Co-funded by the Erasmus+ Programme of the European Union

Realistic Education Among Digital Youth Project
LTT in Bratislava, Slovakia

CSOŠE P. G. FRASSATIHO

Mgr. Ing. Marko Miglierini

19.9. – 23.9.2022

REALISTIC · EDUCATION · AMONG · DIGITAL · YOUTH

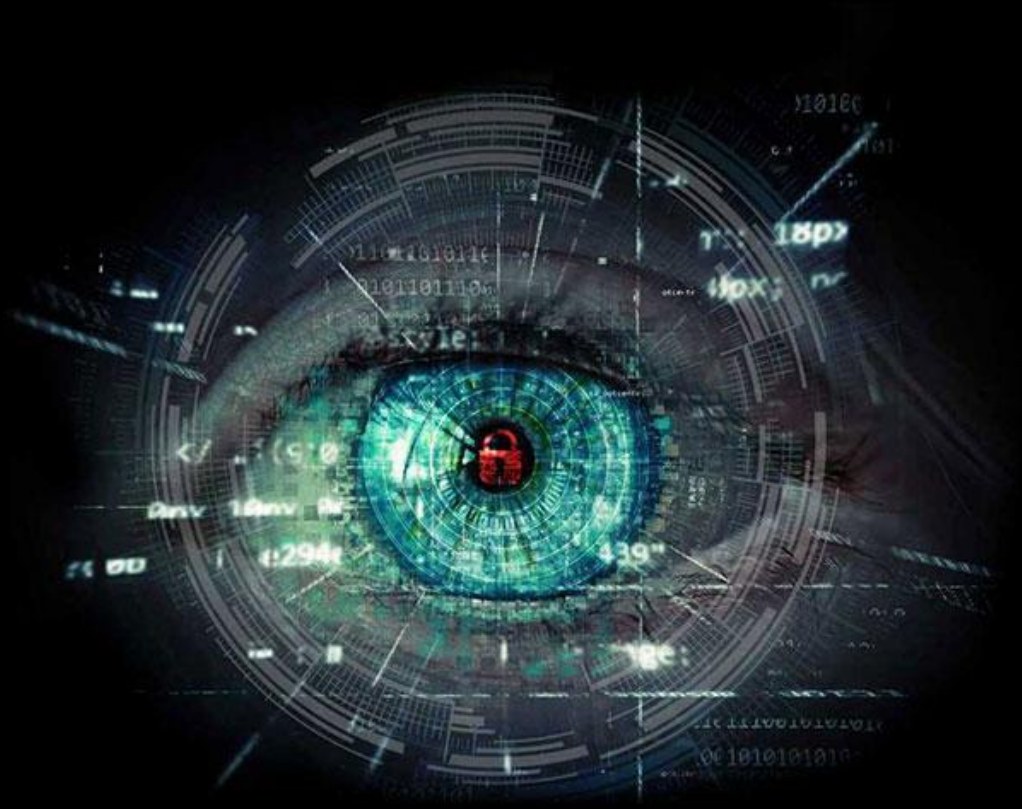
R · E · A · D · Y

Cyber Security

Be aware,
Big Brother is watching…

Orwell: 1984

Content
:



What is cybersecurity?

