Chapter 8 Security and Ethics

Keeping data safe is very important for many reasons. There can be very confidential details that people want to keep safe.

Data can be corrupted or deleted either through accidental or through malicious act. There are many ways to keep data safe.

Hacking is breaking into a computer system and stealing the user’s data without consent. However, there can be ethical hacking which is when a company or people hire ethical hackers to try to break into the safety system to make sure if it is safe and if they need to change it. Cracking is where someone edits a program source code. This is usually done for a malicious purpose. Hacking isn’t necessarily harmful whilst cracking is **always** illegal and is potentially very damaging.

Passwords should be complex, different and shouldn’t be meaningful. It should be irrelevant, something like: W23502Q@#BD9304H.

White hat hacking is ethical hacking however, Black hat hacking is illegal hacking.

***Security and Data Integrity***

**Malware:**

This is software used to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer.

Disrupts operations.
Steals sensitive information.
Allows unauthorized access to system resources.
Slows computer or web browser speeds.
Creates problems connecting to networks.
Results in frequent freezing or crashing.

Install Anti-Virus & Firewall Software. Keep Software & Operating Systems Up-to-Date. Avoid Clicking On Pop-Ups

**Hacking:**

Hacking is the act of gaining illegal access to a computer system. Hacking can lead to identity theft and gain of confidential data.  Data can be deleted, changed and even corrupted. Hacking can be prevented by Firewalls, use of strong passwords and user ids and anti-hacking software. There are two types of hacking, White Hat and Black Hat. White hat is ethical hacking whereas Black hat is illegal hacking

**Viruses:**

Viruses are programs or a program code which can replicate itself with the intention of deleting or corrupting files, or cause the computer to malfunctions. It can delete files and data and it can corrupt them. It can also cause the device to crash and not respond. They can be prevented by antivirus software’s, and staying alert and aware of the emails you open and not using software’s from unknown resources.

**Phishing:**

Phishing is run by a person or a creator that sends out a legitimate looking email. and as soon as the recipient clicks on the link, they are sent to a fake website. The creator of the email can access of personal data and this can lead to fraud or identity theft. This can be prevented by ISPs filters on emails and the user should be alert and aware when opening unknown attachments.

**Pharming:**

Pharming is a code installed on a user’s hard drive or on the web server; the code will re direct the user to a fake website without the user knowing. The creator can get access to personal data and leads to fraud or identity theft.  This can be prevented by anti-spyware software and the user being alert and aware of strange emails from unknowns.

**Wardriving:**

The act of locating and using wireless internet connections illegally; it only requires a laptop (or other portable device), a wireless network card and a antenna to pick up wireless signals. This can potentially lead to the user’s internet time to be stolen, and it is very easy to steals a user’s password and personal details. They can be prevented by the use of Wired Equivalent Privacy (WEP) encryption. Also having a complex password before the internet can be accessed. Use of firewalls to prevent outsiders from gaining access.

**Spyware/Key-Logging software:**

Software that gathers information by monitoring key presses on the user’s keyboard; the information is then sent back to the person who sent the software. This gives access to all the data entered using a keyboard on the user’s computer. The software is able to install other spyware; read cookie data and also change user’s default web browser. It can be prevented by the use of anti-spyware data.  Look out for clues that their keyboard activity is being monitored. Use mouse to select characters for passwords, rather than keyboard to reduce risk.

**Cookies:**is a packet of information sent by a web server to a web browser. Cookies are generated each time the user visits the website.

**Denial of Service (DOS):**

An attack that floods a network send request after request until the network itself shuts down/cannot cope with however many requests.

**Bio-metric systems:**Bio-metric systems are systems that are protected with things like facial recognition, retina scan, finger prints, etc.

**Firewalls:**Hardware or software-based security layer that is positioned between the internet and network/user device. It examines incoming/out coming traffic. Identifies suspicious files/phrases and notifies administrator if anything is flagged. White-lists/blacklists websites/applications. The administrator gets monitor.  Acts as a gateway to the internet.

**Proxy Server:**Remember the websites you have visited, and remembers all the information with it. It keeps the users IP hidden. Acts as a firewall if a firewall isn’t present on a network (limited functionality).

