Regional Training Institute, Jaipur

Indian Audit & Accounts Department

Cyber Security

By Vinod Sencha
CF(IS) RTI Jaipur

Which is the third largest economy?

- USA
- China
- ????

Importance of Cyber Security

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

- Professor Gene Spafford

https://spaf.cerias.purdue.edu/

In security matters:

- There is nothing like absolute security
- We are only trying to build comfort levels, because security costs money and lack of it costs much more
- Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations

Importance of Cyber Security

- The Internet allows an attacker to work from anywhere on the planet.

- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and your organization)
  - Sanctions or termination if policies are not followed

- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights

Cyber Security

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

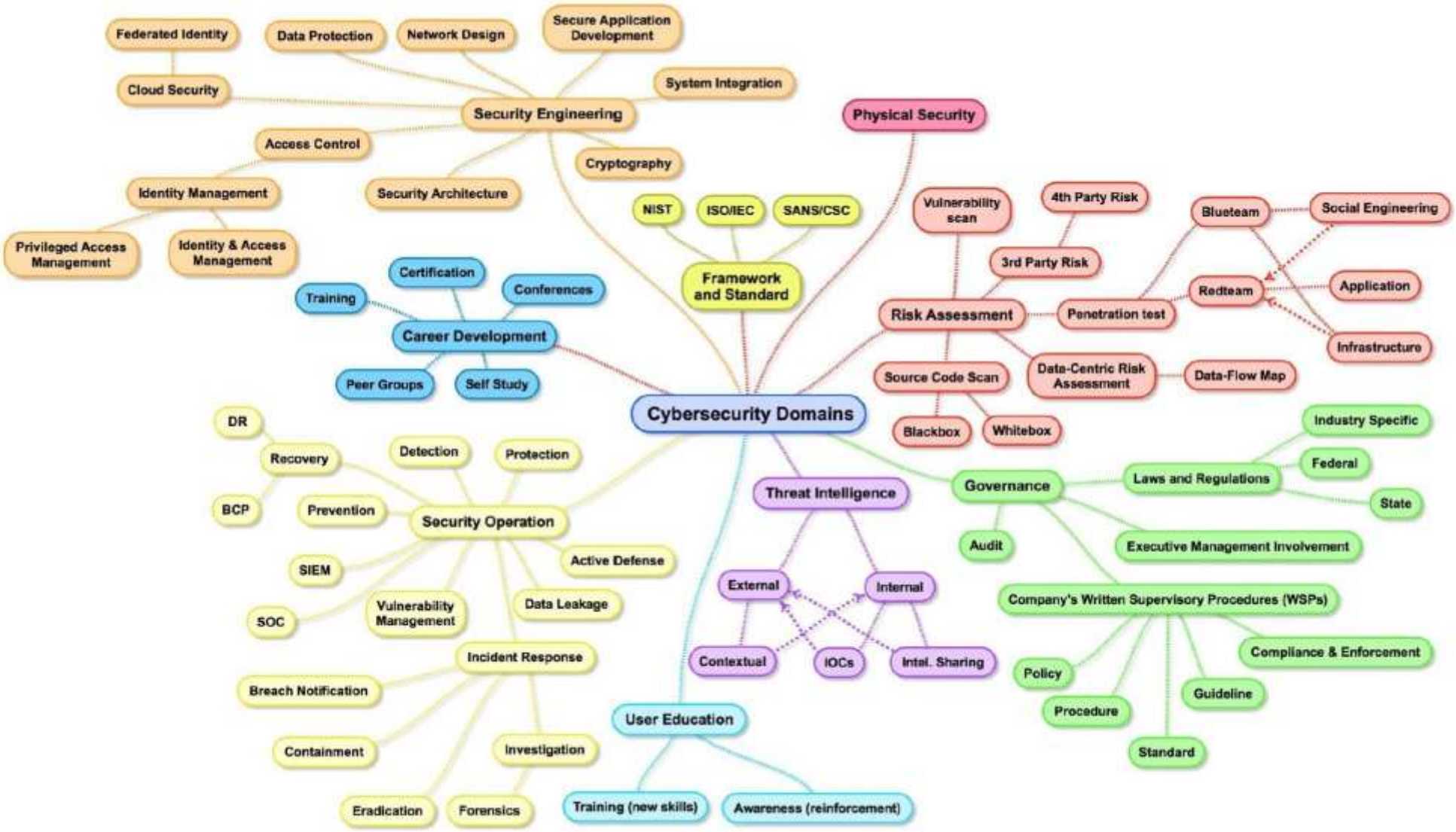
Cyber Security

https://www.varonis.com/blog/data-breach-statistics/

Cyber Security is Safety

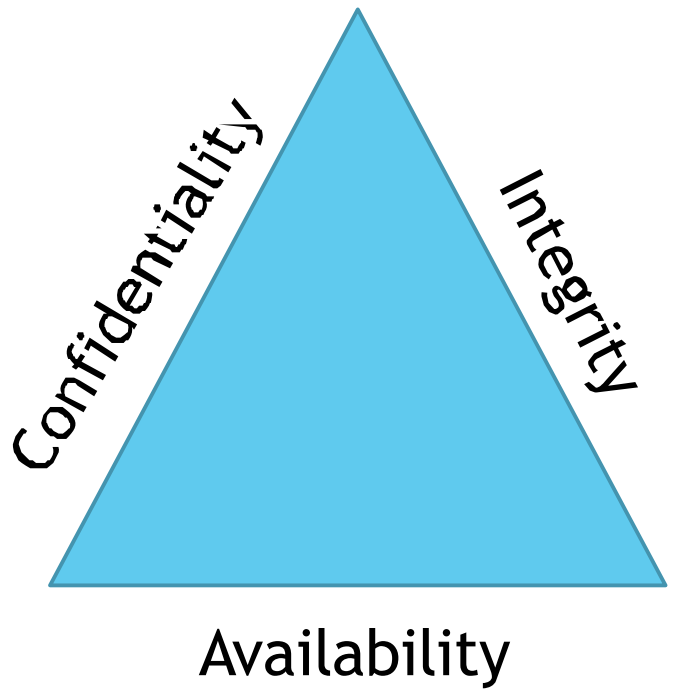
- Security: We must protect our computers and data in the same way that we secure the doors to our homes.
- Safety: We must behave in ways that protect us against risks and threats that come with technology.

Cyber Security Domains



False Sense of Security?

What is a Secure System? (CIA Triad)

