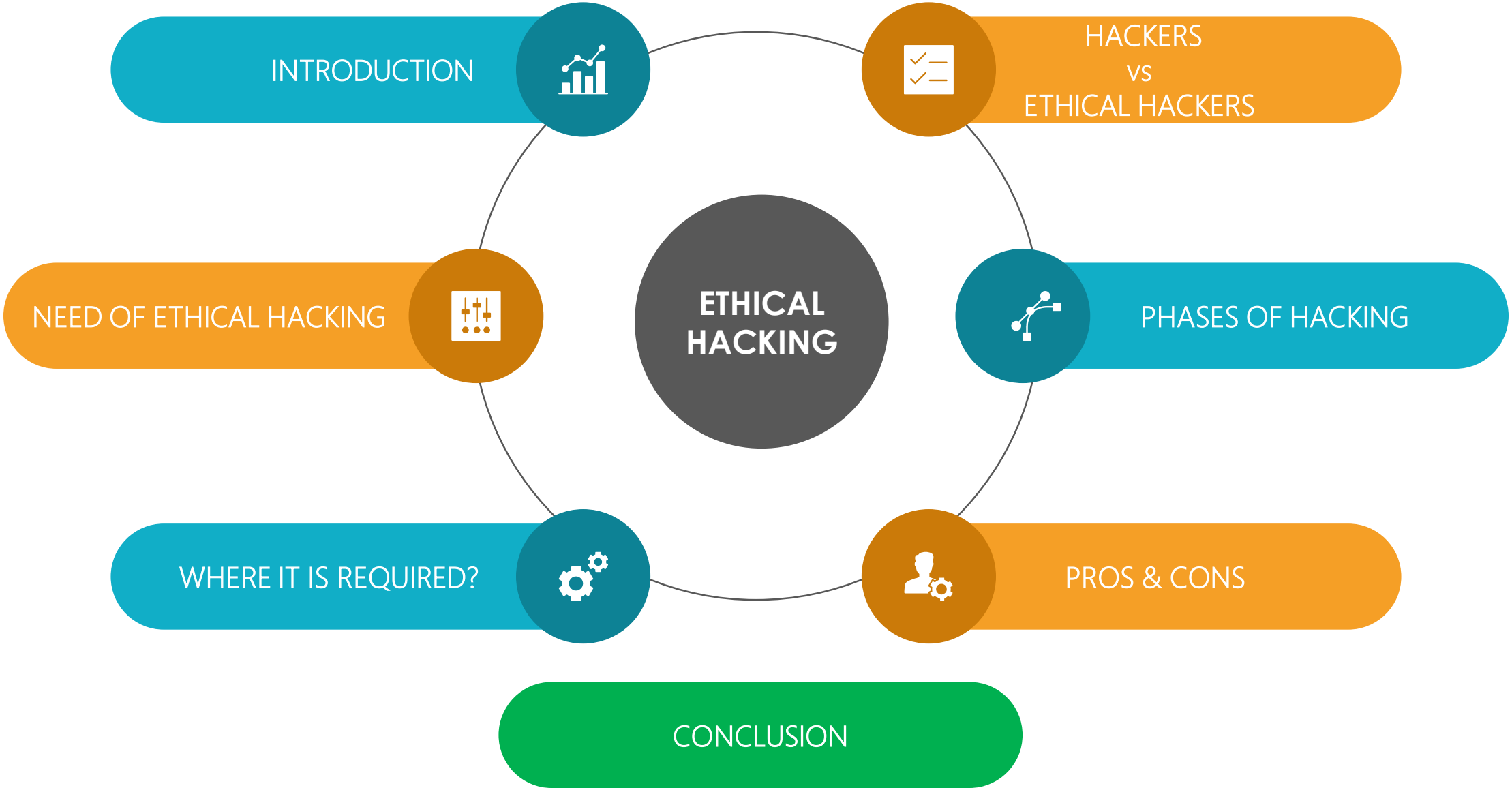
ETHICAL HACKING

Agenda


INTRODUCTION
HACKERS
vs
ETHICAL HACKERS
NEED OF ETHICAL HACKING
ETHICAL
HACKING
PHASES OF HACKING
WHERE IT IS REQUIRED?
PROS & CONS
CONCLUSION

Introduction

What is Hacking…?