A computer that provides an indirect connection to a network or the Internet, often used to provide increased network security. When a computer connects to a proxy server it receives an IP address from the proxy server and not the network or the Internet, Allowance of internet traffic to be filtered so they can block access to a website if necessary

* using CACHE, they can speed up access to information from a website.
* When a website is first visited, the home page is stored on the proxy server, so when the user enters the website again, it goes through the proxy server cache; giving faster access
* maintaining privacy of IP addresses – which improves security
* acting similarly to a firewall

**VPN (Virtual Private Network):**is a method used to add security and privacy to private and public networks. It is recommended to use in the dark and deep web.

**Security Protocols:**

* Secure Sockets Layer (SSL)
* Transport Layer Secuirty (TLS)

**Secure Sockets Layer**(SSL) is a type of protocol (a set of rules used by computers to communicate with each other across a network). This allows data to be sent and received securely over the internet.

When a user logs onto a website, SSL encrypts the data – only the user’s computer and the web server are able to make sense of what is being transmitted. A user will know if SSL is being applied when they see https or the small padlocks in the status bar at the top of the screen.  Padlocks suggests that it is safe and secure

What happens when a user wants to access a secure website?

1. The users web browser sends a message so that it can connect with the required website which is secured by SSL.
2. The web browser then requests that the web server identifies itself ‘
3. The web server responds by sending a copy of its SSL certificate to the user’s web browser
4. If the web browser can authenticate this certificate, it sends a message back to the web server to allow communication
5. Once this message is received, the web server acknowledges the web browser, and the SSL-encrypted two-way data transfer begins.

**Transport Layer Security**(TLS) is similar to SSL but is a more recent security system. TLS is a form of protocol that ensures the security and privacy of data between devices and users when communicating over the internet.  It is essentially designed to provide encryption, authentication and data integrity in a more effective way.

When a website and user are communicating over the internet, TLS is designed to prevent a third-party user or device into this communication since this causes problems with data security.

TLS is formed of 2 layers

1. Record protocol, this part of the communication can be used with or without encryption (it contains the data being transferred over the internet).
2. Handshake protocol: this allows the website and the user to authenticate with each other and make use of encryption algorithms (a secure session between the website and user is established).

**Encryption:**

Encryption is used to protect data in case it has been hacked. Encryption makes the data meaningless unless it somehow gets decrypted. There are 2 types of encryption:

* Symmetric Encryption
* Asymmetric or Public Key Encryption

**Symmetric Encryption**

Symmetric Encryption is a secret key which can be a combination of different characters. If this key is applied to a message, its contents is changed and makes it unreadable unless a user has a decryption key which fixes the problem. Basically, one key is needed to encrypt a message and another key is needed to decrypt message.

However, this key is very vulnerable to Key Distribution Problem. So, the sender and receiver have to have to same key for encryption and decryption.  The sender has to send the key to the receiver and if somehow it gets intercepted by a hacker, this can lead to a failure in encryption and security making the contents unprotected. The hacker can easily decrypt the file/data. There is also an encryption algorithm where you use an algorithm to unlock the file and keep the data safe.

**Asymmetric Encryption**

This type of encryption is a more safe and secure method.

* Public Key is a key that is made available to everybody
* Private Key is a key which is only known by the computer user.

Both type of keys are needed to encrypt and decrypt messages. It works like this: First User A applies a symmetric key to encrypt the message, then the symmetric is then encrypted using the public key known to both A and B. User A sends the message over the internet, User B decrypts the symmetric key by applying their known private key, the decoded symmetric key is used to decrypt the message sent by User A.

**Plain Text or Cypher Text**

* Plain Text is normal text/data before it goes through encryption.
* Cypher text is the output from an encryption algorithm.

**Authentication**

Authentication is used to verify that data comes from a trusted source. It works with encryption to strengthen internet security.

**Computer Ethics**

Computer Ethics is a set of principles set out to regulate the use of computers. Three factors are considered:

* Intellectual Property Rights: this covers copying of software without permission of owners
* Privacy Issues: this covers hacking and illegal access of another person’s personal data
* Effect of computers on society – this covers factors such as job losses and social impacts and so on

**Free Software, Freeware and Shareware**

Free Software is basically when you download software, you can run it, copy it, change it, it doesn’t matter.  Examples: AbiWord, F-Spot and Scribes.

Freeware is a software a user can download from the internet free of charge. Once it has been downloaded, there are no extra fees associated with the software. Examples: Adobe, Skype or media players)

Shareware is a software which users are allowed to try out a software free of charge for a trial period. Examples (Netflix, Music Apps)