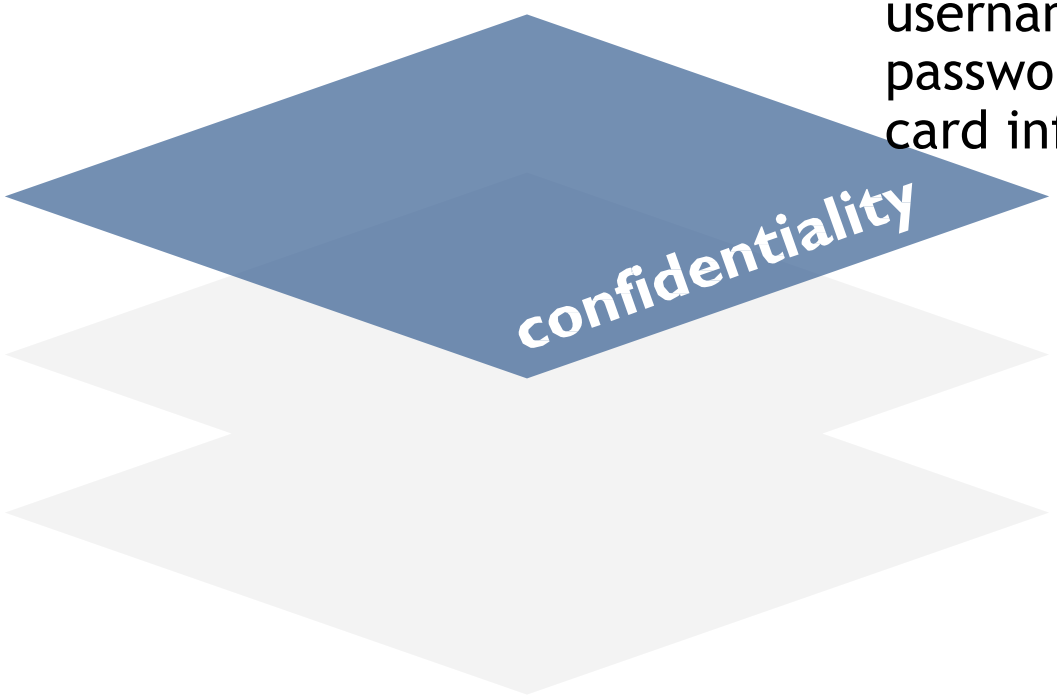


- ***Confidentiality*** – restrict access to authorized individuals
- ***Integrity*** – data has not been altered in an unauthorized manner
- ***Availability*** – information can be accessed and modified by authorized individuals in an appropriate timeframe

CIA Triad

Confidentiality

Example:
Criminal steals customers' usernames, passwords, or credit card information

