental deletion of files by write-protecting disks
- Using data encryption techniques to code data so that it makes no apparent sense.

Topic: 1.4 Security

Accidental damage

Accidental damage refers to the damage caused unintentionally, like deletion of data while the person is unaware of its consequences. Or damage of data by removing important files without intent or amending data without checking new arrivals. To prevent such damages, a well-organized backup is required.

The main factors that had to be on field are:

1) **Medium** – such as Magnetic tapes, CD-RW, external storage devices, zip drive.
2) **Location** – where the medium should be stored, e.g. off site in a fire proof safe.
3) **Type of backup** – full (all data, program and its features) or partial (just the sensitive data changing everyday like in banks or airports)
4) **Timings** – at what time intervals should the data be backed up? e.g. at the end of working data, end of working in morning shift, end of day, end of week, every hour (it all depends on how important your data is, and on your medium space availability)
5) **Testing** – backups needs to be examined i.e. recoverable or not at an instance.

A best example of a suitable backup for students working on a project at school and at home would be:

- Take a copy on to a USB on a regular basis (at the end of each period, lesson or when you're done working on it at home).
- Keep an extra copy in a safe place at home.
- Test the backup to ensure that both the copies work at school and at home.

Getting familiar with malicious actions, including unauthorized viewing, copying and corruption.

It is convenient to have access to vast content on the Internet such as important information, useful services and wonderful entertainment but unfortunately by accessing the Internet, you leave yourself vulnerable to some trouble makers who are waiting for an opportunity to harm you and your computer. Yes, we're talking about computer viruses, spyware/adware and hackers.

Computer viruses, spyware and adware! What these species are?

Computer viruses are software programs designed to access your computer without your consent, interfere with your computer's operation and records, corrupts, or deletes your personal data.

Adware are software programs designed for advertising and changing your computer's configuration. Spyware is software designed to collect personal information like what websites you visit or even discreetly transmit your personal information, such as your credit card number from your computer without your knowledge.

Topic: 1.4 Security

Another threat over the internet is of "Hackers". The term hacker is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

How hectic could they be?

While viruses can be intentionally destructive, for example, by destroying data, many viruses are fairly benign or just plain annoying. Adware is mainly annoying but spyware can be downright dangerous if it manages to get hold of important information like your passwords or credit card information. Hackers can breaks into someone else's computer system, often on a network; by passes, passwords or licenses in computer programs or in other ways intentionally breach computer security.

How does a person know if his/her computer is infected?

The worse with viruses, adware/spyware and hackers are that they silently operate for a relatively long period of time in your computer without being detected. Therefore it's very important to follow the preventive methods described later in this guide. The common symptoms of a virus infection are that your computer works slower than normal, it stops responding and freezes often, crashes and restarts frequently or fails to run normally. Other possible symptoms are that the applications don't work properly and you can't print correctly, the discs and disc drives on your computer are inaccessible and you often see unusual error messages.

The signs of spyware or adware infection are similar to the signs of a computer virus infection, but in addition to those you might get unwanted pop-up windows on your screen even if you're not browsing in the Internet, your web browser's start up page can be different than it should be or you might notice an unwanted toolbar on your web browser.

It can be difficult to detect a hacker on a computer because nothing changes to help disguise the hack. Below are the most common things that change after a computer is hacked.

- New programs installed
- Computer passwords have changed
- Increased network activity
- Unknown programs wanting access
- Security programs uninstalled
- Computer doing things by itself

Topic: 1.4 Security

1.4.2 How can a computer get rid of intruders?

The idea of having unwanted software running on your computer is scary; by following a few easy steps you can keep your computer free from viruses, adware, spyware and other trouble makers.

Installing a fire wall

An Internet firewall is a computer program or hardware appliance designed to prevent unauthorized access to private computers or networks. Firewall screens out viruses, worms, malware and hackers that try to access your computer over the Internet. Installing a firewall is the most effective and the most important first step you can take to protect your computer. Install the firewall before you access the Internet for the first time and keep it running at all times.

Firewalls can be either hardware or software but the ideal firewall configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access to your computer.

How it works?

A firewall enforces a policy or set of rules governing the flow of data to and from the outside world. Firewalls that are used to protect home computers are usually based on packet filtering, i.e. Data packets (small units of information) are admitted or rejected according to the way these rules are configured. For the typical home user their primary function is to block uninvited incoming connections. Most firewall tools will come with a sensible set of rules by default.

