Cyberattacks

Cyberattacks are when hackers of one kind or another attempt to break into computer systems either to steal data, to delete or modify data, or to make a system unusable. The motives for doing so vary - it may be to try to obtain money, it may be out of spite, to 'prove you can', it may be for a love of destruction, or there may be political reasons behind it. Whilst many hackers are still one, usually young, individuals, there are parts of the world where hacking is becoming increasingly 'industrialised' as well as being use for political reasons.

Cyber Attack Protection
Keep your user data private
Check your privacy settings
Update your antivirus
Log out
Respect others
Use strong passwords
Scan e-mails before opening
Check website URL

There are two main approaches to hacking -

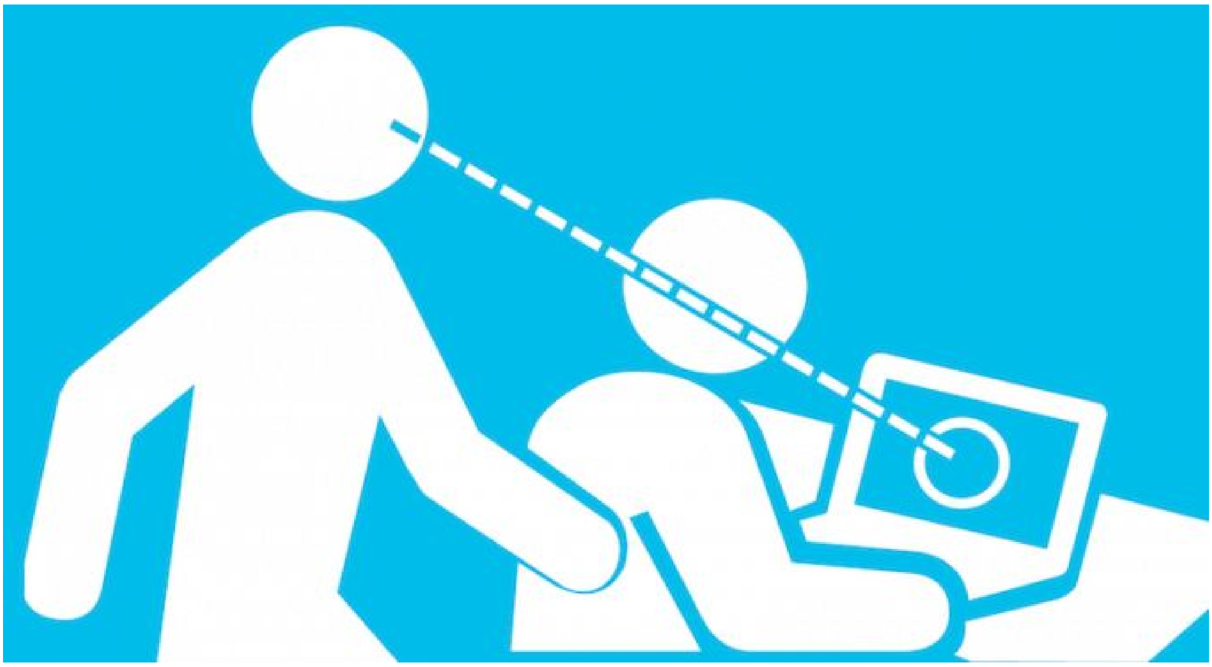
Target the user

We often say that a user is often the weakest, or least secure, area of any computer system. Hacking approaches that target users are frequently called 'social engineering' - this involves tricking or conning people into doing what you want them to do so that you can gain access to a system.

Two common approaches are:
Phishing - this involves sending emails claiming to be from some organisation or authority (e.g. eBay or PayPal), and asking the users to log on to a website via a link. This website actually belongs to the hackers, so the user is revealing their log-on information to the

hackers. Two-factor authentication is a good protection against phishing, although it can still be breached if the hackers are quick enough.
For an example of how effective phishing can be, listen to this podcast - https://gimletmedia.com/shows/reply-all/rnhoww

Question 1 - What is spear-phishing?