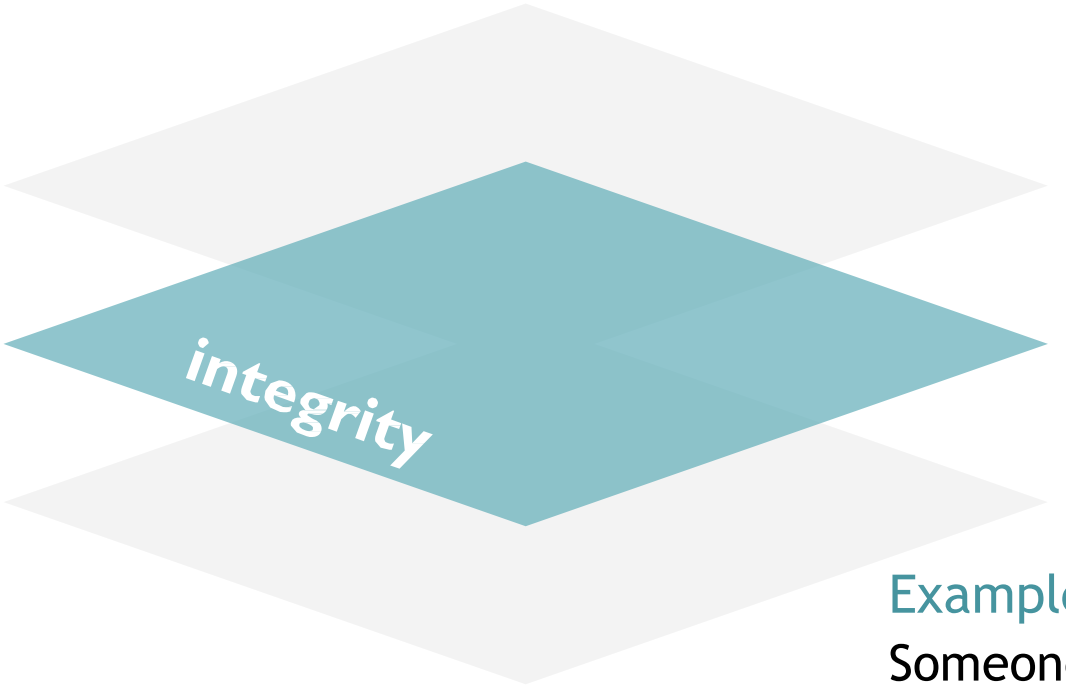


Protecting information from unauthorized access and disclosure

CIA Triad

Integrity

Protecting information from unauthorized modification

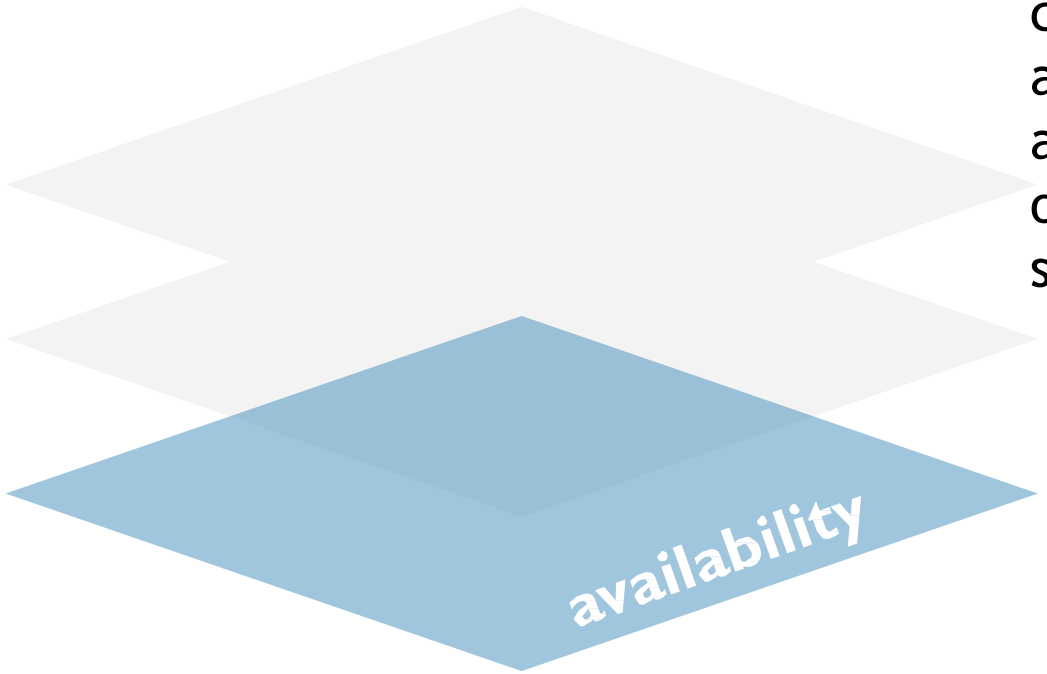


Example:
Someone alters payroll information or a proposed product design

CIA Triad

Availability

Preventing disruption in how information is accessed



Example:

Your customers are unable to access your online services

Threats and Vulnerabilities

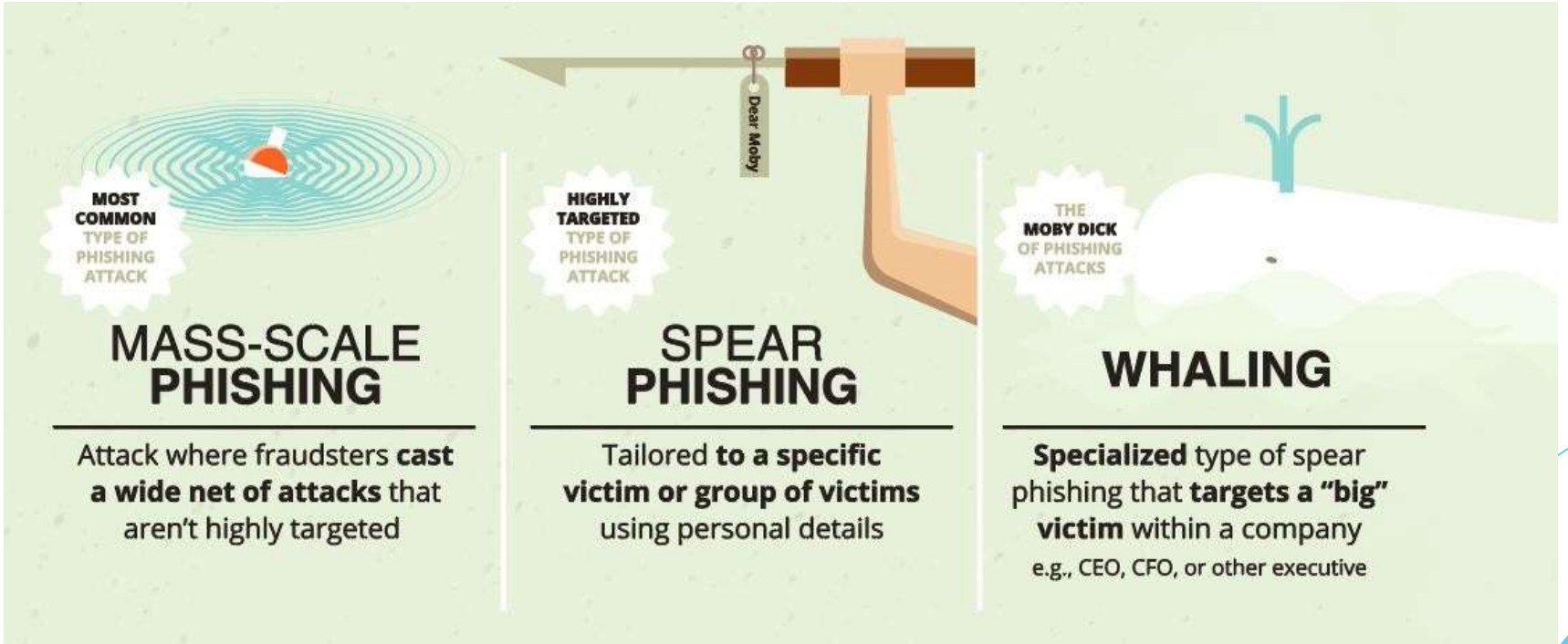
- What are we protecting our and our stakeholders information from?
- **Threats:** Any circumstances or events that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable
- **Vulnerabilities:** Weakness in an information system or its components that could be exploited.