Firewalls are setup at every connection to the Internet, therefore subjecting all data flow to careful monitoring. Firewalls can also be tuned to follow "rules". These Rules are simply security rules that can be set up by you or by the network administrators to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owners/administrators immense control over the traffic that flows in & out of their systems or networks.

Rules will decide who can and cannot connect to the internet, what kind of connections can be made, which or what kind of files can be transmitted in and out. Basically all traffic in & out can be watched and controlled thus giving the firewall installer a high level of security & protection.

Topic: 1.4 Security

Firewall's logic

Firewalls use 3 types of filtering mechanisms:

- **Packet filtering or packet purity**
  Data flow consists of packets of information and firewalls that analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.

- **Proxy**
  Firewalls in this case assume the role of a recipient & in turn sends it to the node that has requested the information & vice versa.

- **What is a proxy server?**
  A proxy server is computer that functions as an intermediary between a web browser (such as Internet Explorer) and the Internet. Proxy servers help improve web performance by storing a copy of frequently used webpages. When a browser requests a webpage stored in the proxy server's collection (its cache), it is provided by the proxy server, which is faster than going to the web. Proxy servers also help improve security by filtering out some web content and malicious software.
  Proxy servers are used mostly by networks in organizations and companies. Typically, people connecting to the Internet from home will not use a proxy server.

- **Inspection**
  In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing and request & check for the same matching characteristics in the inflow to decide if it is relevant information that is coming through.

Firewall rules

Firewall rules can be customized as per your needs, requirements & security threat levels. You can create or disable firewall filter rules based on conditions such as:

IP Addresses
Blocking off a certain IP address or a range of IP addresses, which you think are predatory. What is my IP address? Where is an IP address located?

Domain names
You can only allow certain specific domain names to access your systems/servers or allow access to only some specified types of domain names or domain name extension like (.edu or .mil).

Topic: 1.4 Security

Protocols
A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP, ICMP, Telnet or SNMP.

Ports
Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for & also close down possible entry points for hackers or malignant software.

Keywords
Firewalls also can sift through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in.

Firewalls are a must have for any kind of computers that go online. They protect you from all kinds of abuse & unauthorized access like Trojans that allow taking control of your computers by remote logins or backdoors, virus or use your resources to launch DOS attacks.
Firewalls are worth installing. Be it a basic standalone system, a home network or an office network, all face varying levels of risks & Firewalls do a good job in minimize these risks. Tune the firewall for your requirements & security levels and you have one less threat to worry about.

How passwords are essential in keeping data safe while stored and transmitted

Passwords are very important in keeping your online information safe. What is very important is the strength of the password that you choose. Your password should meet the following criteria:

- Be at least 6 - 8 characters
- Contain at least one character from ALL of the following four classes:
  Uppercase letters (e.g. A, B, C), Lower case letters (eg. a, b, c), Numbers (eg. 1, 2, 3), Punctuation symbols (e.g. ~!@#$%^&*()+-=)
- Doesn't contain your first name, your last name, your user ID, the word Optus, SingTel, a day of the week, month of the year or the word password.
- Is not a common word or keyboard sequence (e.g. 123, QWERTY, asdf, zxcv, poiuy).
  You should change your password regularly and never share your password to others.

For more efficient security**, Biometric** passwords give more security.

Topic: 1.4 Security

Biometric passwords

Biometric password systems use handwriting, hand geometry, voiceprints, iris structure and vein structure. You'll also learn why more businesses and governments use the technology and whether contact lenses fake, recorded voice and silicone hand could really get James Bond into the lab (and let him save the world).
You take basic security precautions every day you use a key to get into your house and log on to your computer with a username and password. You've probably also experienced the panic that comes with misplaced keys and forgotten passwords. It isn't just that you can't get what you need -- if you lose your keys or wrote your password on a piece of paper, someone else can find them and use them just as you would.

Instead of using something you have (like a key) or something you know (like a password), biometrics use **your body** to identify you. Biometrics can use **physical characteristics**, like your face, fingerprints, irises or veins, or **behavioral characteristics** like your voice, handwriting or typing rhythm. Unlike keys and passwords, your personal traits are extremely difficult to lose or forget. They can also be very difficult to copy. For this reason, many people consider them to be safer and more secure than keys or passwords.

