System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information. The malware and the attacker identify and exploit the vulnerability of the computer system to gain unauthorized access.

System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing.

Generally, the motive of the hackers behind System Hacking is gaining access to the personal data of an individual or sensitive information belonging to an organization in order to misuse the information and leak it which may cause a negative image of the organization in the minds of people, Privilege Escalation, Executing malicious applications to constantly monitor the system.

Goals of System Hacking

- Gaining Access
- Escalating privileges
- Executing applications
- Hiding files
- Clearing tracks

Password cracking

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

With the information malicious actors gain using password cracking, they can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.

A password cracker recovers passwords using various techniques. The process can involve comparing a list of words to guess passwords or the use of an algorithm to repeatedly guess the password.

What is a default password?

A default password is a standard preconfigured password for a device or software. Such passwords are the default configuration for many devices and, if unchanged, present a serious security risk

Password complexity

- Be at least 12 characters long. The shorter a password is, the easier and faster it will be cracked.
- Combine letters and a variety of characters. Using numbers and special characters, such as periods and commas, increases the number of possible combinations.
- Avoid reusing a password. If a password is cracked, then a person with malicious intent could use that same password to easily access other password-protected accounts the victim owns.
- Pay attention to password strength indicators. Some password-protected systems include a password strength meter, which is a scale that tells users when they have created a strong password.
- Avoid easy-to-guess phrases and common passwords. Weak passwords can be a name, a pet's name or a birthdate -- something personally identifiable. Short and easily predictable patterns, like 123456, password or qwerty, also are weak passwords.
- Use encryption. Passwords stored in a database should be encrypted.
- Take advantage of password creation tools and managers. Some smartphones will automatically create long, hard-to-guess passwords. For example, Apple iPhones will create strong website passwords for users. An iPhone stores the passwords in its password manager, iCloud Keychain and automatically fills the password into the correct field so the user doesn't have to remember the complicated password

Types of Passwords Attack

There are three types of password attacks:

Non-electric attacks
Online attacks
Offline attacks

1) Non-electric attacks

A non-electric attack is a type of attack that uses chicanery to get sensitive information of users or perform actions through which the security of a network will be compromised. Non-electric attacks are as follows:

- Social Engineering

Social engineering is the process in which a user is tricked into believing that the hacker is a legitimate agent. The hacker uses a common tactic. Hacker poses as technical support and calls a victim. Hackers ask for a network access password so that he can provide assistance. If the person has done this using fake credentials and fake uniforms, this technique will become effective. But these days, this technique is less common.

- Shoulder Surfing

Shoulder attacks are performed by the most confident hackers. The hacker can take the look of an aircon service technician, parcel courier or anything else so that they can easily access an office building. Once they entered the office, they will get a kind of free pass, and they can note the passwords that are entered by the staff members of the company.

- Spidering

The techniques which are used in phishing attacks and social engineering attacks are also used in spidering. Savvy hackers have understood that the passwords used in the corporate office are made of business-related words. In the brute force attack, the custom words list is built by Website sales material, listed customers on websites, studying corporate literature, and website of competitions. The process is automated by really savvy hackers.

2) Online attacks

Active online attacks can be categorized as follows:

Guess

Guess is like a best friend of password cracker. If all the attacks fail, the hacker can try to guess your password. These days, there are various password managers who create various password strings that are impossible to guess for a hacker. Many users set a random password based on their memorable phase of life like family, interests, pets, dob, hobbies, and so on

Brute Force attack

In the Brute force attack, we access a system using the different methods of hacking, which involves password guessing. For example, a hacker can use the relevant clues and guess the person's password. Many people use the same password on many sites. Using the previous data breaches, so the password can be exposed using the previous data breaches. Using some most commonly used passwords, a hacker attempts to guess the associated username, which is the reverse brute force attack.