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

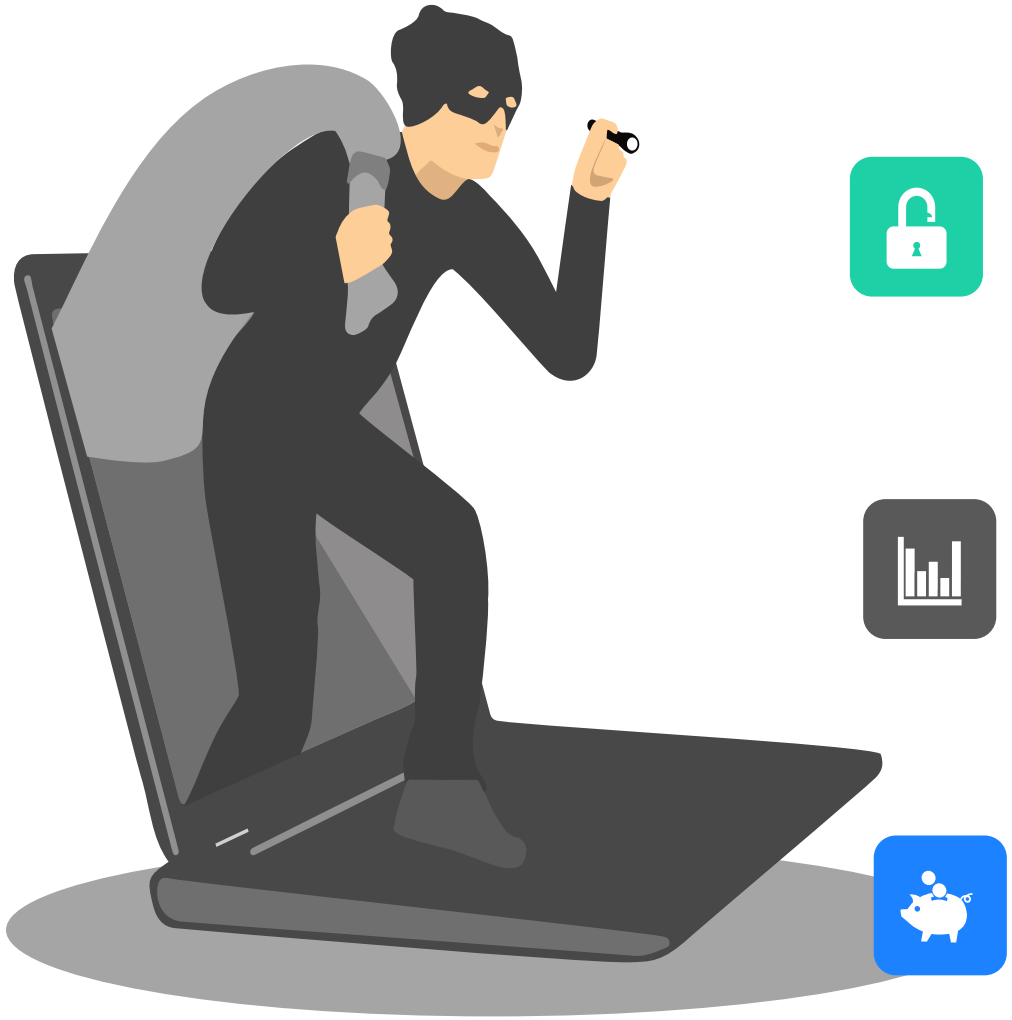
Who needs cyber security?

Everyone who is connected to the Internet needs cyber security. This is because most cyber attacks are automated and aimed to exploit common vulnerabilities rather than specific websites or organizations.

BE AWARE!

Everything you type into non secured PC or laptop is possibly like you shout your information to the whole world, to anybody, and everybody...

Why is cyber security important?



Cyber attacks are increasingly sophisticated

It is a critical, board-level issue

Cyber crime is a big business

1. The cybersecurity glossary

Blackhat hacker

A **person who** uses programming skills to cause **damage** to a computer system, steal data and in general conduct illegal cyber activities.