Biometric systems can seem complicated, but they all use the same three steps:

- **Enrollment**: The first time you use a biometric system, it records basic information about you, like your name or an identification number. It then captures an image or recording of your specific trait.
- **Storage**: Contrary to what you may see in movies, most systems don't store the complete image or recording. They instead analyze your trait and translate it into a code or graph. Some systems also record this data onto a **smartcard** that you carry with you.
- **Comparison:** The next time you use the system, it compares the trait you present to the information on file. Then, it either accepts or rejects that you are who you claim to be.

Systems also use the same three components:

- A **sensor** that detects the characteristic being used for identification
- A **computer** that reads and stores the information
- A **Software** that analyzes the characteristic, translates it into a graph or code and performs the actual comparisons

Next, we'll examine how biometrics provides security using other traits, starting with handwriting.

Handwriting

At first sight, using handwriting to identify people might not seem like a good idea. After all, many people can learn to copy other people's handwriting with a little time and practice. It seems like it would be easy to get a copy of someone's signature or the required password and learn to forge it.

Topic: 1.4 Security

But biometric systems don't just look at how you shape each letter; they analyze the act of writing. They examine the pressure you use and the speed and rhythm with which you write. They also record the sequence in which you form letters like whether you add dots and crosses as you go or after you finish the word.

Unlike the simple shapes of the letters, these traits are very difficult to forge. Even if someone else got a copy of your signature and traced it, the system probably wouldn't accept their forgery. A handwriting recognition system's sensors can include a touch-sensitive writing surface or a pen that contains sensors that detect angle, pressure and direction. The software translates the handwriting into a graph and recognizes the minute changes in a person's handwriting from day to day and over time.

Hand and finger geometry

Individual's hands and fingers are unique -- but not as unique as other traits, like fingerprints or irises. That's why businesses and schools, rather than high-security facilities, typically use hand and finger geometry readers to **authenticate** users, not to **identify** them. Disney theme parks, for example, use finger geometry readers to grant ticket holders admittance to different parts of the park. Some businesses use hand geometry readers in place of timecards.

Systems that measure hand and finger geometry use a digital camera and light. To use one, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. It uses this information to determine the length, width, thickness and curvature of your hand or fingers. It translates that information into a numerical template.

Hand and finger geometry systems have a few strengths and weaknesses. Since hands and fingers are less distinctive than fingerprints or irises, some people are less likely to feel that the system invades their privacy. However, many people's hands change over time due to injury, changes in weight or arthritis. Some systems update the data to reflect minor changes from day to day.

Voice prints

Your voice is unique because of the shape of your vocal cavities and the way you move your mouth when you speak. To enroll in a voiceprint system, you either say the exact words or phrases that it requires, or you give an extended sample of your speech so that the computer can identify you no matter which words you say.

When people think of voiceprints, they often think of the wave pattern they would see on an oscilloscope. But the data used in a voiceprint is a sound **spectrogram**, not a wave form. A spectrogram is basically a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds create different shapes within the graph. Spectrograms also use colors or shades of grey to represent the acoustical qualities of sound. Some companies use voiceprint recognition so that people can gain access to information or give authorization without being physically present. Instead of stepping

up to an iris scanner or hand geometry reader, someone can give authorization by making a phone call. Unfortunately, people can bypass some systems, particularly those that work by phone, with a simple recording of an authorized person's password. That's why some systems use several randomly-chosen voice passwords or use general voiceprints instead of prints for specific words. Others use technology that detects the artifacts created in recording and playback.

Iris scanning

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris. When you look into an iris scanner, either the camera focuses automatically or you use a mirror or audible feedback from the system to make sure that you are positioned correctly. Usually, your eye is 3 to 10 inches from the camera. When the camera takes a picture, the computer locates:

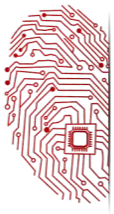
- The center of the pupil
- The edge of the pupil
- The edge of the iris
- The eyelids and eyelashes

It then analyzes the patterns in the iris and translates them into a code. Iris scanners are becoming more common in high-security applications because people's eyes are so unique (the chance of mistaking one iris code for another is 1 in 10 to the 78th power. They also allow more than 200 points of reference for comparison, as opposed to 60 or 70 points in fingerprints.