Dictionary attack

This attack shows a sophisticated brute force attack example. In the Dictionary attack, an attacker uses a dictionary that contains words. The words are nothing but a straightforward name. In other words, the attacker uses the words that most of the users use as their password. In dictionary attacks, every word in the dictionary is a test in seconds. Most of the dictionary contains the credentials gained from previously hacked passwords. Dictionary also contains the word combinations and most commonly used passwords.

Phishing

Phishing is a very easy way to hack the password of any user. In this attack, the hacker asks the user to enter his password. In the phishing email, a hacker sent the fake login page to the unsuspected user, which is associated with any service, the hacker wants to access. The page requests the user to write some terrible problem which he finds in their security. After that, the page skims their password. Now the hackers can use that password to get the sensitive information of the user. When the users are giving you a password happily, then why will you trouble to crack the passwords.

Malware

The Umbrella of malware contains a host of malicious tools, screen scrapers, and keyloggers. To steal the person's information, these malicious software are used. Ransomware software, which is highly disruptive malicious software, attempts to block the access of the entire system. The malware families have some highly specialized malware that specially targets the password.

3) Offline attacks

Offline attacks are as follows:

Offline Cracking

We should remember that not all attackers hack through the internet connection. Mostly works done offline. You imagine that through the blocking automated guessing application, your password is safe. In this application, if a user enters the wrong passwords three or four times, the system lockout the user. This process will be true if all password hacking takes place online, but it's not. Offline hacking takes place using the hashes set in the password file, which was obtained from a compromised system.

Rainbow table attack

As the name implies, the rainbow table is not colorful. The password is encrypted using cryptographic alias or hash whenever it is stored on the system. This encryption makes it impossible for a hacker to determine the original password. To bypass this, the hacker must maintain and share the directories built from previous hacks containing passwords and their corresponding hashes. This process reduces the time of hackers breaking into the system.

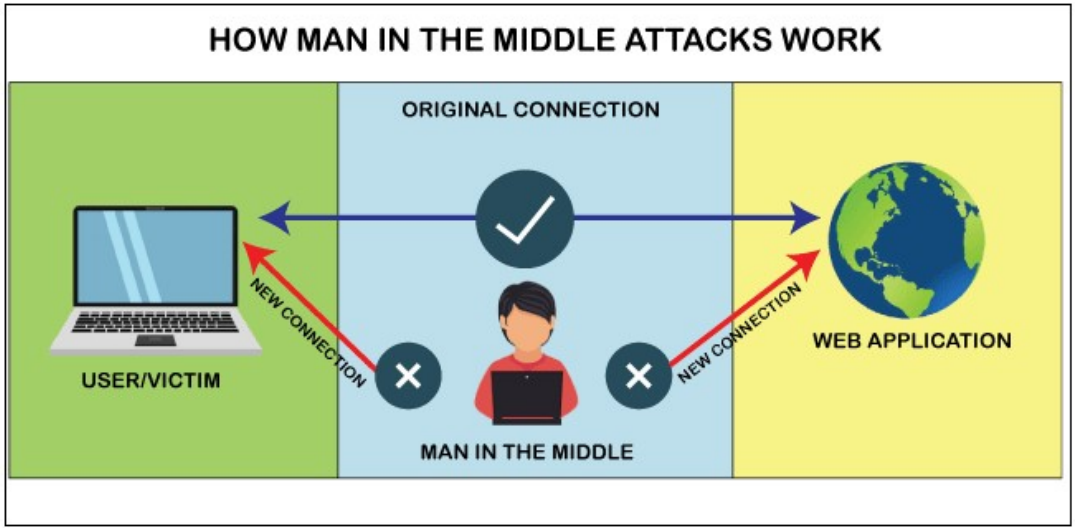
Network Analyzers

Network analyzers are the type of tools that allows monitor and intercept the package, which is sent over the network. The package contains a plain text password, and that tool lifts that password.

