CYBERSECURITY GLOSSARY OF TERMS

As the world faces the impact of increased Cybersecurity exposures, it is imperative that we all became familiar with aspects of the related risks.

At **CyberEYE**, we have complied some of the key terms used in the Cybersecurity space so you can refer to them at your convenience.

We trust this serves to assist you.

Compiled by G. Figaro of CyberEYE Ltd

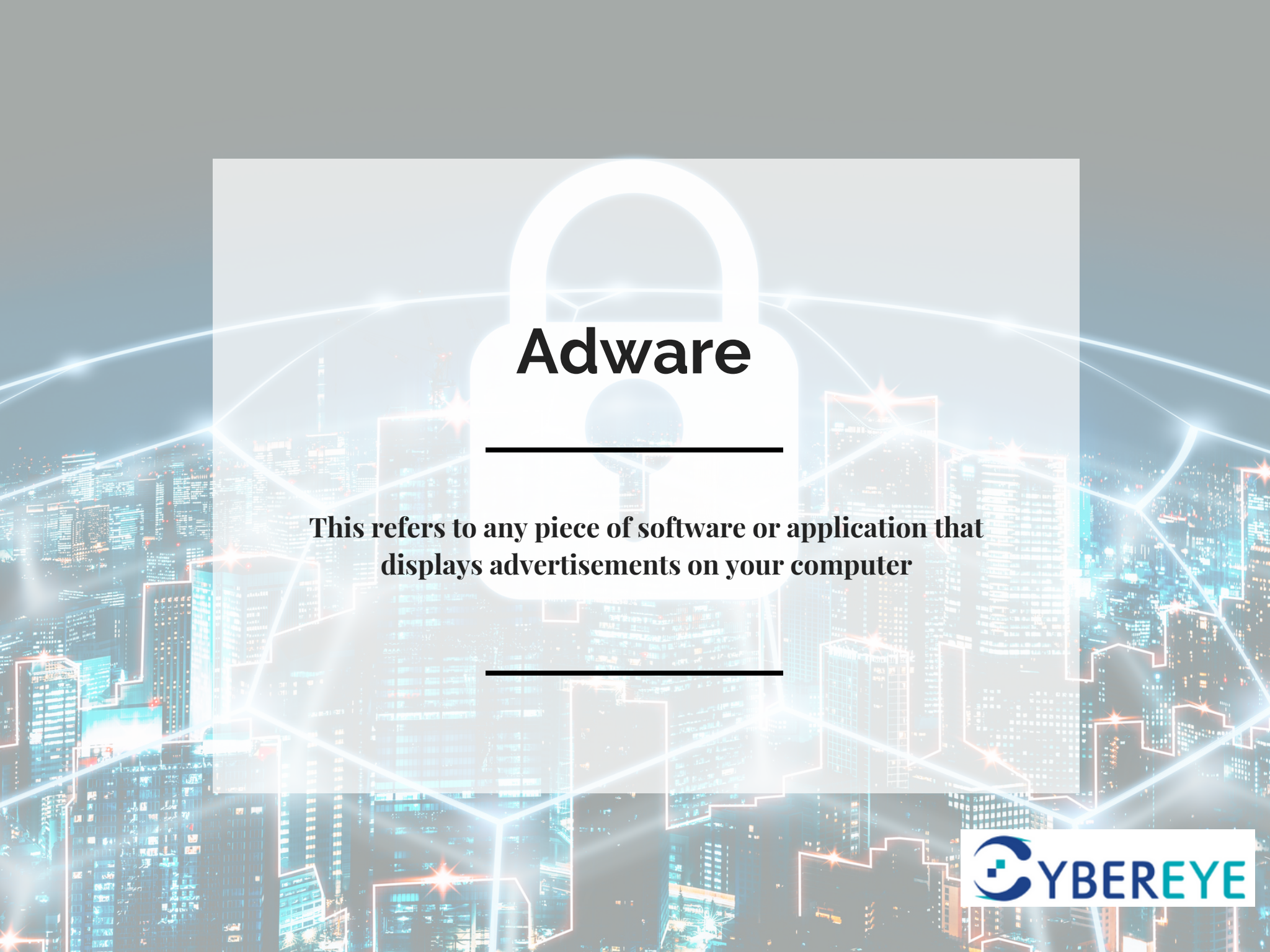
CYBEREYE

Advanced Persistent Threat (APT)

This is an attack in which an unauthorized user gains access ti a system or network without being detected.