The iris is a visible but protected structure, and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings.

Use of SECURE SOCKET LAYER (SSL)

Organizations that use the Web to collect and transmit sensitive data to customers or other organizations need to secure their Web site. The general standard is the use of secure socket layers (SSL), which encrypts data transmitted via a Web site. Upon opening an Internet browser, an open or closed lock appears in the lower right hand corner of the Web site. If the lock is closed, it means the data transmitted over the Web site is secure, generally by SSL. This allows the transmission and collection of private data over a Web site, without worrying about a hacker accessing it. There is no such thing as security without risks, but the use of SSL and secure Web sites when transmitting data significantly reduces the risk of it being inappropriately intercepted. Secure Web sites can be established by using internal Web analysts/programmers or working with a vendor who has expertise in creating an appealing and secure Web experience. SSL uses both symmetric and asymmetric encryption algorithms. Symmetric algorithms use the same key to encrypt and decrypt data. They are faster than asymmetric algorithms but can be



Topic: 1.4 Security

insecure. Asymmetric algorithms use a pair of keys. Data encrypted using one key can only be decrypted using the other. Typically, one of the keys is kept private while the other is made public. Because one key is always kept private, asymmetric algorithms are generally secure; however, they are much slower than symmetric algorithms. To reap the benefits of both algorithms, SSL encapsulates a symmetric key that is randomly selected each time inside a message that is encrypted with an asymmetric algorithm. After both the client and server possess the symmetric key, the symmetric key is used instead of the asymmetric ones.

When server authentication is requested, SSL uses the following process:

1. To request a secure page, the client uses HTTPS.
2. The server sends the client its public key and certificate.
3. The client checks that the certificate was issued by a trusted party (usually a trusted Certificate Authority) that the certificate is still valid, and that the certificate is related to the contacted site.
4. The client uses the public key to encrypt a random symmetric encryption key and sends it to the server, along with the encrypted URL required and other encrypted HTTP data.
5. The server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and HTTP data.
6. The server sends back the requested HTML document and HTTP data that are encrypted with the symmetric key.
7. The client decrypts the HTTP data and HTML document using the symmetric key and displays the information.

SSL versus TLS

SSL TLSTLS (Transport Layer Security) and SSL (Secure Sockets Layer) are protocols that provide data encryption and authentication between applications and servers in scenarios where that data is being sent across an insecure network, such as checking your email (How does the Secure Socket Layer work?). The terms SSL and TLS are often used interchangeably or in conjunction with each other (TLS/SSL), but one is in fact the predecessor of the other — SSL 3.0 served as the basis for TLS 1.0 which, as a result, is sometimes referred to as SSL 3.1. With this said though, is there actually a practical difference between the two?

Which is more secure – SSL or TLS?

It used to be believed that TLS v1.0 was marginally more secure than SSL v3.0, its predecessor. However, SSL v3.0 is getting very old and recent developments have shown that SSL v3.0 is now completely insecure. As SSL v3.0 is effectively “dead” as a useful security protocol. Places that still allow its use for web hosting as placing their “secure web sites” at risk. Unfortunately, even now a majority of web sites do not use the newer versions of TLS and permit weak encryption ciphers.

Topic: 1.4 Security

What happens if I do not select either one?

If neither SSL nor TLS is used, then the communications between you and the server can easily become a party line for eavesdroppers. Your data and your login information are sent in plain text for anyone to see; there is no guarantee that the server you connect to is not some middle man or interloper. For more on this, see: the case for email security.

ENCRYPTION

The translation of data into a secret code. Encryption is the most effective way to achieve ***data security***. To read an encrypted file, you must have access to a secret key or password that enables you to ***decrypt*** it. Unencrypted data is called ***plain text*** ; encrypted data is referred to as ***cipher*** *text*.

Security Encryption Systems

Computer encryption is based on the science of cryptography, which has been used as long as humans have wanted to keep information secret. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

The Greek historian Plutarch wrote, for example, about Spartan generals who sent and received sensitive messages using a scytale, a thin cylinder made out of wood. The general would wrap a piece of parchment around the scytale and write his message along its length. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense. But if the other general receiving the parchment had a scytale of similar size, he could wrap the paper around it and easily read the intended message.