HACKING REFERS TO ACTIVITIES THAT SEEK TO COMPROMISE DIGITAL DEVICES, SUCH AS COMPUTERS, SMARTPHONES, TABLETS, AND EVEN ENTIRE NETWORKS.

What is Ethical hacking…?

ETHICAL HACKING IS CONDUCTED BY HACKERS AS WELL, BUT THEIR INTENTION BEHIND HACKING IS TO SECURE THE ENVIRONMENT AND NOT FOR MALICIOUS PURPOSES.

Hackers vs Ethical Hackers

Hacker vs Ethical Hacker

A HACKER IS A PERSON WHO FINDS AND EXPLOITS THE WEAKNESS IN COMPUTER SYSTEMS AND/OR NETWORKS TO GAIN ACCESS. HACKERS ARE USUALLY SKILLED COMPUTER PROGRAMMERS WITH KNOWLEDGE OF COMPUTER SECURITY.

IN OTHERWORDS AN ETHICAL HACKER IS ALSO A SKILLED COMPUTER PROGRAMMER BUT HE EARNS SOME SECURITY CERTIFICATES TO WORK IN A DEFENSIVE PATH TO PROTECT THE ORGANIZATION ENVIRONMENT.

Types of Hackers…

1 BLACK HAT HACKERS

Completely hack for their own personal gains probably by hurting others.

2 WHITE HAT HACKERS

Hack for the good things and also act for Defensive purpose.

3 GREY HAT HACKERS

Who work both offensively and Defensively at various times depends on their need.

Methods of Hacking

Major Hacking Methods…

Phishing

Social Engineering

keyloggers

Spoofing

Skimming

Botnets

Need of Ethical Hacking

Primary Need...

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses.

Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.

Hacking can lead to loss of business for organizations that deal in finance. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Ethical Hacking is about improving the security of computer systems and/or computer networks.

Phases of Hacking

Reconnaissance

This is the first phase where the Hacker tries to collect information about the target.

Scanning

This phase includes usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data.

Gaining Access

In this phase, hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2.