WHAT KINDS OF THREATS ARE THERE?

- Phishing and Spear-phishing Attacks
- Social Engineering Scams
- Common Malware and Ransomware
- Business Email Compromise
- Fake websites that steal data or infect devices
- And much more

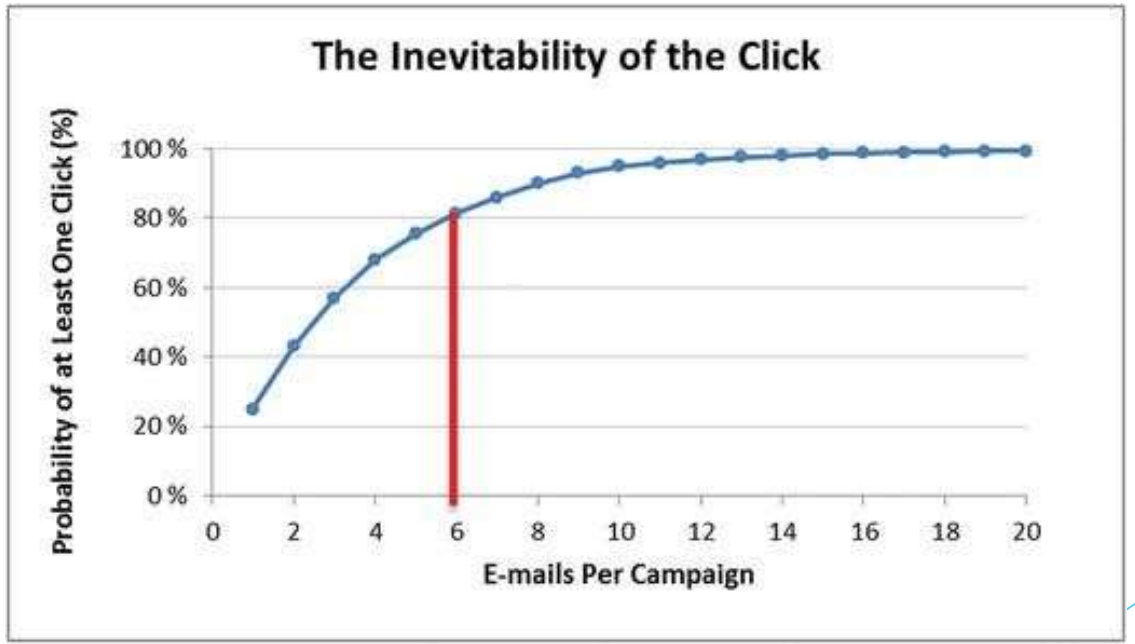
Phishing

- Phishing refers to the practice of creating fake emails or SMS that appear to come from someone you trust, such as: Bank, Credit Card Company, Popular Websites
- The email/SMS will ask you to “confirm your account details or your vendor’s account details”, and then direct you to a website that looks just like the real website, but whose sole purpose is for steal information.
- Of course, if you enter your information, a cybercriminal could use it to steal your identity and possible make fraudulent purchases with your money.