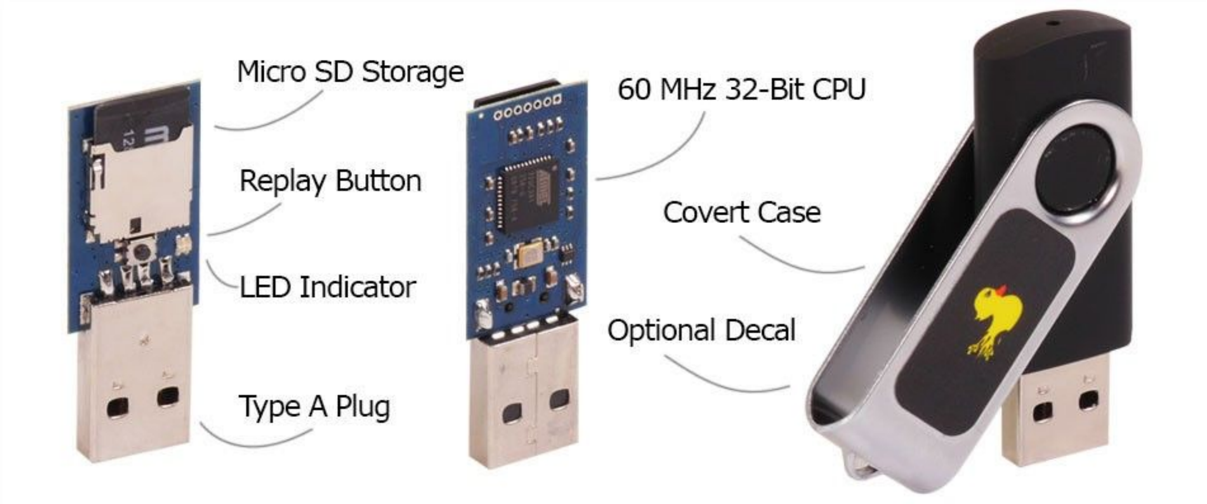
Shoulder surfing - much simpler than phishing, shoulder surfing simply involves looking over someone's shoulder when they are using their computer and reading their password, or user information, from the screen. Shoulder surfing is best prevented by having a well organised office and restricting where unknown people can stand. However, screens do exist that can only be viewed from directly in front of them, making it harder for people to spy on the screen.

Question 2 - Describe another approach to social engineering hacking.

Target Technical Weaknesses

Networks are extremely complex, involving many interacting parts, which means their behaviour in totality can be hard to predict. This in turn means there are often security vulnerabilities that the designers did not intend.

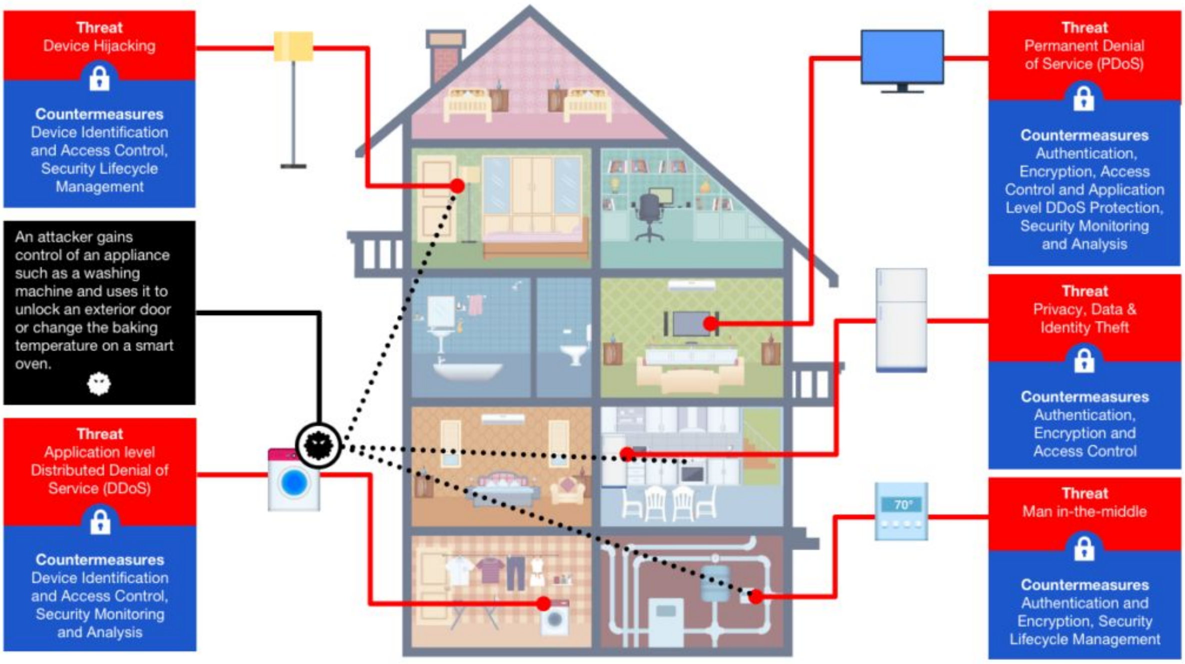
Attacks that take advantage of technical weaknesses include:



USB devices - portable storage means employees can potentially copy and steal data that may be valuable or sensitive. However, USB devices can also carry software, with or without the knowledge of the person using it. These can be used to install malicious software like viruses and other malware onto systems, or can be self contained hacking tools. A machine is much more vulnerable to software attached to it than to software attacking via a network connection.

Question 3 - What is a key-logger and how could it be used in a hacking attack?

Question 4 - You can set a computer so that it boots from the software on a USB stick, rather than from it’s own hard drive. Why does this make a device very vulnerable to hacking?



Threat
Device Hijacking

Countermeasures
Device Identification and Access Control, Security Lifecycle Management

An attacker gains control of an appliance such as a washing machine and uses it to unlock an exterior door or change the baking temperature on a smart oven.

Threat
Application level Distributed Denial of Service (DDoS)

Countermeasures
Device Identification and Access Control, Security Monitoring and Analysis

Threat
Permanent Denial of Service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Privacy, Data & Identity Theft

Countermeasures
Authentication, Encryption and Access Control

Threat
Man in-the-middle

Countermeasures
Authentication and Encryption, Security Lifecycle Management

Smart Devices Exploitation - the much discussed ‘internet of things’ turns out to be a security nightmare. Everything from smart thermostats, smart light bulbs, smart doorbells, smart cameras, digital hubs, runs software that can be exploited. Tens of thousands, potentially millions, of these devices have already been compromised and can be used for Denial of Service attacks by hackers, and may be leaking information about their owners.

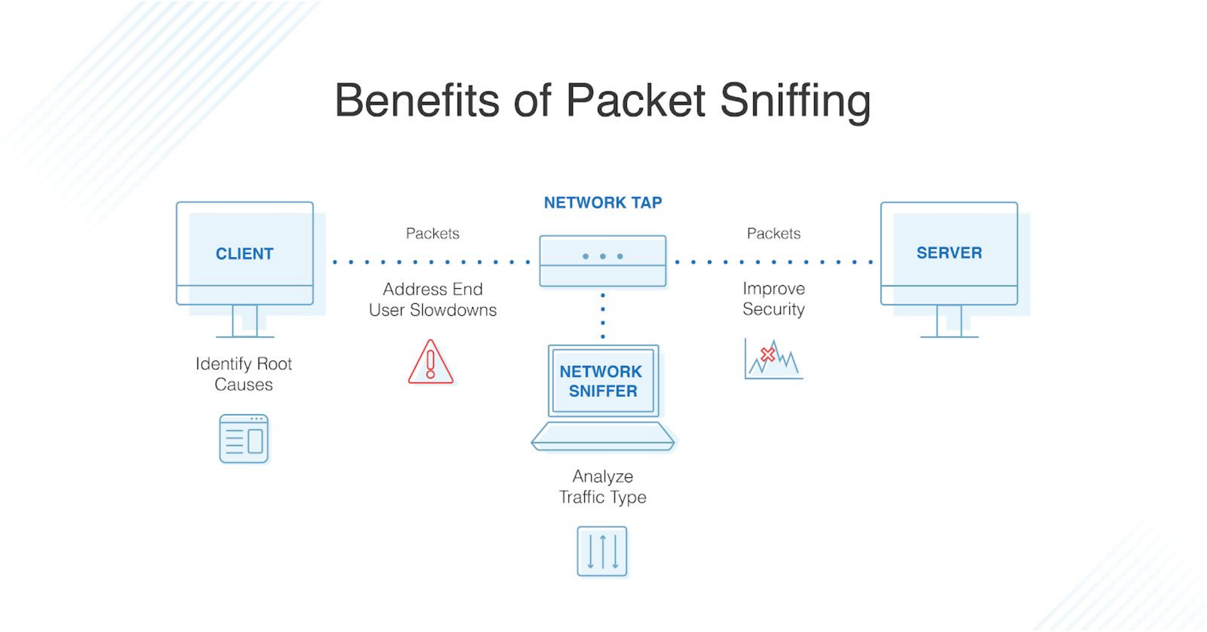
Question 5 - What is a Denial of Service attack?