Adware

This refers to any piece of software or application that displays advertisements on your computer



Access

The ability to interact and/ or communicate with a system in order to gain information from the system or to control its components and functions

CYBEREYE

Anti-Virus Software

This is a computer program used to prevent, detect and remove malware.

Artificial Intelligence (AI)

This refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.

CYBEREYE

Attachment

This is a computer file sent with an email message.

CYBEREYE

Authentication

The process of identifying a user's identity, making sure they can have access to the system and files. This can be accomplished by a password, retina scan, fingerprint etc.

Back Door

A back door is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.

Backup

To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss.

Baiting

This involves enticing an online victim with an incentive,

Behavioral Analytics

Behavioral analytics is the process of collecting and analyzing data from actions performed by users of a digital product, such as an application etc.

CYBEREYE

Black Hat Hacker

A person who hacks into a computer network with malicious or criminal intent.

Bluetooth

This is a wireless technology for exchanging data over short distances.

Bot/ Botnet

This is combination of the words "robot" and "network". A botnet is a network of computers that have been infected with a virus and are now working continuously in order to create security breaches.

Broadband

This is a high speed data transmission system where the communications circuit is shared between multiple users.

Browser

A browser is software that is used to access the internet.
Examples are Chrome, Safari, Edge, Firefox etc.

Brute Force Attack

This is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.

CYBEREYE

Bug

This refers to an error, fault or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.

CYBEREYE

BYOD

Means "Bring Your Own Device". It refers to a company security policy that allows staff to use their personal devices for company business. A BYOD policy sets limitations and restrictions on whether or not a personal phone or laptop can be connected to a corporate network.

CYBEREYE

Clickjacking

A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.

Cloud

A technology that allows us to access our files and/ or services through the internet from anywhere in the world. Technically speaking, it is a collection of computers with large storage capabilities that remotely serve requests.

CYBEREYE

Cookie

These are small files which are stored on a user's computer. they provide a way for a website to recognize you and keep track of your preferences.

Critical Update

A fix for a specific problem that addresses a critical, non-security related bug in computer software,

Cyber Hygeine

This refers to fundamental cybersecurity best practices that an organization's security practitioners and users can undertake

CYBEREYE

Cyber Warfare

This typically refers to cyber attacks perpetrated by one nation state against another.

Data Breach

This is the result of a hacker successfully breaking into a system, gaining control of its network and exposing its data. This typically involves financial information, confidential files, personal data etc.

CYBEREYE

Data Lake

A data lake is a storage repository that holds a vast amount of raw data in its native format until it is needed for analytics applications.

CYBEREYE

DDoS

This is an acronym for " Distributed Denial of Service". It is a favourite "Black Hat" Tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.

CYBEREYE

Deepfake

An audio or video clip that has been edited and manipulated to seem real or believable. They can have far reaching consequences especially in terms of financial, political or bias-based impacts.

CYBEREYE

Domain

A series of computers and associated peripherals like routers, printers, scanners etc, that are all connected as one entity.

Domain Name

The part of a network address which identifies it as belonging to a particular domain.

Domain Name Server (DNS)