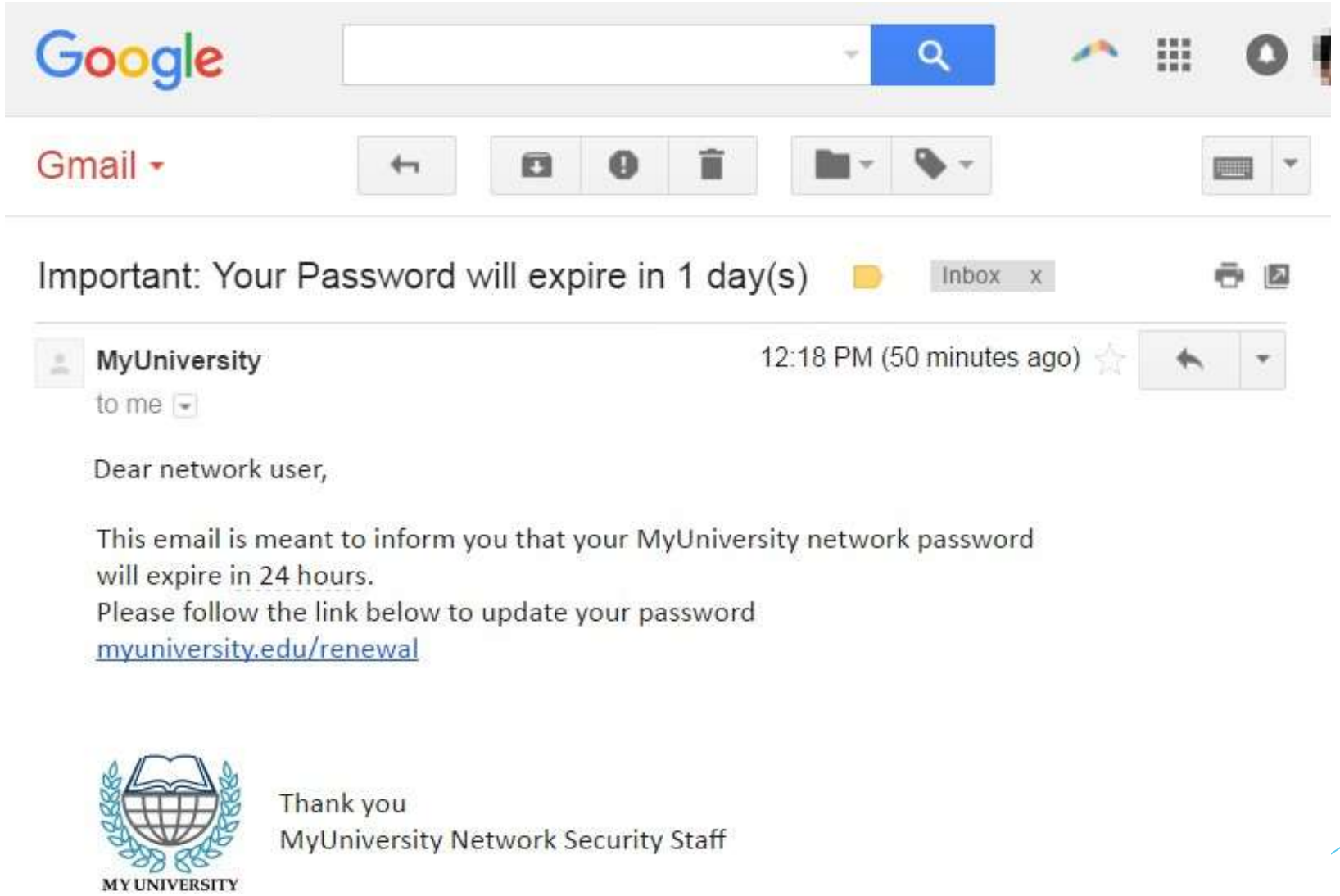


Phishing Statistics

- Verizon DBIR 2020: Phishing is the biggest cyber threat for SMBs, accounting for 30% of SMB breaches
- KnowBe4: 37.9% of Untrained Users Fail Phishing Tests
- 84% of SMBs are targeted by Phishing attacks
- A new Phishing site launches every 20 seconds
- 74% of all Phishing websites use HTTPS
- 94% of Malware is delivered via email



Example of Phishing



Social Engineering

- When attempting to steal information or a person's identity, a hacker will often try to trick you into giving out sensitive information rather than breaking into your computer.
- Social Engineering can happen:
- Over the phone
- By text message
- Instant message
- Email

Malware

- Malware = “malicious software”
- Malware is any kind of unwanted software that is installed without your consent on your computer and other digital devices.
- Viruses, Worms, Trojan horses, Bombs, Spyware, Adware, Ransomware are subgroups of malware.