Question 6 - Give two motivations for Denial of Service attacks on websites.

Unpatched Software - as security vulnerabilities are identified they will be patched by software companies: fixes will be released for users to download and install. However, many users do not do this, meaning that many systems are running software with known, published, security vulnerabilities. All hackers have to do is keep up with known security issues and look for unpatched systems of which they can take advantage.

Question 7 - read this short article:
https://www.zdnet.com/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/
What does it tell you about why hacking attempts are more effective than you might expect?

Eavesdropping - this means listening in to other people's communications. It can simply mean listening to people's phone calls, but more often now involves 'packet sniffing', meaning copying data being transmitted across networks. If this data is not encrypted then the hackers have free access to any and all data being transmitted. It is therefore vital that all important communications are fully encrypted.



Question 8 - Why is it generally a very bad idea to send important information like passwords via email?

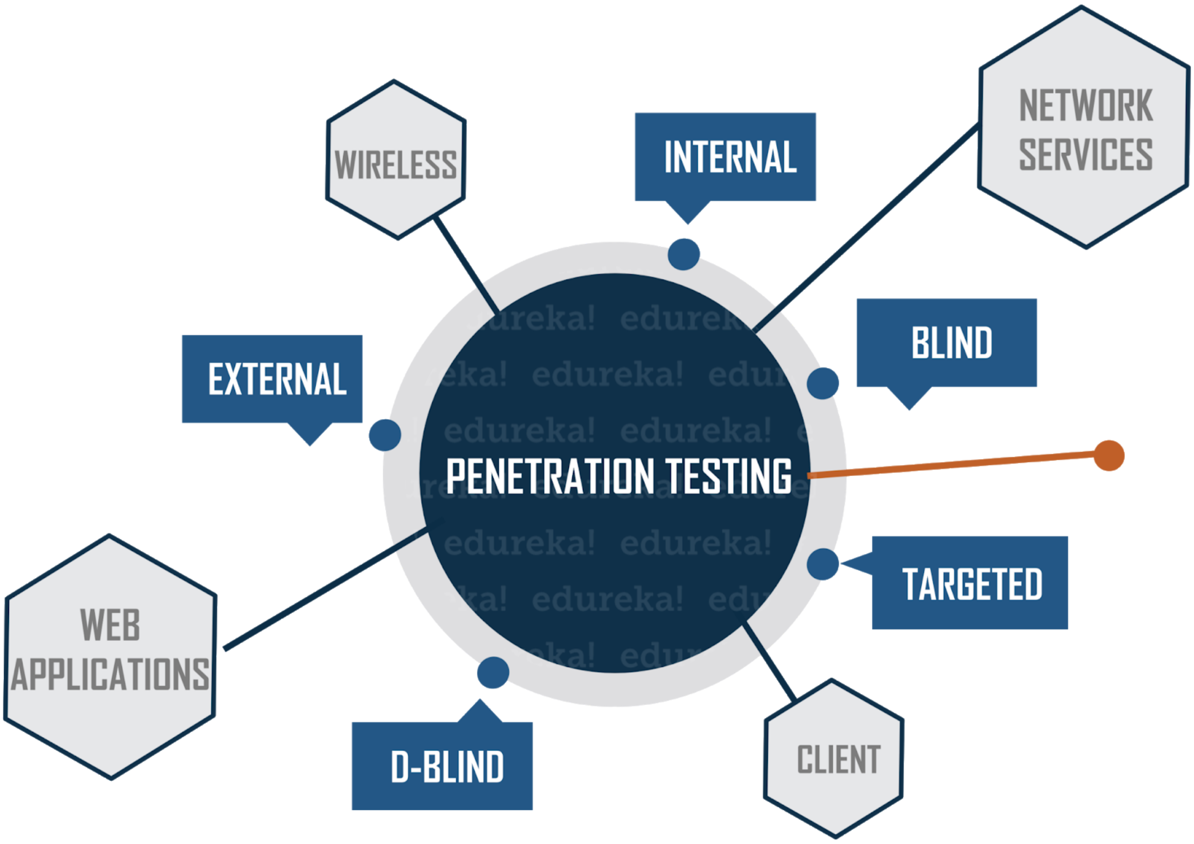
For a deep dive into the culture of cybersecurity, particularly how leadership works in very large organisation you can watch this interview https://www.mcchrystalgroup.com/insights/no-turning-back-episode-16-jamil-farshchi/ with the Chief Information Security Officer of Equifax, an extremely large American company.