A server that converts recognizable domain names into their unique IP address

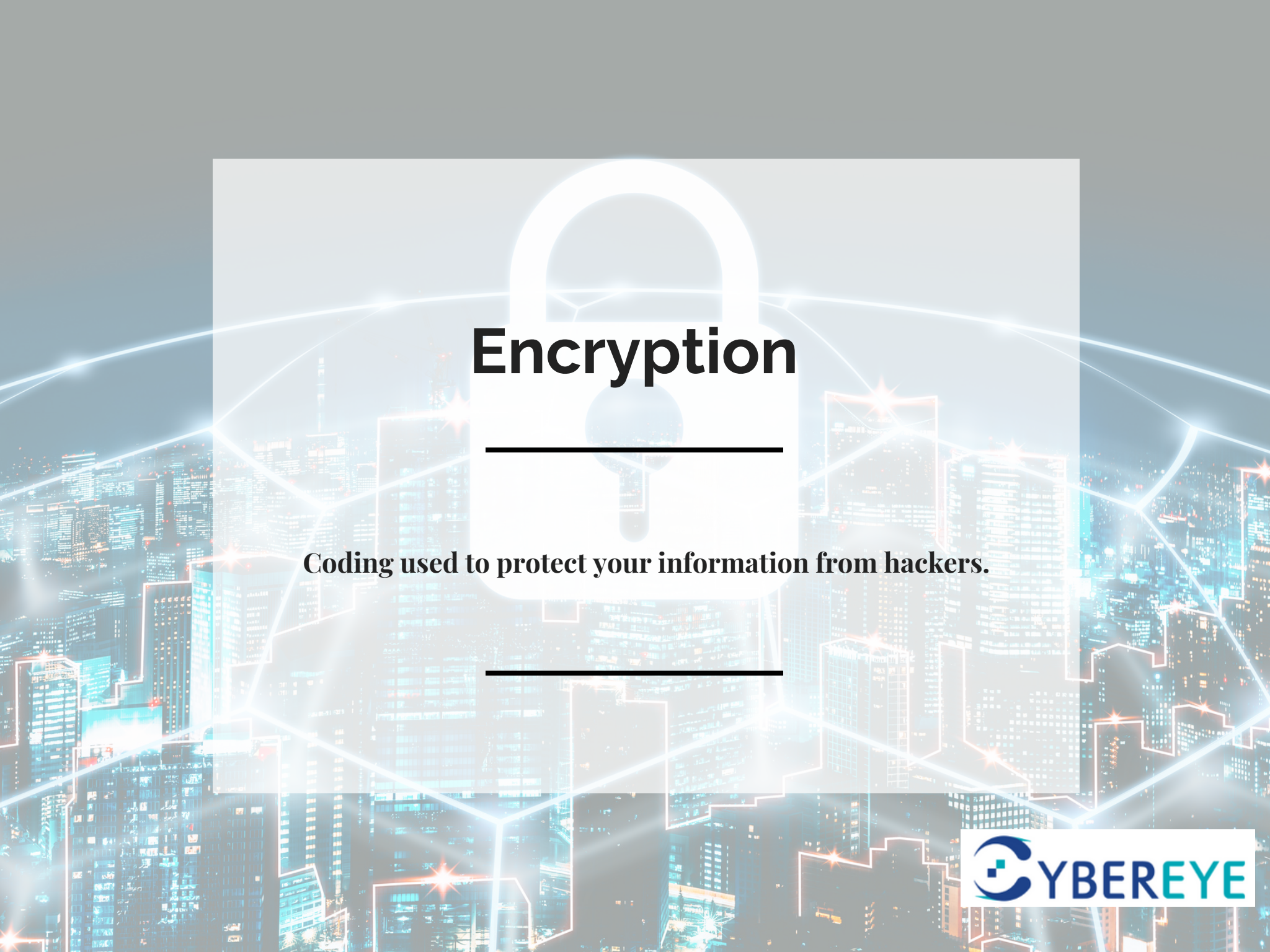
Download

To copy data from one computer system to another, typically over the internet.

Dynamic Testing

Dynamic Testing is a type of Software Testing which is performed to analyze the dynamic behavior of the code. It includes the testing of the software for the input values and output values that are analyzed.

CYBEREYE



Encryption

Coding used to protect your information from hackers.