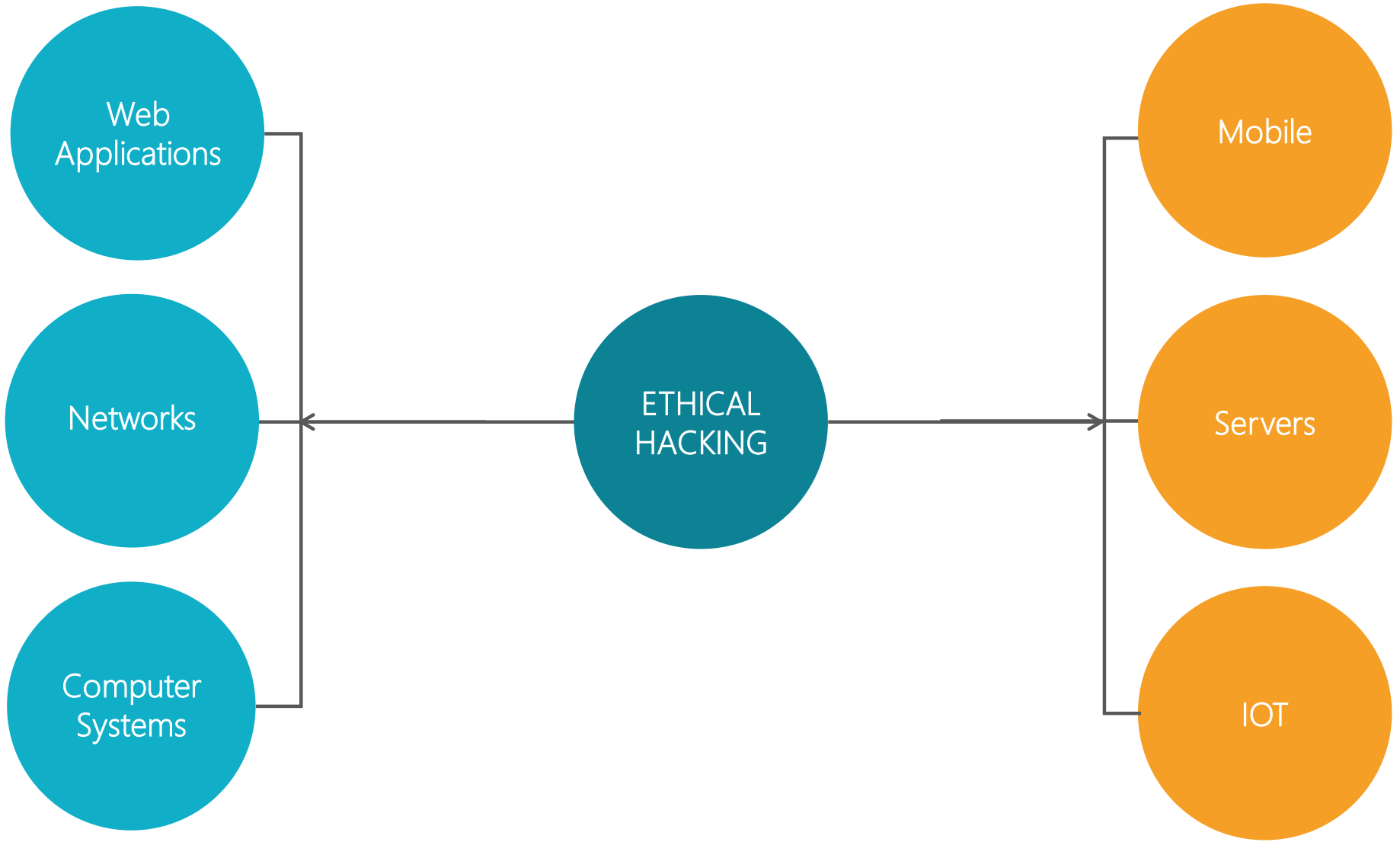
Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks.

Clearing Tracks

This includes clearing out Sent emails, clearing server logs, temp files, etc.

Where it is required



Hacking prevention

What to do...

First and foremost, download a reliable anti-malware product (or app for the phone), which can both detect and neutralize malware and block connections to malicious phishing websites.

Second, only download phone apps from the legitimate marketplaces that police themselves for malware-carrying apps, such as Google Play and Amazon Appstore.

Whether you're on your phone or a computer, make sure your operating system remains updated. And update your other resident software as well.

Avoid visiting unsafe websites, and never download unverified attachments or click on links in unfamiliar emails.

Hacking Impact

How Hacking affects

The malicious spam emails, disguised as familiar brands, trick your end users into clicking malicious download links or opening an attachment loaded with malware.

Cyber Criminals can enter into an organizations network with the help of Social Engineering, it may leads to complete organization compromise.

In an interesting twist, Emotet has evolved from being a banking Trojan in its own right into a tool for delivering other malware, including other banking Trojans like Trickbot.

Pros $ Cons

Pros…

"To catch a thief you have to think like a thief".

Helps in finding and closing the open vulnerabilities in the system or network.