Identifying Vulnerabilities

If you've got a network system you're going to want to know where it is vulnerable, so you can fix it. Here are techniques that organizations use:

Ethical Hacking

Ethical hackers are security experts who are paid to try to break into systems. An organisation would pay an ethical hacker - sometimes called a 'white hat hacker' to try to and break in, and therefore test their security. They will try to use all the techniques a real hacker would use, and see if any of them are effective. If they are, they will feed this information back so that the organisation can fix their vulnerabilities.

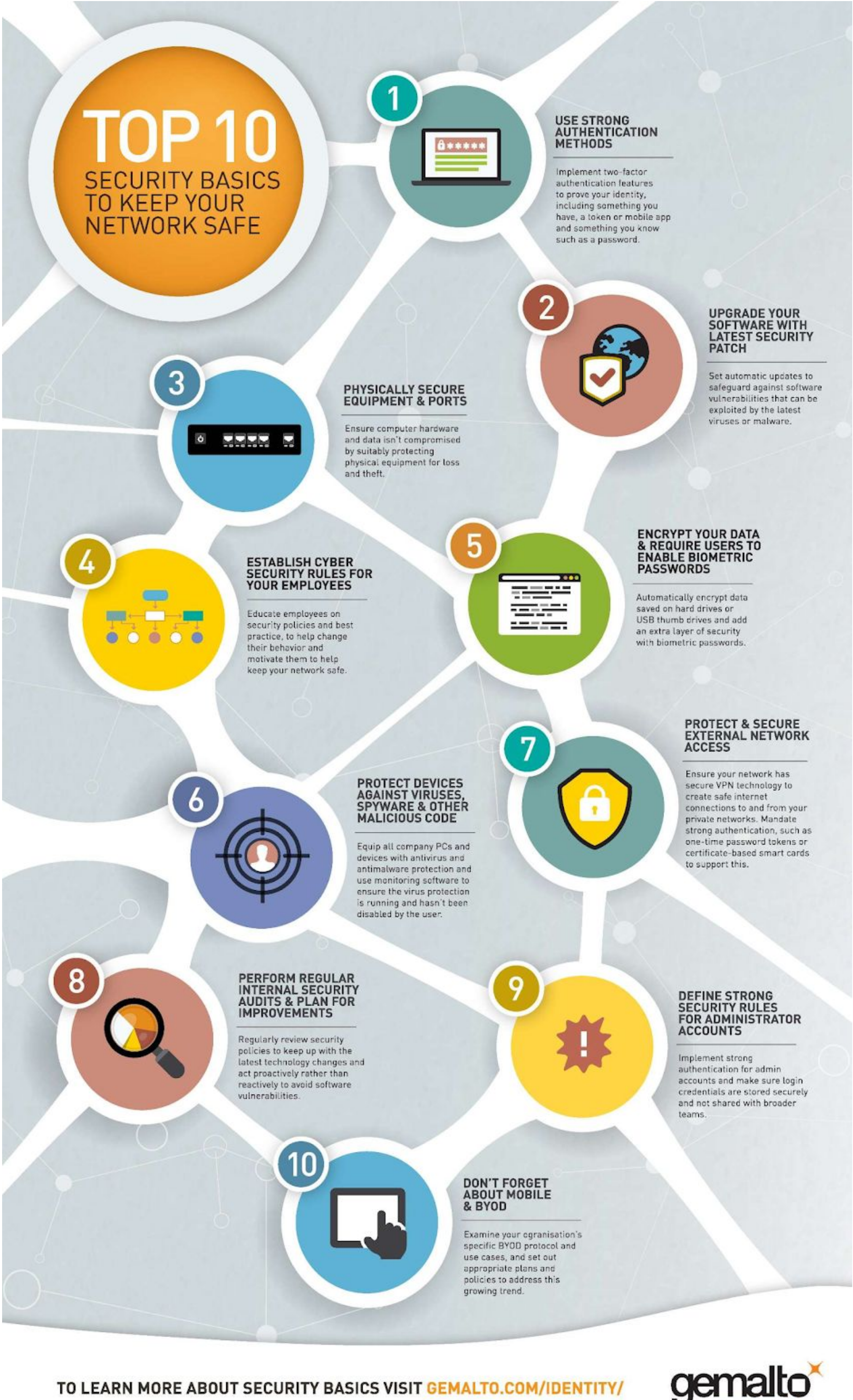


Penetration Testing

This is the hacking that is usually done by the ethical hackers. Penetration testing is about trying to break into a system - either via the software or staff - and therefore finding where the weak points in the system are.

Commercial Analysis Tools

Special software exists which systematically scans a network system looking for vulnerabilities. It will look for unpatched software, and issues that have been identified in other systems. Naturally, hackers also use these same tools to try to find vulnerabilities they can exploit.



TOP 10 SECURITY BASICS TO KEEP YOUR NETWORK SAFE

1 **USE STRONG AUTHENTICATION METHODS**

Implement two-factor authentication features to prove your identity, including something you have, a token or mobile app and something you know such as a password.

2 **UPGRADE YOUR SOFTWARE WITH LATEST SECURITY PATCH**

Set automatic updates to safeguard against software vulnerabilities that can be exploited by the latest viruses or malware.

3 **PHYSICALLY SECURE EQUIPMENT & PORTS**

Ensure computer hardware and data isn't compromised by suitably protecting physical equipment for loss and theft.

4 **ESTABLISH CYBER SECURITY RULES FOR YOUR EMPLOYEES**

Educate employees on security policies and best practice, to help change their behavior and motivate them to help keep your network safe.

5 **ENCRYPT YOUR DATA & REQUIRE USERS TO ENABLE BIOMETRIC PASSWORDS**

Automatically encrypt data saved on hard drives or USB thumb drives and add an extra layer of security with biometric passwords.

6 **PROTECT DEVICES AGAINST VIRUSES, SPYWARE & OTHER MALICIOUS CODE**

Equip all company PCs and devices with antivirus and antimalware protection and use monitoring software to ensure the virus protection is running and hasn't been disabled by the user.