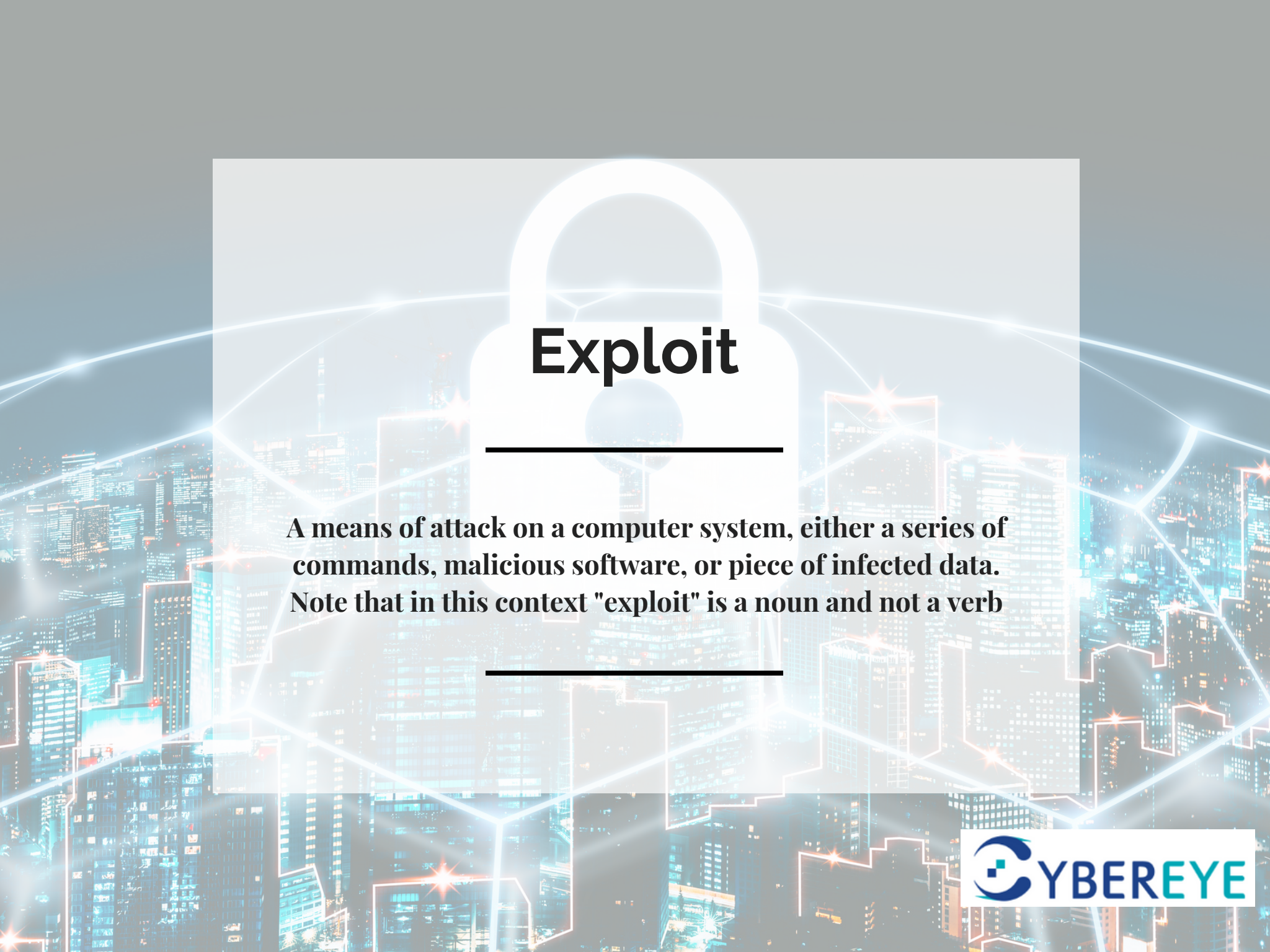
CYBEREYE

Ethical Hackers

See "White Hat Hackers"

Exploit

A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context "exploit" is a noun and not a verb



Firewall

Any technology, be it software or hardware, used to keep intruders out.