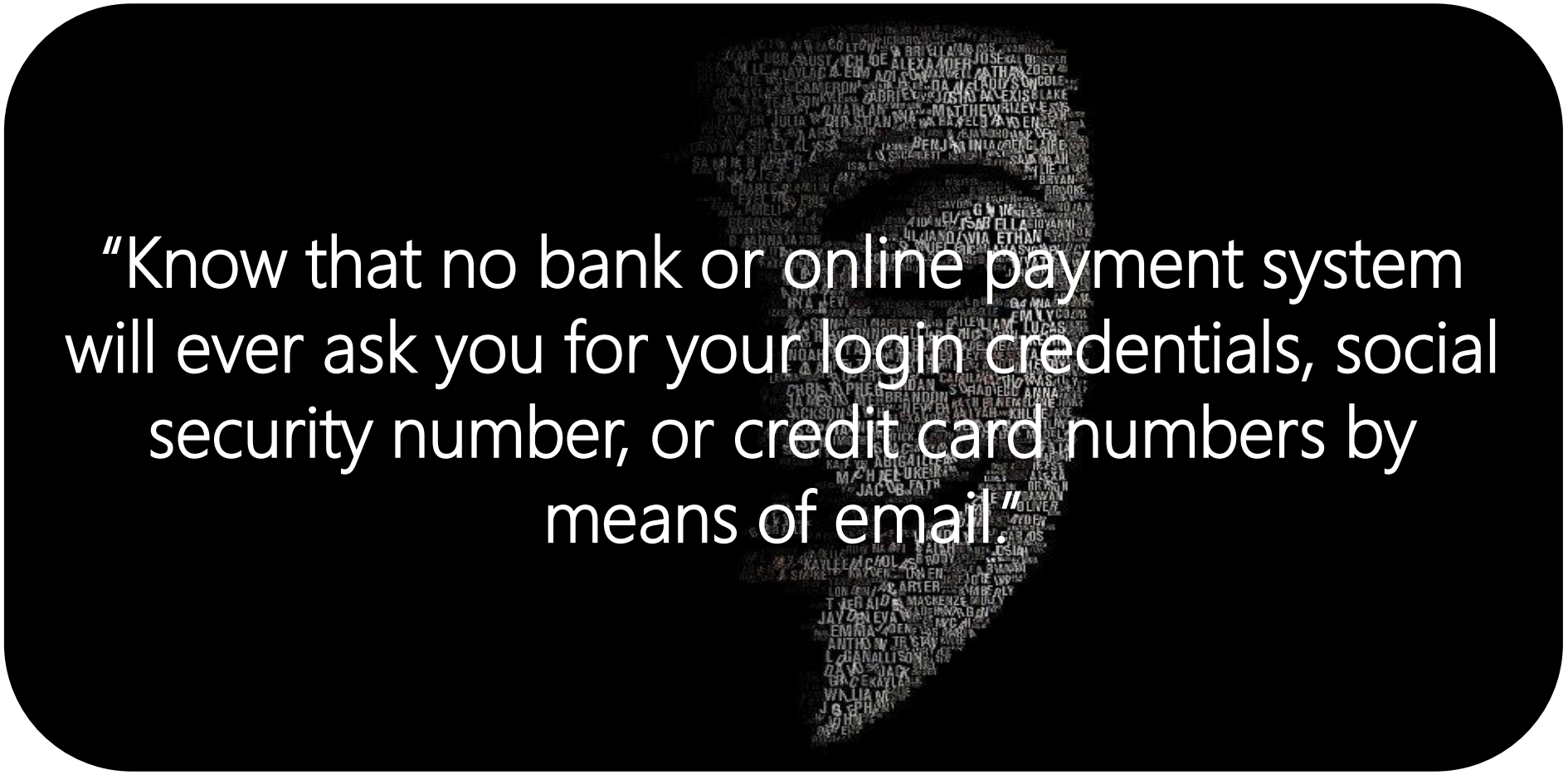
Provides security to banking and financial establishments and Prevents website defacements.