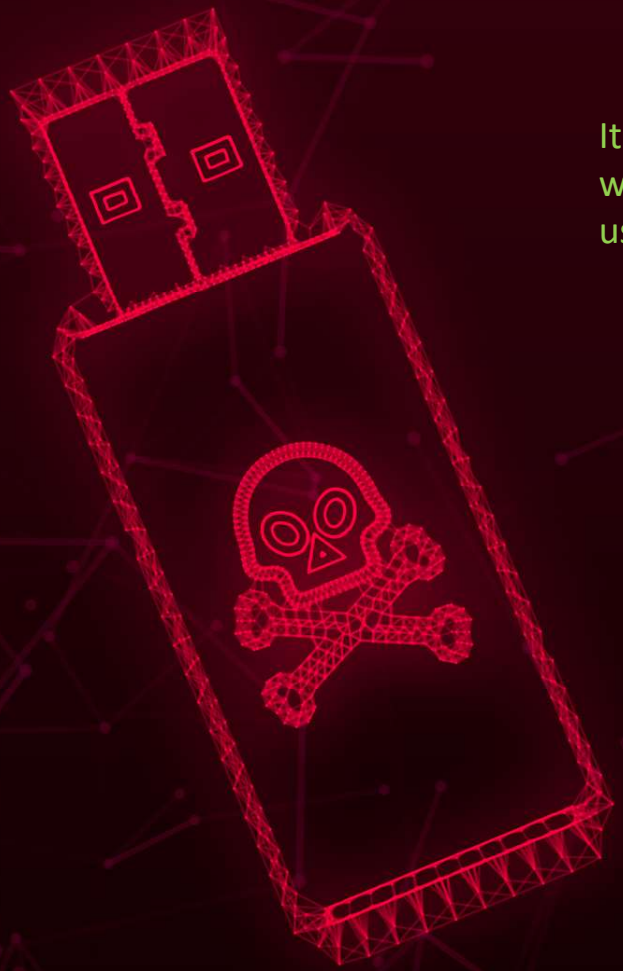
Man-in-the-middle (MITM) Attacks

A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties and achieves access to the data that the two people were trying to deliver to each other. A man-in-the-middle attack also helps a malicious attacker, without any kind of participant recognizing till it's too late, to hack the transmission of data intended for someone else and not supposed to be sent at all. In certain aspects, like MITM, MitM, MiM or MIM, MITM attacks can be referred.

If an attacker puts himself between a client and a webpage, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways.



