

The Good and Bad of the Internet

Objectives

- To learn about the good and bad of the internet
- To learn about the dark web
- To learn about the virus, worm, and trojan horse
- To talk about security flaws, from spoofing, to the middle man attack
- Learn about white hat, grey hairs, and black hat hacker

Lessons

To learn about the good and bad about the internet, and how to respect the internet



Bring out examples of each topic

What is the good thing about the internet?

- Faster communication
- Access to information (learning)
- Good for the economy

What is the bad thing about the internet?

- **Criminal activity**

Internet crime is any crime or illegal online activity committed on the Internet, through the Internet or using the Internet. The widespread Internet crime phenomenon encompasses multiple global levels of legislation and oversight. In the demanding and continuously changing IT field, security experts are committed to combating Internet crime through preventative technologies, such as intrusion detection networks and packet sniffers.

- **Internet misuse**

maladaptive pattern of Internet use, characterised by psychological dependence, withdrawal symptoms when off-line for prolonged periods, loss of control, compulsive behaviour, and clinically significant impairment of normal social interactions or distress

Adverse effects Cyberaffairs, addiction to online games, violence following financial miscalculations by day traders, and other risky behaviour

- Wrong information, which facilitates propaganda

Etymologically, the word propaganda comes from the word propagate – to spread. In its oldest context, it simply refers to the spreading of a message, whether through word of mouth, or through print media. It's similar both to publishing and to evangelizing, in that sense.

What is a virus?

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

What is a worm?

A worm is a type of malware that can copy itself and often spreads through a network by exploiting security vulnerabilities. It can spread through email attachments, text messages, file-sharing programs, social networking sites, network shares, removable drives, and software vulnerabilities.

What is a trojan horse?

A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

What is spoofing?

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an **advanced persistent threat** or a **man-in-the-middle attack**.

Successful attacks on organizations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organization's public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.

TYPES OF SPOOFING ATTACKS



Caller ID



Website spoofing



Email spoofing



IP spoofing



Text message spoofing



DNS spoofing



ARP spoofing



GPS spoofing



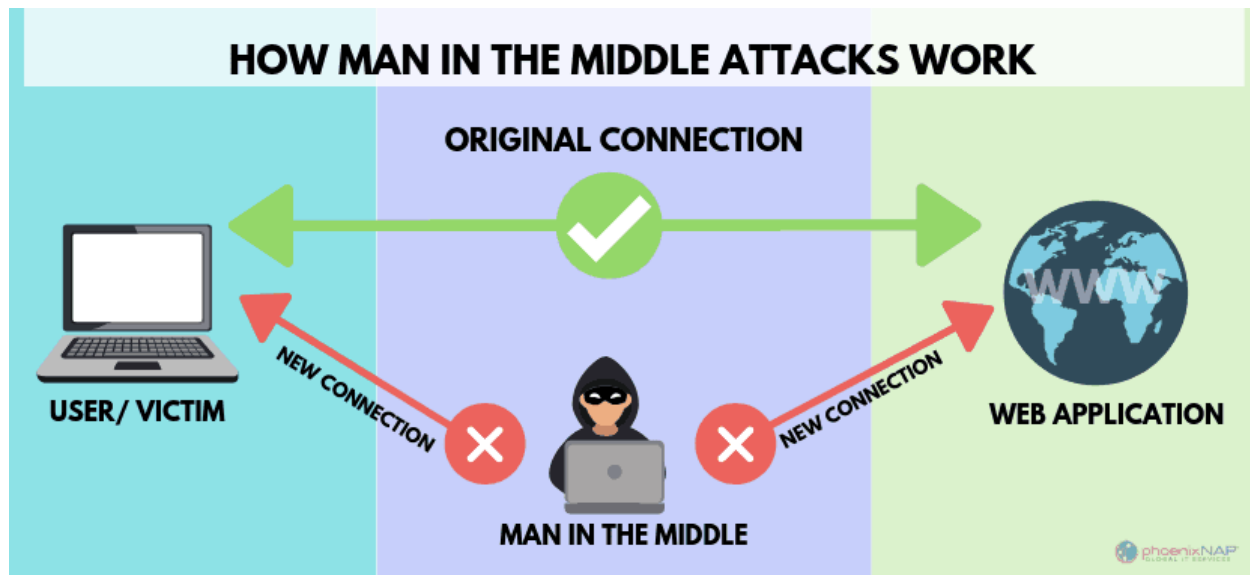
Extension spoofing



Man-in-the-middle spoofing

What is a 'man in the middle' attack

The act of listening to internet traffic, and using the information to hack electronic devices and systems



In cryptography and computer security, a **man-in-the-middle**, **monster-in-the-middle**, [1][2] **machine-in-the-middle**, **monkey-in-the-middle**, [3] **meddler-in-the-middle** [4] (MITM) or **person-in-the-middle** [5] (PITM) attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties. [6] One example of a MITM attack is active eavesdropping, in which 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. This is straightforward in many circumstances; for example, an attacker within the reception range of an unencrypted Wi-Fi access point could insert themselves as a man-in-the-middle. [7][8][9]



As it aims to circumvent mutual authentication, a MITM attack can succeed only when the attacker impersonates each endpoint sufficiently well to satisfy their expectations. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority. [10][8]

What is a Hacker?

A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more.

Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.

Challenges

 Name	 Question
<u>Most Popular White Hacker</u>	Give us a summary on what these hackers did that made them popular
<u>Most Popular Grey Hat Hacker</u>	Give us a summary on what these hackers did that made them popular
<u>Most Popular Black Hat hacker</u>	Give us a summary on what these hackers did that made them popular
<u>The Tor Network</u>	Give me a popular protocol that blew the core protocol up, amongst the internet, including the damages that it did, that is still affecting us to this very day
<u>Other hacking methods</u>	Provide 3 different ways in which hackers acquire your information, and where does it end up
<u>Hackers tools</u>	Research on the most popular hacking tools known to man, and provide the basic information about it