Hacking

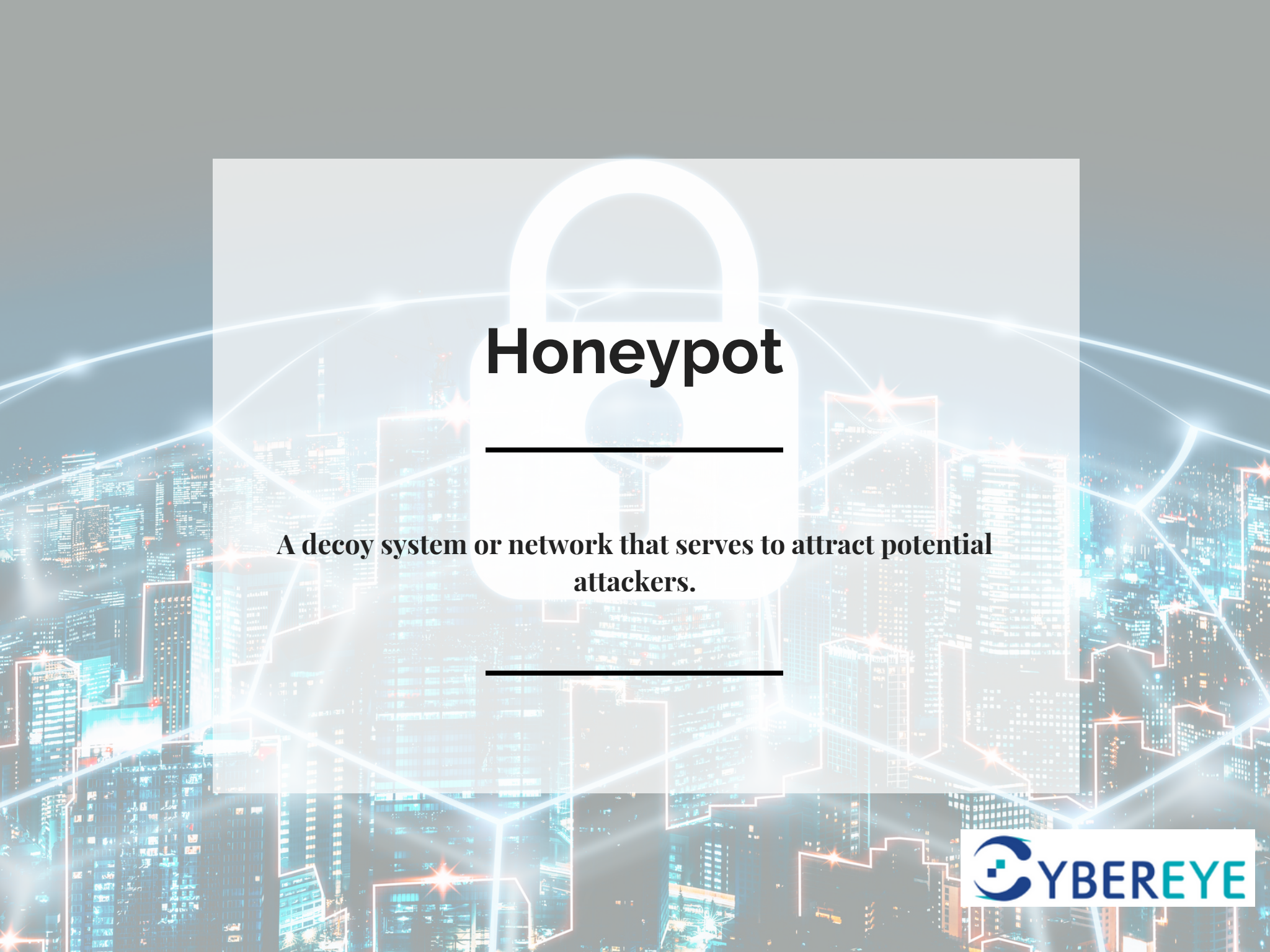
This refers to unauthorized intrusion into a computer or a network

CYBEREYE

Homomorphic Encryption

This refers to a form of encryption that permits users to perform computations on its encrypted data without first decrypting it.

CYBEREYE



Honeypot

A decoy system or network that serves to attract potential attackers.

CYBEREYE

HTML

This stands for "Hypertext Markup Language". It is the standard markup language for creating web pages and web applications.

Identity and Access Management (IAM)

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities

CYBEREYE

Identity Theft

This is a crime in which someone uses personally identifiable information in order to impersonate someone else.

CYBEREYE

Incident Response Plan

This is a policy which lays out the organization's response ro an information security incident.

Internet of Things (IoT)

This refers to billions of physical devices around the world that are now connected to the internet and are collecting and sharing data.

IP Address

An internet version of a home address for your computer which is identified when it communicates over a network (such as when it connects to the internet).

CYBEREYE

Keystroke Logger

This is a software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.

Malvertising

The use of online advertising to deliver malware.

Malware

A blend of the words "malicious" and " software". It describes a variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses and trojans are all considered to be malware and are often delivered via spam e-mails.

CYBEREYE

Man in the Middle Attack

An attack on the "middleman", in this case, defined as the Wi-Fi system that connects users to the Internet. Hackers who commit Man in the Middle Attacks can break the Wi-Fi's encryption and use this as a means of stealing your personal data because they are now in the system

CYBEREYE

Multi-Factor Authentication (MFA)

This provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.

CYBEREYE


Packet Sniffer
Software designed to monitor and record network traffic.
CYBEREYE

Patch

This is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.

Pen/Penetration Testing

This practice is a means of evaluating security strength by using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws with teh intent to address same.

CYBEREYE

Phishing

A scam where a hacker poses as a legitimate business or organization in order to fool the victim into giving them sensitive personal information or inducing them to click on a link or attachment that ends up delivering malware.

CYBEREYE

Proxy Server

This is another computer system which serves as a hub through which internet requests are processed,

Pre-Texting

This is an the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.

CYBEREYE

Ransomware

A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything.