USB PASSWORDS STEALERS

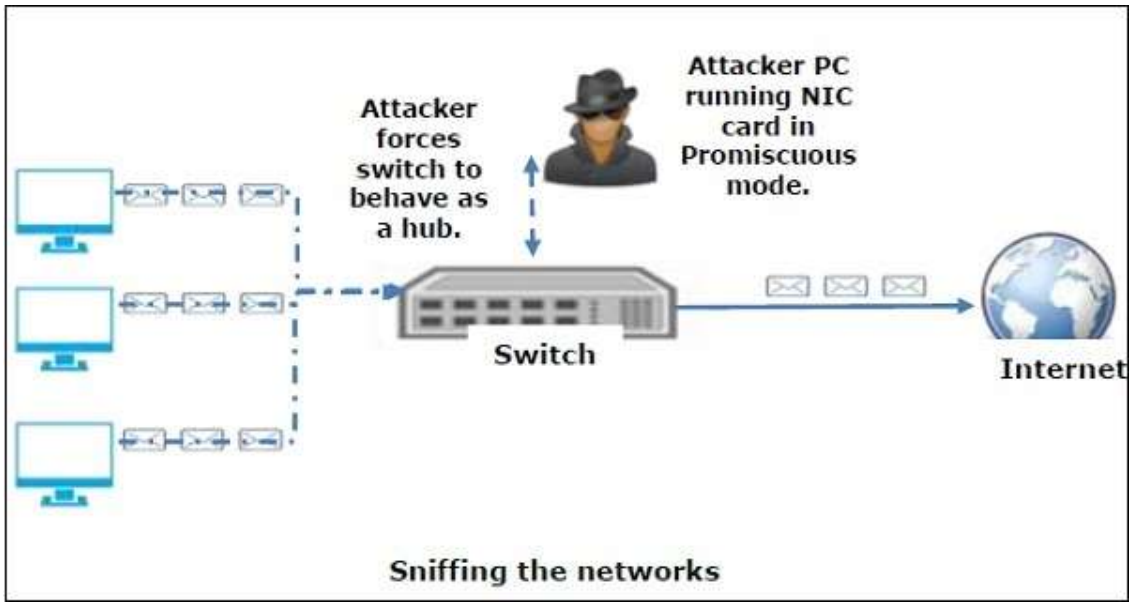


It’s a Special type of USB device that is made to steal the password when connected into a system. These type of USB devices are mostly used by hackers to gain the password and other credentials.

Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called wiretapping applied to the computer networks.

A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.



Sniffing the networks

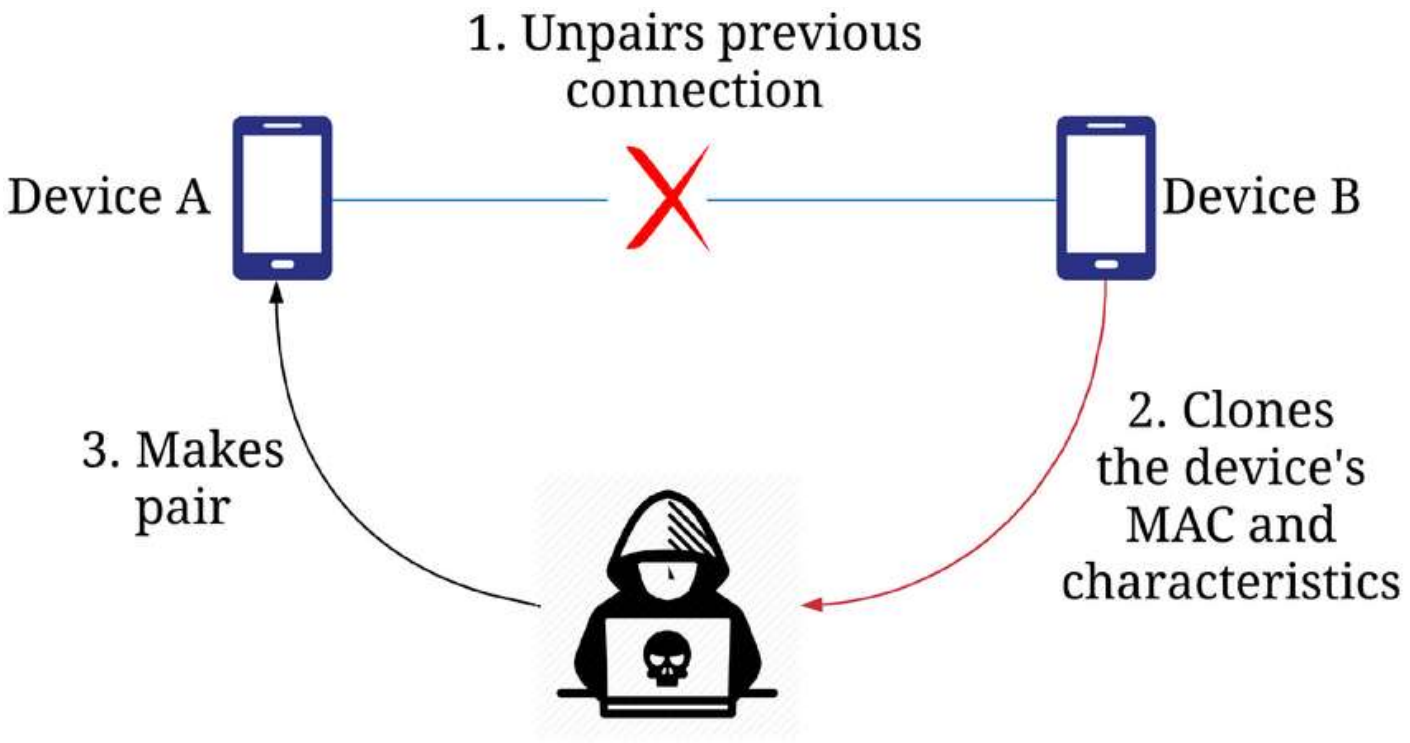
Types of Sniffing
Sniffing can be either Active or Passive in nature.

