Network attacks

As workforces have become more mobile, employees no longer always work on a single trusted network, making security more difficult.

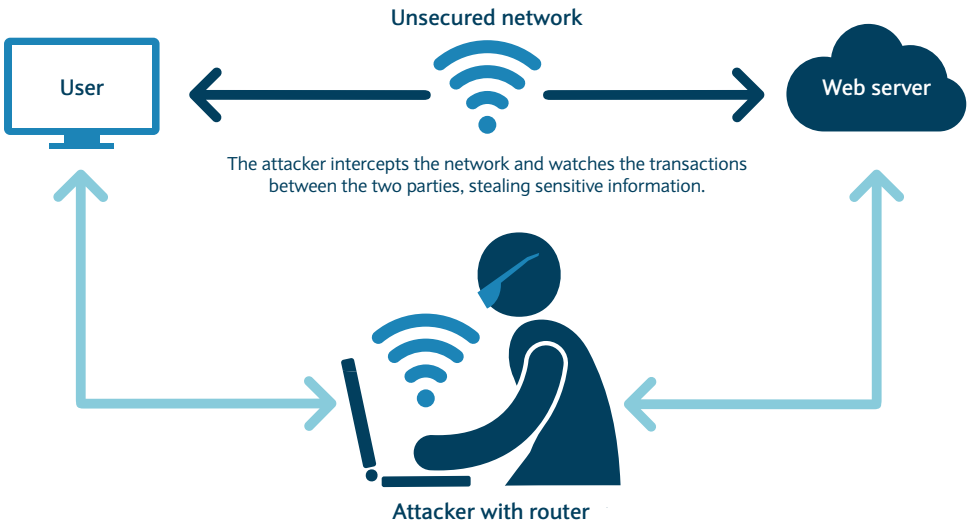
Emails are the main communication method for most companies, yet it is often forgotten how unsecure the communications are. An email can be thought of like a postcard – it can be read as it moves across networks.

It is therefore important that sensitive information is only sent over encrypted networks. Secure Sockets Layer (SSL) is the standard security technology for establishing an encrypted link between a web server and a browser.

Man-in-the-Middle Attack

There are various different types of network attack, but all require the exploitation of an unsecured network. Where the network is not encrypted, an unknown third party may intercept communications that are being sent. In a 'Man-in-the-Middle Attack', the attacker intercepts the network and watches the transactions between the two parties. They are then able to steal sensitive information, such as account passwords, banking details, or customer data.

A common example of a Man-in-the-Middle Attack is 'active eavesdropping'. This is when the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.



Distributed Denial of Service Attack

A Distributed Denial of Service Attack (DDoS attack) is when a hacker tries to bombard a website with traffic from multiple sources, causing the site to become overwhelmed and crash.

Attackers create a network of infected computers known as botnets by sending and spreading malware through websites, emails and social media.

1/3 of all downtime incidents are attributed to DDoS attacks[9]

Once the malware has been distributed it allows the hacker to launch an attack remotely, sometimes using a botnet of over a million different users, without their knowledge.

There are places on the Dark Web where it is possible buy and sell botnets or individual DDoS attacks. For a small fee, a fraudster can disrupt an organisation's online operations, causing them to lose out on sales and suffer from damage to their reputation.

[9]Verisign/Merril Research, 2015.

Protecting your business against network attacks

- Use a Virtual Private Network (VPN) for remote access. VPNs add privacy and security to public networks and are used by corporations to protect sensitive data
- In the absence of a VPN, avoid unknown public Wi-Fi sources and only use trusted secure connections
- On sites that require you to input sensitive information, look for 'https' at the beginning of the website URL – the 's' stands for 'secure'
- Ensure there is a padlock symbol in the URL address bar - this shows that your connection is secure
- Configure routers to halt more simple attacks by stopping invalid IP addresses
- Use intrusion-detection systems (IDS) which can provide some protection against valid protocols being used against you in an attack
- Invest in DDoS mitigation appliances which can help to block illegitimate traffic to your website
- Consider buying excess bandwidth that can handle spikes in demand. Alternatively, use an outsourced provider where you can buy services on demand, such as burstable circuits that provide more bandwidth when you require it.