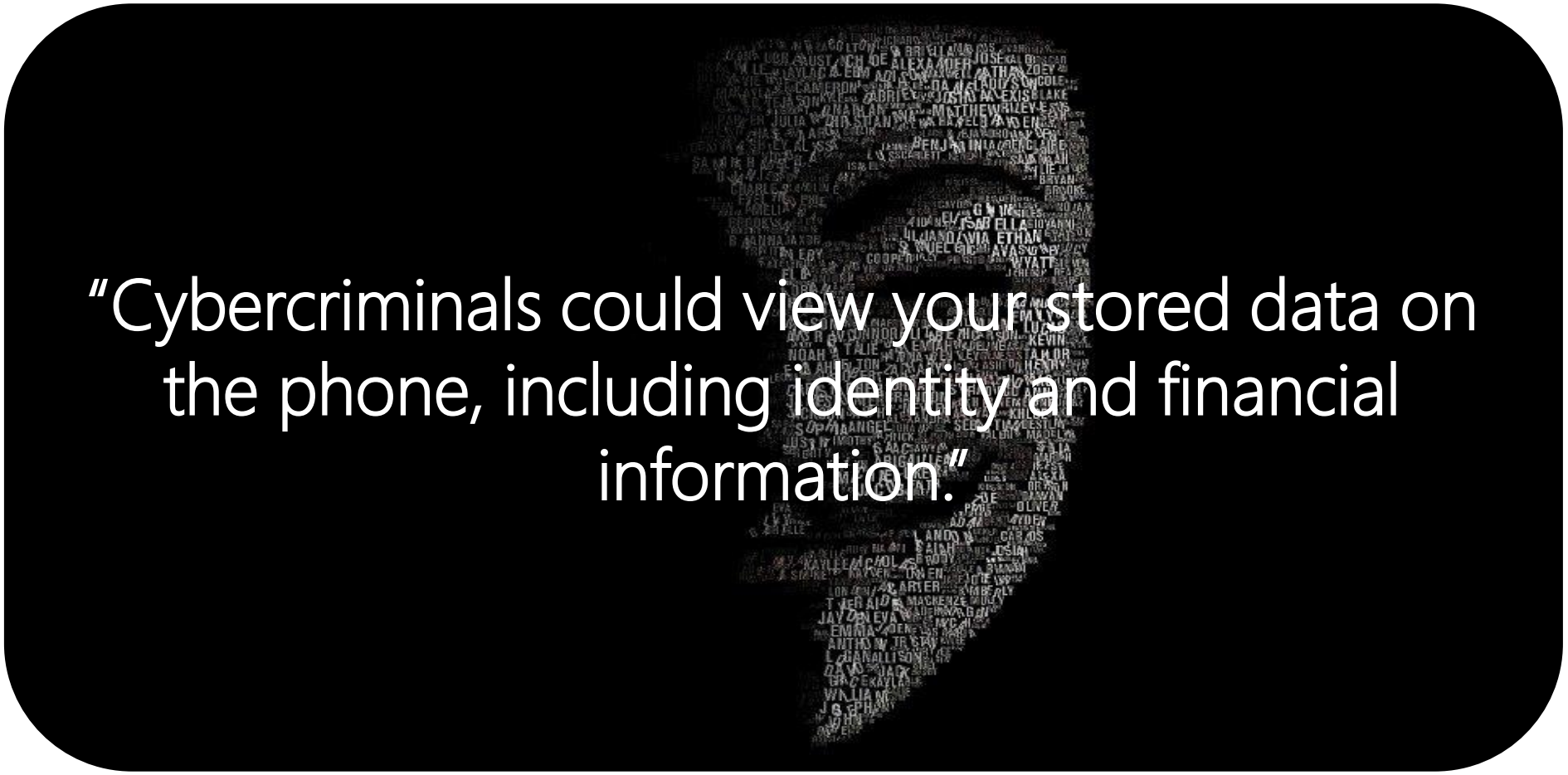
Cons…

All depends upon the trustworthiness of the Ethical Hacker.

Hiring professionals is expensive thing.


“Hacking has evolved from teenage mischief into a billion-dollar growth business.”


“Know that no bank or online payment system will ever ask you for your login credentials, social security number, or credit card numbers by means of email.”


"Cybercriminals could view your stored data on the phone, including identity and financial information."

Conclusion

Before we stop...

Backup all your data. This goes for all the endpoints on your network and network shares too. As long as your data is archived, you can always wipe an infected system and restore from a backup.

Educate staff on creating strong passwords and implement some form of multi-factor authentication (MFA)—two-factor authentication at a bare minimum.

The main thing we should do is to keep ourselves updated about those software's we are using for official and reliable sources.

Who am I

Naveen kumar
Certified Ethical Hacker
IT Associate (Cyber Security) – APTS
Vijayawada

Thank You