Passive Sniffing
In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

Active Sniffing
In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port

MAC spoofing attack

A MAC spoofing attack is where the intruder sniffs the network for valid MAC addresses and attempts to act as one of the valid MAC addresses. The intruder then presents itself as the default gateway and copies all of the data forwarded to the default gateway without being detected. This provides the intruder valuable details about applications in use and destination host IP addresses. This enables the spoofed CAM entry on the switch to be overwritten as well



Wireless network & types

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.

There are four main types of wireless networks.

Wireless Personal Area Networks (WPAN) are short-range networks that connect devices within a relatively small area. A WPAN generally connects devices within a person's reach, though the range can extend up to about 30 feet. Using Bluetooth technology, a WPAN can interconnect compatible devices near a central location, such interconnecting a headset to a laptop on your desk.

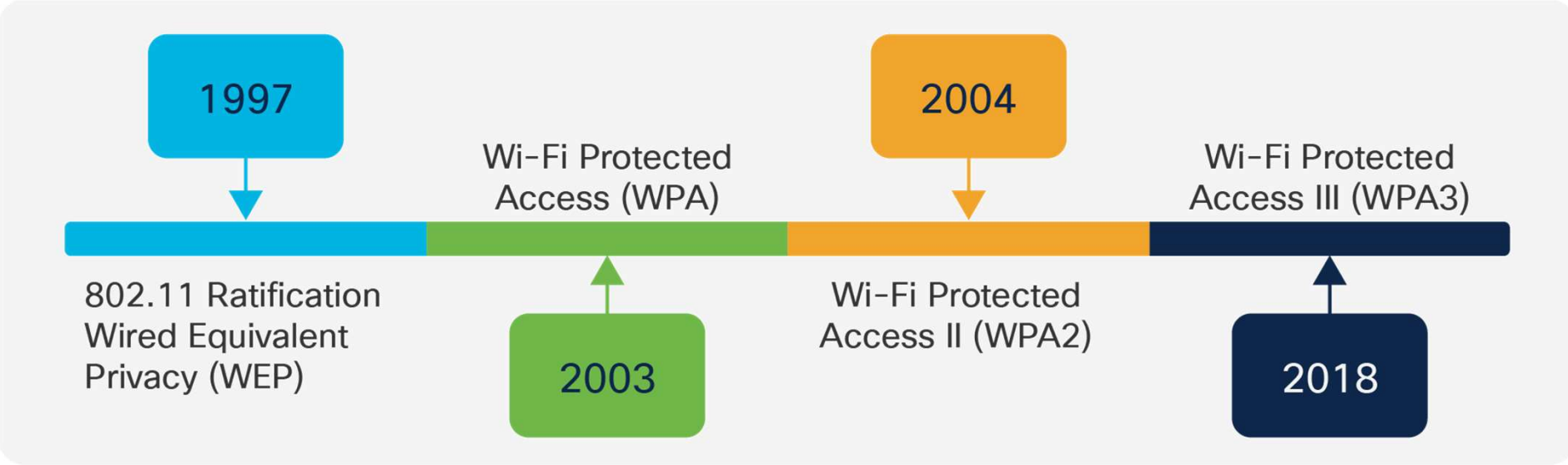
Wireless Local Area Networks (WLAN) are wireless networks that use radio waves, not Bluetooth technology like WPANs. There is usually at least one cable that is the access point for internet access, such as a wired internet connection going into a router, which then broadcasts the wireless signal to other devices. WLANs are used for connecting to local resources and to the internet. The range can be confined to a single room or home or spread across an entire building or campus with the use of spread-spectrum or OFDM technologies.