Whitehat hacker

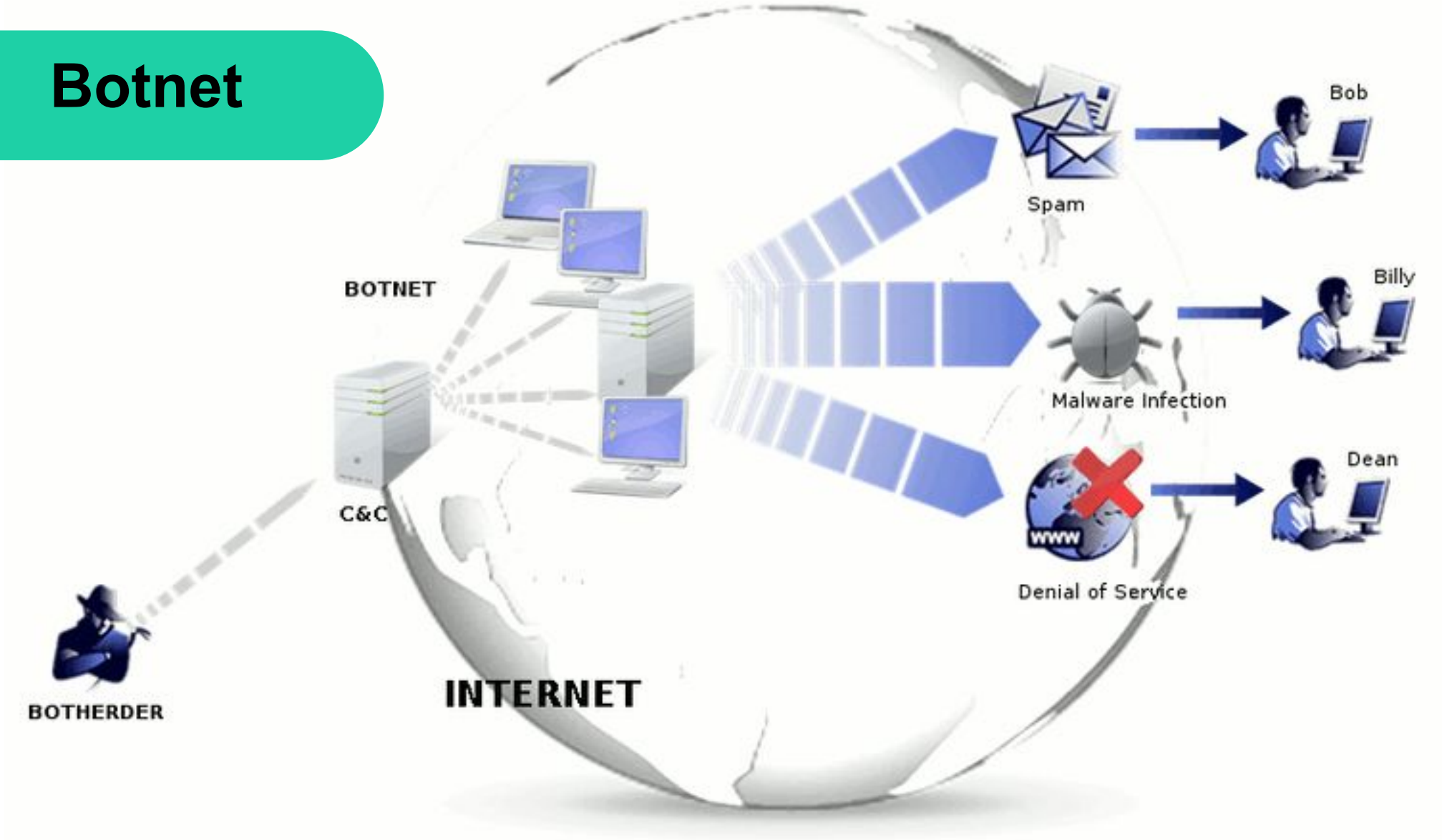
A **person who uses his hacking skills for an ethical purpose**, as opposed to a Blackhat hacker, who typically has a malicious, harmful intent. Businesses hire these individuals to test their cybersecurity level.

Exploit

A malicious **application or script** that can be used to take advantage of a **computer's vulnerability**.