The Greeks were also the first to use ciphers, specific codes that involve substitutions or transpositions of letters and numbers. As long as both generals had the correct cipher, they could decode any message the other sent. To make the message more difficult to decipher, they could arrange the letters inside the grid in any combination.

Most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer to crack. Ciphers are also better known today as algorithms, which are the guides for encryption -- they provide a way in which to craft a message and give a certain range of possible combinations. A key, on the other hand, helps a person or computer figure out the one possibility on a given occasion.

Computer encryption systems generally belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption (Not is syllabus)

Topic: 1.4 Security

Symmetric Key

Just like two Spartan generals sending messages to each other, computers using symmetric-key encryption to send information between each other must have the same key.

In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.

The same goes for computers, but, of course, the keys are usually much longer. The first major symmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES), uses a 56-bit key.

Because computers have become increasingly faster since the '70s, security experts no longer consider DES secure -- although a 56-bit key offers more than 70 quadrillion possible combinations (70,000,000,000,000,000), an attack of brute force (simply trying every possible combination in order to find the right key) could easily decipher encrypted data in a short while. DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption standard for a long time coming: A 128-bit key, for instance, can have more than 300,000,000,000,000,000,000,000,000,000,000,000,000 key combinations [source: CES Communications].

Getting known to the need of keeping online systems safe from attacks including denial of service attacks, phishing, pharming.

Denial of Service Attacks (DoS)

DoS stand for Denial of Service. A malicious hacker uses a DoS attack to make a computer resource (i.e. – website, application, e-mail, voicemail, and network) stop responding to legitimate users. The malicious hacker does this by commanding a fleet of remotely-controlled computers to send a flood of network traffic to the target. The target becomes so busy dealing with the attacker's requests that it doesn't have time to respond to legitimate users' requests. That can cause the target system to stop responding, resulting in long delays and outages.

Topic: 1.4 Security

What is a pharming scam?

Phishing scams involve emails that trick you into clicking on a link to a scam website where you are asked to enter your personal, password or financial information. Pharming scams however automatically redirect you to these scam websites, often without your knowledge.

Pharming is when you are redirected to a fake/scam version of a website which may look identical to the website you were trying to view. This is sometimes referred to as page-hijacking or page-jacking. In this scam, the legitimate URL you typed into your browser or the bookmarked link you followed automatically changes and redirects you to a fake address, often which looks very similar to the legitimate address.

There are two main methods of committing pharming scams, both leading to potential identity fraud. In the first, a victim's computer is infected with a virus or malware which then causes technical changes on the computer which redirect you to the fake website, even if you type in the correct internet address or clicked on a bookmark/favorite entry. This style of pharming may be identified by some antivirus/antispyware software programs.

The second type of pharming is more sophisticated and generally undetectable by antivirus/antispyware programs making it very hard to protect yourself. In this case, an external DNS server, rather than your computer, is attacked resulting in you being unknowingly redirected to a fake/scam copy of a legitimate site. As your computer is not infected, antivirus software cannot help you.

The scam websites which you are redirected to are set up by scammers and may look identical to legitimate websites which request your personal details such as online banking websites.

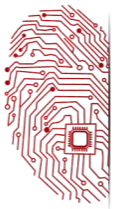
The fake site will ask you to enter sensitive personal details such as:

- usernames
- passwords
- bank account and credit card numbers
- Email addresses.

If successful, a pharming scam will most likely lead to identity theft using the personal details you enter into the fake website.

Warning signs

- Legitimate websites which ask you to enter sensitive personal details are commonly encrypted to protect your details. This is usually identified by the use of “https:” rather than “http:” at the start of the internet address or a closed padlock or unbroken key icon at the bottom right corner of your browser window. If these are missing or there is an open padlock or broken key icon present, the website is not secure and could be a scam site.



Topic: 1.4 Security

- The pharming website will often have a striking resemblance to a legitimate site however the internet address will be slightly different, as may some elements of the visual appearance of the site.
- The site may ask you for personal information which the original site didn't, for example an online banking website will usually ask you to enter your username and password, however a pharming site may also request your bank account or credit card number.