Wireless Wide Area Networks (WWAN) can be maintained over large areas, such as cities or countries, via multiple satellite systems, antenna sites or mobile phone signals. With a wide coverage area, WWANs provide a way to stay connected when other forms of network access are unavailable.

Wireless Metropolitan Area Networks (WMAN) connect several different WLANs in a metropolitan area, such as different buildings in a city.

Types of encryption network(WEP/ WPA/ WPA2),

Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients. Wireless networks are often less secure than wired ones, so wireless security protocols are crucial for keeping you safe online. The most common Wi-Fi security protocols today are WEP, WPA, and WPA2.



WEP (Wired Equivalent Privacy) is the oldest and most common Wi-Fi security protocol. It was the privacy component established in the IEEE 802.11, a set of technical standards that aimed to provide a wireless local area network (WLAN) with a comparable level of security to a wired local area network (LAN).

The Wi-Fi Alliance ratified WEP as a security standard in 1999. Once touted to offer the same security benefits as a wired connection, WEP has been plagued over the years by many security flaws. And as computing power has increased, these vulnerabilities have worsened. Despite efforts to improve WEP, it's still vulnerable to security breaches. The Wi-Fi Alliance officially retired WEP in 2004.

WPA (Wi-Fi Protected Access) is a wireless security protocol released in 2003 to address the growing vulnerabilities of its predecessor, WEP. The WPA Wi-Fi protocol is more secure than WEP, because it uses a 256-bit key for encryption, which is a major upgrade from the 64-bit and 128-bit keys used by the WEP system.

WPA also uses the Temporal Key Integrity Protocol (TKIP), which dynamically generates a new key for each packet, or unit of data. TKIP is much more secure than the fixed-key system used by WEP.

Still, WPA is not without flaws. TKIP, the core component of WPA, was designed to be implemented onto WEP-enabled systems via firmware updates. This resulted in WPA still relying on easily exploitable elements.

WPA2 (Wi-Fi Protected Access 2) is the second generation of the Wi-Fi Protected Access wireless security protocol. Like its predecessor, WPA2 was designed to secure and protect Wi-Fi networks. WPA2 ensures that data sent or received over your wireless network is encrypted, and only people with your network password have access to it.

A benefit of the WPA2 system was that it introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol. Used by the US government to protect classified data, AES provides strong encryption.

Unfortunately, like it's predecessor, WPA2-enabled access points (usually routers) are vulnerable to attacks through WEP. To eliminate this attack vector, disable WEP and, if possible, make sure your router's firmware doesn't rely on WEP.

Defend against Wifi cracking attack

- Update Security patches - If any of your devices have been affected, make any security updates as soon as they are made available. Especially Linux or Android. You may need to contact vendors the latest available updates.
- 'Double up' on encryption - This helps the prevention of reading of data and modification of data. This is one of the core functions of encryption so you want on add extra layers when you can.
- Use VPN's – to encrypt the traffic. So if you are on your old android phone, put on your VPN and then the attacker won't be able to modify the data to insert ransomware and won't be able to read your data because it is encrypted.
- Use HTTPS - Check for the little green padlock! Check for HTTPS! Check HTTPS has not been stripped and replaced with HTTP. So when you are in your browser, double check HTTPS is there, double check for the green padlock and that HTTPS hasn't been stripped out.
- Use other encryption
- Don't send sensitive data in plain text
- Switch off Wi-Fi if not needed
- Use 3G/4G or alternative network