Botnet's can be used for all kinds of malicious activities

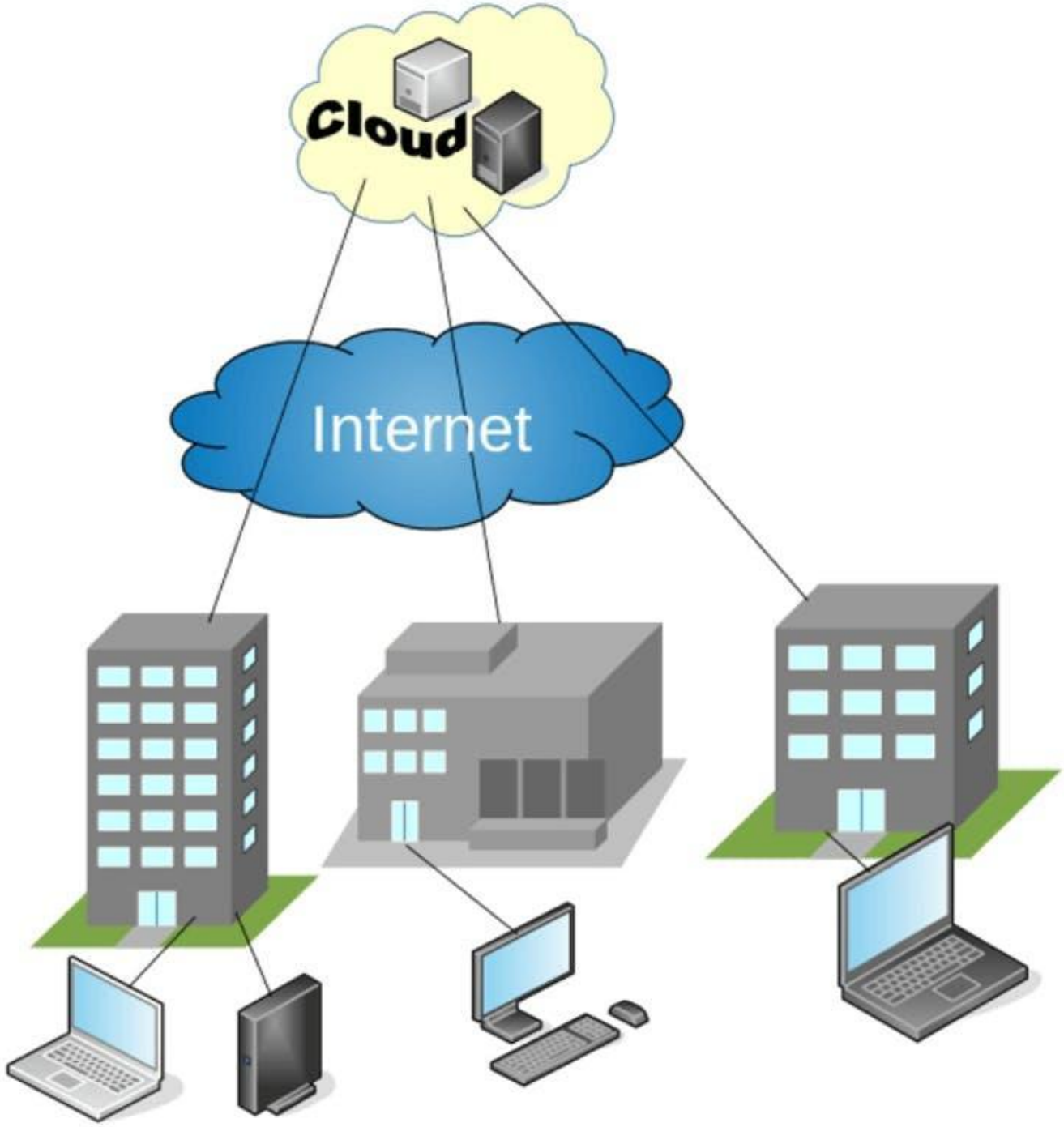
Botnet



Cloud/computing

Cloud is a large storage capabilities that remotely serve customer files from anywhere in the world and backuped safely.

Cloud computing uses a **network of remote servers** hosted on the Internet to process data, rather than a local server or a PC.



Command-and-control server

An **application that controls all bots in a botnet** . The hacker will send a command through this server, which then relays it to all compromised computers in the network.

DDoS

An acronym that stands for **distributed denial of service – a form of cyber attack**. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).

Encryption

An algorithmic technique that **changes file content** into something **unreadable** to those outside the chain of communication. If we use a Caesar cipher on the word "hello", it becomes "ifmmp".

Firewall

A “wall” or filter is created that judges each attempted interaction with a user’s computer and Internet connection to determine “should this be allowed entry or not?” Firewalls can be hardware or software-based.

E.g. **You leave “bad guys” outside of your systems**.

Phishing

A technique used by hackers **to obtain sensitive information**: passwords, bank accounts or credit cards. An unexpected email is received disguised as being from a legitimate source. It attempts to trick you into either replying with the information they seek, like bank details, or to click a malicious link or run an attachment.

Malware

An umbrella term that describes **all forms of malicious software** designed to cause havoc on a computer. Typical forms include viruses, trojans, worms and ransomware.