Protect yourself from pharming websites

- Never provide your personal, credit card or account details online unless you have verified the website is authentic.
- You can verify a website's authenticity by looking for "https:" at the beginning of the internet address, the locked padlock icon or the unbroken key icon.
- If you know what the correct internet address should be, check the address of the site you are viewing matches and ensure it hasn't changed from what you entered or expected.
- Check if the website has a digital certificate. If it has one it will generally appear as a padlock icon alongside the web address. You can click on the icon to ensure that the certificate has been verified, is official and has not expired.
- Keep your computer programs updated - many programs give you the option to receive updates automatically. Install and regularly update antivirus, antispyware and firewall software.
- Remain cautious when downloading free software from the web as these often carry viruses or malware.
- If you think you have provided your account details to a scammer, contact the organization you hold your account with immediately, such as your bank or email provider.

What is phishing?

'Phishing' refers to emails that trick people into giving out their personal and banking information; they can also be sent by SMS. These messages seem to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers. The scammers are generally trying to get information like your bank account numbers, passwords and credit card numbers, which they will then use to steal your money.

Phishing emails often look genuine and use what look to be genuine internet addresses—in fact, they often copy an institution's logo and message format, which is very easy to do. It is also common for phishing messages to contain links to websites that are convincing fakes of real companies' home pages.

The website that the scammer's email links to will have an address (URL) that is similar to but not the same as a real bank's or financial institution's site. For example, if the genuine site is at 'www.realbank.com.au', the scammer may use an address like 'www.realbank.com.au.log107.biz' or 'www.phoneybank.com/realbank.com.au/login'.

Topic: 1.4 Security

Warning signs

- You receive an email or SMS claiming to be from a financial institution or telecommunication provider. This message may seem to be from your bank, service provider or a business you don't have an account with. The email contains a link that leads you to a website where you are prompted to enter your bank account details.
- The email does not address you by your proper name.
- The email might contain typing errors and grammatical mistakes.
- The email might claim that your details are needed for a security and maintenance upgrade, to 'verify' your account or to protect you from a fraud threat. The email might even state that you are due to receive a refund for a bill or other fee that it claims you have been charged.

Protect yourself from phishing scams

- **NEVER** send money or give credit card or online account details to anyone you do not know and trust.
- Do not give out your personal, credit card or online account details over the phone unless you made the call and know that the phone number came from a trusted source.
- Do not open suspicious or unsolicited emails (spam)—ignore them. You can report spam to Australian Communications and Media Authority. If you do not wish to report the message, delete it.
- Do not click on any links in a spam email or open any files attached to them.
- Never call a telephone number that you see in a spam email or SMS.
- If you want to access an internet account website, use a bookmarked link or type the address in yourself—**NEVER** follow a link in an email.
- Check the website address carefully. Scammers often set up fake websites with very similar addresses.
- Never enter your personal, credit card or online account information on a website if you are not certain it is genuine.
- Never send your personal, credit card or online account details through an email.

We may not think about if often, but there are several ethical and legal issues that surround our computer use. It is our responsibility to ensure that we are using computers in a manner that will not bring harm to others.

Topic: 1.4 Security

1.4.4 INTERNET SECURITY FOR REAL LIFE SCENARIOS

ONLINE BANKING

Most Internet banking is automatically conducted over a relatively safe kind of Internet connection called Secure Socket Layers (SSL), and the banks themselves have high security which is rarely breached, but the weak link is your own personal computer, and it's a very weak link indeed.

Most personal computers are shot through with security holes. This is especially true of PCs running Windows. You'll find some examples on this page. The big problem is that if a hacker breaches the security on your computer, they can access your Internet bank account through it and pretend that they're you. The bank won't know the difference and you'll find it very difficult to persuade them that somebody else transferred all the money out of your account, even though the transaction was conducted on your computer using your telephone and your Internet connection.

If you decide to take on the security challenge of Internet banking, here are some important tips:

If you have a computer at work, running on a big network, it's highly likely that it's much safer than your machine at home. Its level of security can be measured (roughly) by how strict the limitations are on its use. For example, are you able to download software from the Internet and install it on your machine? Are you able to view all kinds of files on the Internet, including Java and streaming content? If you can't do these things (not just because they're against the rules but because your computer physically won't allow them) then it's likely that your security at work is very good. You may decide to use this computer for your entire Internet banking (assuming, of course, that you've asked your employer for permission).