7 **PROTECT & SECURE EXTERNAL NETWORK ACCESS**

Ensure your network has secure VPN technology to create safe internet connections to and from your private networks. Mandate strong authentication, such as one-time password tokens or certificate-based smart cards to support this.

8 **PERFORM REGULAR INTERNAL SECURITY AUDITS & PLAN FOR IMPROVEMENTS**

Regularly review security policies to keep up with the latest technology changes and act proactively rather than reactively to avoid software vulnerabilities.

9 **DEFINE STRONG SECURITY RULES FOR ADMINISTRATOR ACCOUNTS**

Implement strong authentication for admin accounts and make sure login credentials are stored securely and not shared with broader teams.

10 **DON'T FORGET ABOUT MOBILE & BYOD**

Examine your ogranisation's specific BYOD protocol and use cases, and set out appropriate plans and policies to address this growing trend.

TO LEARN MORE ABOUT SECURITY BASICS VISIT GEMALTO.COM/IDENTITY/

gemalto

Review of network and user policies

Policies are the set of rules that users agree to within an organisation. The College, for instance, has an IT policy for staff and students. These policies are used to encourage good practice, and to ban dangerous activity (e.g. bringing in USB sticks from outside the organisation, or installing software without permission). A good set of network policies will ensure everyone is informed about how to keep the network safe, but it still relies on people following the rules and doing what they have agreed to do.

Regularly reviewing policies is essential, as they can quickly got out of date as new threats appear and the circumstances of the business constantly change.

Network policies should contain rules such as:

- What users are not allowed to do with the IT equipment - e.g. not install their own software, not download files from the internet, not bring in storage devices from home.
- What should be done if a problem is found
- The backup policy - when and how backups are made and who is responsible
- How software will be updated and patched
- Any other rules that help keep the system safe - e.g. no drinks in the computer room, keeping doors locked, nor disclosing passwords, etc.

Question 9 - Why might an excellent network user policy still not be effective at improving the security within an organisation?

Question 10 - Suggest 5 specific rules that a network use policy should contain that tell users what **not** to do.