Ransomware

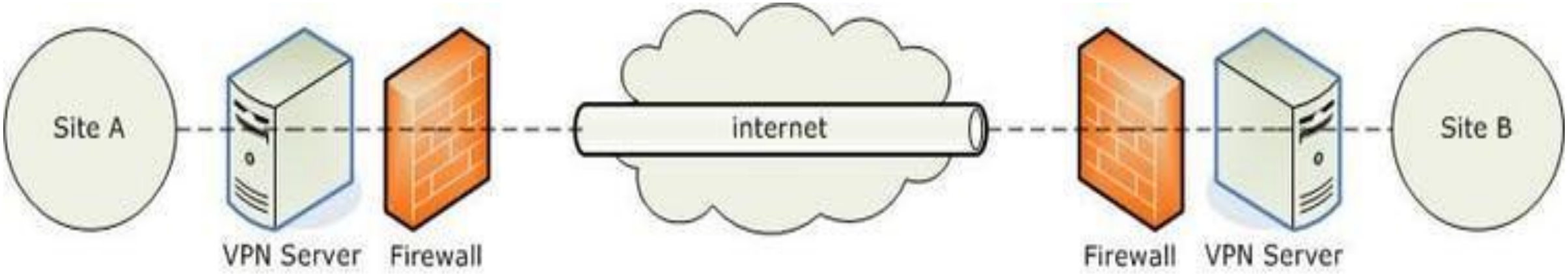
A form of malware that deliberately **prevents you from accessing files** on your computer. It will typically encrypt files and request that a ransom be paid in order to have them decrypted.

Spoofing

A technique **hackers use to hide their identity,** pretend to be someone else or simply try to fool you over the Internet. It looks like it's coming from another source, sending e-mails that appear to come from a different person, and website spoofing - fake website to trick users into entering sensitive information.

Virtual Private Network

A tool that allows the **user to remain anonymous while using the Internet.** It does this by masking location and encrypting traffic as it travels between the user's computer and the website they're visiting.



Virus

A type of malware for personal computers, dating back to the days of floppy disks. Typically **corrupts, erase or modify information on a computer** before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.