Red Team Testing

Red Teaming places your organization's security team as close to a real security incident as possible, accurately testing incident response.

CYBEREYE

Rootkit

Another kind of malware that allows cybercriminals to remotely control your computer. Rootkits are especially damaging because they are hard to detect meaning they can live in your system for an extended period of time before being identified.

CYBEREYE

Router

This is a piece of network hardware that allows communication between your local home network and the internet

Scam

This term is used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.

CYBEREYE

Scareware

This type of malware is designed to trick victims into purchasing and downloading potentially dangerous software.

Secure Software Development Life Cycle (SSDLC)

This is a process for planning, implementing and maintaining software systems

Security Awareness Training

This is a training program aimed at heightening security awareness within an organization.

Security Operations Centre (SOC)

A SOC monitors an organization's security operations to prevent, detect and respond to any potential threat.

CYBEREYE

Segmentation

From a cybersecurity point of view, this is a physical or virtual architectural approach dividing a network into multiple segments, each acting as its own subnetwork providing additional security and control.

Smishing

Any kind of phishing that involves a text message.

Social Engineering

A technique use to manipulate and deceive people to gain sensitive and private information. Scams based on social engineering are built around how people think and act. Once a hacker understands what motivates a person's actions, they can usually retrieve what they are looking for, such as financial data and passwords

CYBEREYE

Software

A set of programs that tell a computer to perform a task. these instructions are compiled into a package that users can install and use.

Spear Phishing

This is an email-spoofing attack that targets a specific organization or individual , seeking unauthorized access to sensitive information.

CYBEREYE

Spoofing

When a hacker changes the IP address of an email so it seems to come from a trusted source.

Spyware

A form of malware used by hackers to spy on you and your computer activities. If a mobile device such as a phone for example, is infected with spyware, a hacker can read your text messages, redirect your calls and even track where you are physically located.

CYBEREYE

Static Testing

Static Testing is a type of a Software Testing method which is performed to check the defects in software without actually executing the code of the software application. Static testing is performed in early stage of development to avoid errors as it is easier to find sources of failures and it can be fixed easily

CYBEREYE

Tailgating

This involves someone who lacks the proper authentication but follows an employee into a restricted area

Trojan Horse

Yet another form of malware. This is a misleading computer program that looks harmless, but in fact allows the hacker ti enter your system via a back door which allows them to control your device.

Two Factor Authentication (2FA)

This is often referred to as two-step verification. It is a security process in which the user provides two authentication factors to verify their identity.

Universal Serial Bus (USB)

This is the most popular connection used to connect a computer to devices such as digital cameras, printers, scanners and external hard drives.

CYBEREYE

Virus

Malware which changes, corrupts or destroys information. It is then passed on to other systems, usually by otherwise benign means (such as sending an email). In certain cases, viruses can cause physical damage.

CYBEREYE

VPN

This is an acronym for "Virtual Private Network". A VPN is a method of connecting a series of computers and devices in a private encrypted network, with each user's IP address being replaced by the VPN's Ip address. users get Internet anonymity, making it difficult for hackers to attack.

CYBEREYE

Vulnerability

A vulnerability refers to a flaw in the system that can leave it open to attack.

Vishing

This is the telephone equivalent to phishing, It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft,

CYBEREYE

Whaling

This is a specific form of phishing that targets high profile executives and managers.

White Hat Hacker

A hacker who is invited to test out computer systems and servers, looking for vulnerabilities, for the purpose of informing the host of where securities need to be improved or introduced. They are intended to be harmless and serve only as a means to proactively identify and mitigate cybersecurity risks

CYBEREYE

Wi-Fi

This is a facility that allows computers, smartphones, or other devices to connect to the internet or communicate with one another wirelessly within a particular area,

CYBEREYE

Worm

This is malware that can reproduce itself for the purposes of spreading itself to other computers in the network. They are particularly troubling as they can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data

CYBEREYE

Zero-Day

This refers to a recently discovered vulnerability that hackers can use to attack systems

CYBEREYE

Zero-Trust Architecture

This is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage

CYBEREYE

Information was compiled from the following sources:

https://www.simplilearn.com
https://www.cybintsolutions,com
https://www.metacompliance.com
https://www.allot.com
https://www.techtarget.com
https://www.paloaltonetworks.com
https://amplitude.com
https://www.packetlabs.net
https://www.cisa.gov
https://www.redseal.net
https://www.geeksforgeeks.org

CYBEREYE