The only downside to this is that your network manager can spy on you and even collect your password as you type it in, but the chances are that they're earning plenty of money themselves and don't need to steal yours.

However when you access your account, make sure you use a good password. Here are some tips on passwords. Never, ever, store an important password in the Password List of your computer. Anybody with a decent knowledge of computing can read stored passwords in a couple of seconds (even, a competent eight year old could do it).

If you bank through your home PC, you'll need to learn more about security. Start with the Tin Hat security tips. It's pretty much essential that you run anti-virus software and a firewall to keep out hackers. You'll also need the latest version of your operating system.

Macs are relatively secure, though recently they've been attacked more often... Again, you need the latest version of your operating system for maximum security. Each time a new version comes out it plugs more of the leaks in the previous effort.

Topic: 1.4 Security

If you're running Linux, it's likely that you know a fair amount about computer vulnerabilities yourself. You'll also know that Linux can be made safe. You're off to a good start.

ONLINE SHOPPING:

Online shopping can be a convenient and fun activity, provided you take a few precautions to ensure that your information and money stay safe. Take the time to review these tips on what to do when making a purchase in order to have the best experience possible.

When Making a Purchase:

- **Don't shop at a site if you're not comfortable**—If you feel that the site may not be secure, you're probably right. Little things such as misspellings, requests for excessive personal information, and low-resolution logos and photos may be warning signs.
- **Never click on links from spam emails to make purchases**—it's always a bad idea to click on a link in an email from someone you don't know, but it's particularly dangerous if you buy on a site advertised in a spam email. Always try to use a search engine to locate legitimate e-tailor sites.
- **Check the web address to make sure you are on the correct site**—Once you arrive at a site, you need to make sure that it is legitimate and not a fake or spoofed version.
- **Check that the site is secure**—Look for a security seal, such as the McAfee SECURE Trustmark, indicating that the site has been scanned and verified as secure by a trusted third party. This security seal indicates that the site will protect you from identity theft, credit card fraud, spam and other malicious threats.
  In addition, check to see if the site uses encryption—or scrambling—when transmitting information over the Internet by looking for a lock symbol on the page and checking to make sure that the web address starts with "https://", rather than "http://" which indicates that encryption is being used.
- **Use a credit card or an online payment service**—if the site turns out to be fraudulent, your credit card company will usually reimburse you for the purchase; and in the case of credit card fraud, and the law should protect you. Some credit card companies even offer extended warranties on purchases. With debit cards, it can be more difficult to get your money back and you don't want your account to be drained while you're sorting things out with your bank.
  Another option savvy shoppers sometimes use is a one-time-use credit card, which includes a randomly generated number that can be used for one transaction only. If the number is stolen it cannot be used again. Using this type of credit card also ensures that a thief does not have access to your real credit card number.
  Online payment services, like PayPal also offers another way for you to pay for your online purchases. These services let you pay with an account from the online payment service, without having to share your bank or credit card information with e-tailors.
- **Do not use a public computer to shop online**—Computers save or "cache" information to speed up your Internet experience. And, if you are using a public computer, information such as your browsing history and even your login information may be accessible to strangers who use the computer after you. If you leave the computer without logging out of certain sites, others might be

Topic: 1.4 Security

able to access your accounts. To protect yourself, do all of your online shopping from your secure home computer.

- **Only use a secure connection when you place your order**—Never shop using an unsecured wireless network because hackers can access your payment information if the network is not protected.

  You also want to make sure that your computer is protected with comprehensive and up-to-date security software such as McAfee Total Protection, which helps safeguard you from viruses, spyware, and other emerging threats. Additionally, it protects against "keylogger"malware on your machine, which is malicious software that records your keystrokes, including when you type in your credit card numbers and other personal details that you type on your keyboard.
- **Use strong passwords**—***Choose passwords*** that are difficult to guess and are at least 10 characters long consisting of a combination of numbers, letters, and symbols. Remember to keep your passwords private and don't set your computer to remember your credit card number or password when you create an account on an online shopping site.

  Also, don't enter your personal information into popups or at any web page that asks for personal details above and beyond standard requests. For example, you should never have to reveal your Social Security number to an online shopping site.