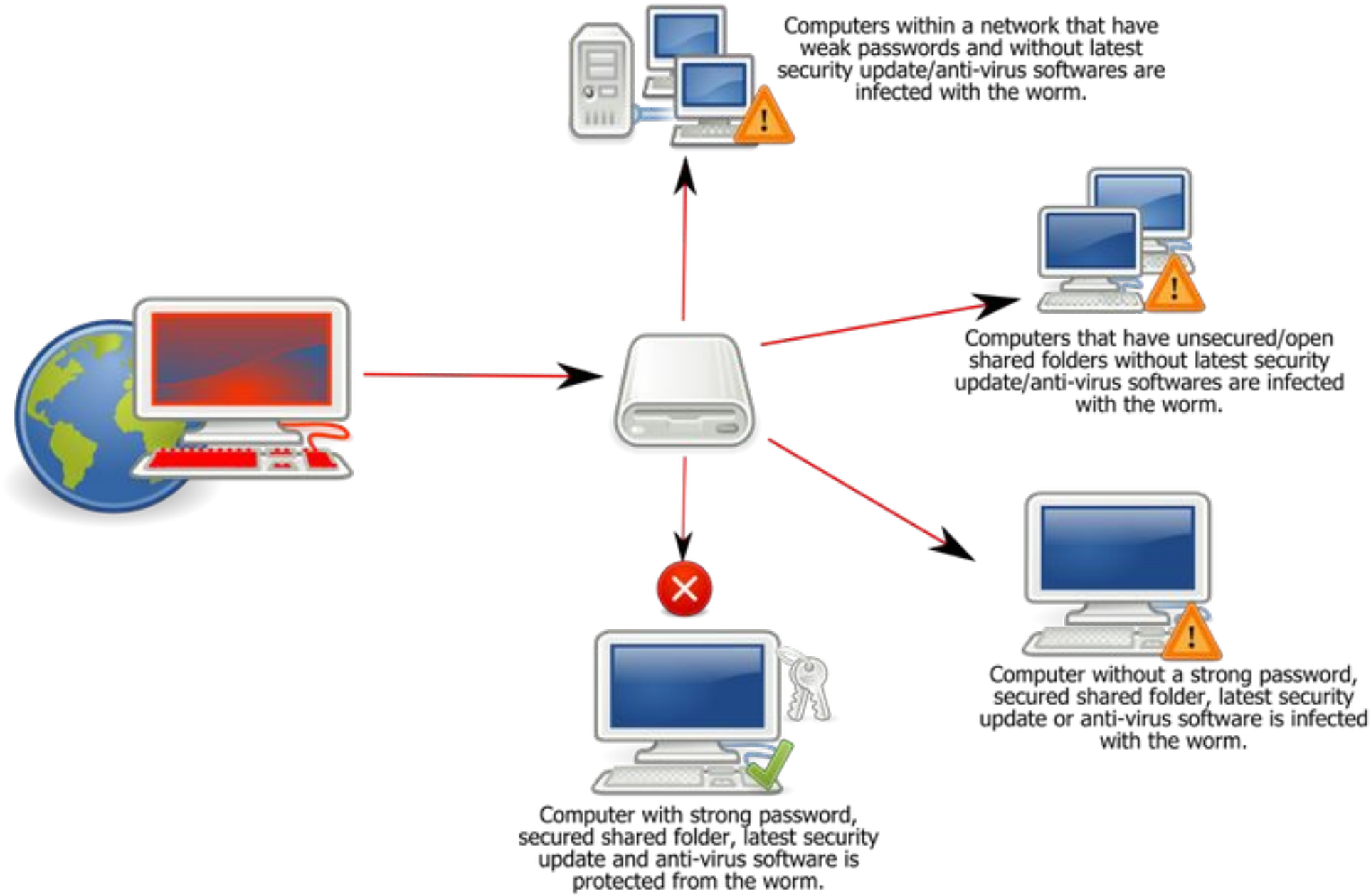
Trojan horse

An umbrella term that describes all forms of malicious software **designed to cause havoc on a computer.** Typical forms include viruses, trojans, worms and ransomware.

Worm

A piece of **malware that can replicate itself** in order to spread the infection to other connected computers. It will actively hunt out weak systems in the network to exploit and spread. On the next slide there is an example of a common worm, named the Win32 Conficker.

Worm:Win32 Conficker



https:// vs http://

Two protocols that allow computers to communicate.

HTTP helps nternet browsers communicate. **HTTPS it adds security**. It encrypts all data by creating a secure tunnel between you and the website you're visiting - in online shopping and internetbanking.

Zero Day

A particular form of **software exploit**, usually malware. They are **unknown to the public** or the software vendor. Because few people are aware of the vulnerability, they have "zero days" to protect themselves from its use.

Zombie

A **computer system that has been infected** by malware and is now part of a hacker's botnet.

Backdoors — Setting or code which allows remote access

Formjacking — Inserts malicious code into online forms

Cryptojacking — Installs illicit cryptocurrency mining software

Dangerous cybersecurity myths

- A basic antivirus will be enough to protect my business
- Cybersecurity isn't my responsibility
- Hackers don't target small businesses
- My passwords will keep me safe
- We only need to protect against hackers

Best practices

1. Staff awareness training

2. Application security

3. Network security

4. Leadership commitment

5. Password management

1.Staff awareness training

Human error is the leading cause of data breaches. It is therefore essential that you equip staff with the knowledge to deal with the threats they face. You will show employees how security threats affect them and help them apply best-practice advice to real-world situations.

2. Application security

Web application vulnerabilities are a key point of intrusion for cyber criminals.

3. Network security

It is the process of **protecting the usability and integrity of your network** and data. You should conduct a network penetration test, which assesses your network for vulnerabilities and security issues.

4. Leadership commitment

Leadership commitment is esential to cyber resilience. Without it, it is tough to establish or enforce effective processes. Companies should be prepared to invest in appropriate cyber security resources, such as awareness training.

5. Password management

For example, almost half of the UK population uses **‘password’, ‘123456’ or ‘qwerty’** as their password. It is needed to implement a password management policy that provides guidance to ensure staff create strong passwords and keep them secure.

THANK YOU

FOR YOUR PATIENCE