Viruses

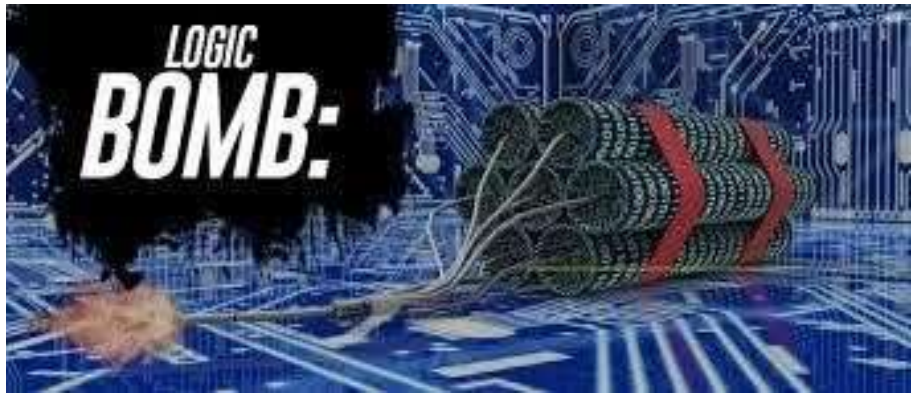
- A virus tries to infect a carrier, which in turn relies on the carrier to spread the virus around.
- A computer virus is a program that can replicate itself and spread from one computer to another.

Viruses cont.

- **Direct infection**: virus can infect files every time a user opens that specific infected program, document or file.
- **Fast Infection**: is when a virus infects any file that is accessed by the program that is infected.
- **Slow infection**: is when the virus infects any new or modified program, file or document.
- Great way to trick a antivirus program!
- Sparse Infection: is the process of randomly infecting files, etc. on the computer.
- RAM-resident infection: is when the infection buries itself in your Computer's Random Access Memory.

Bombs

- Logic Bombs: is programming code that is designed to execute or explode when a certain condition is reached.
- Most the time it goes off when a certain time is reached or a program fails to execute. But it these bombs wait for a triggered event to happen.
- Most common use of this is in the financial/business world.
- Most IT employees call this the disgruntled employee syndrome.



Trojans

- Trojan horse: is a program or software designed to look like a useful or legitimate file.
- Once the program is installed and opened it steals information or deletes data.
- Trojan horses compared to other types of malware is that it usually runs only once and then is done functioning.
- Some create back-door effects
- Another distribution of Trojans is by infecting a server that hosts websites.
- Downfall of Trojans: very reliant on the user

Worms

- Worms and viruses get interchanged commonly in the media.
- In reality a worm is more dangerous than a virus.
- User Propagation vs. Self Propagation
- Worm is designed to replicate itself and disperse throughout the user's network.
- Email Worms and Internet Worms are the two most common worm.

Email Worm

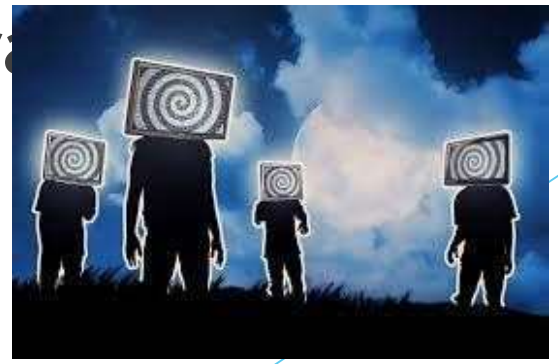
- Email worm goes into a user's contact/address book and chooses every user in that contact list.
- It then copies itself and puts itself into an attachment; then the user will open the attachment and the process will start over again!
- Example: I LOVE YOU WORM

Internet Worms

- An Internet Worm is designed to be conspicuous to the user.
- The worms scans the computer for open internet ports that the worm can download itself into the computer.
- Once inside the computer the worms scans the internet to infect more computers.

Zombie & Botnet

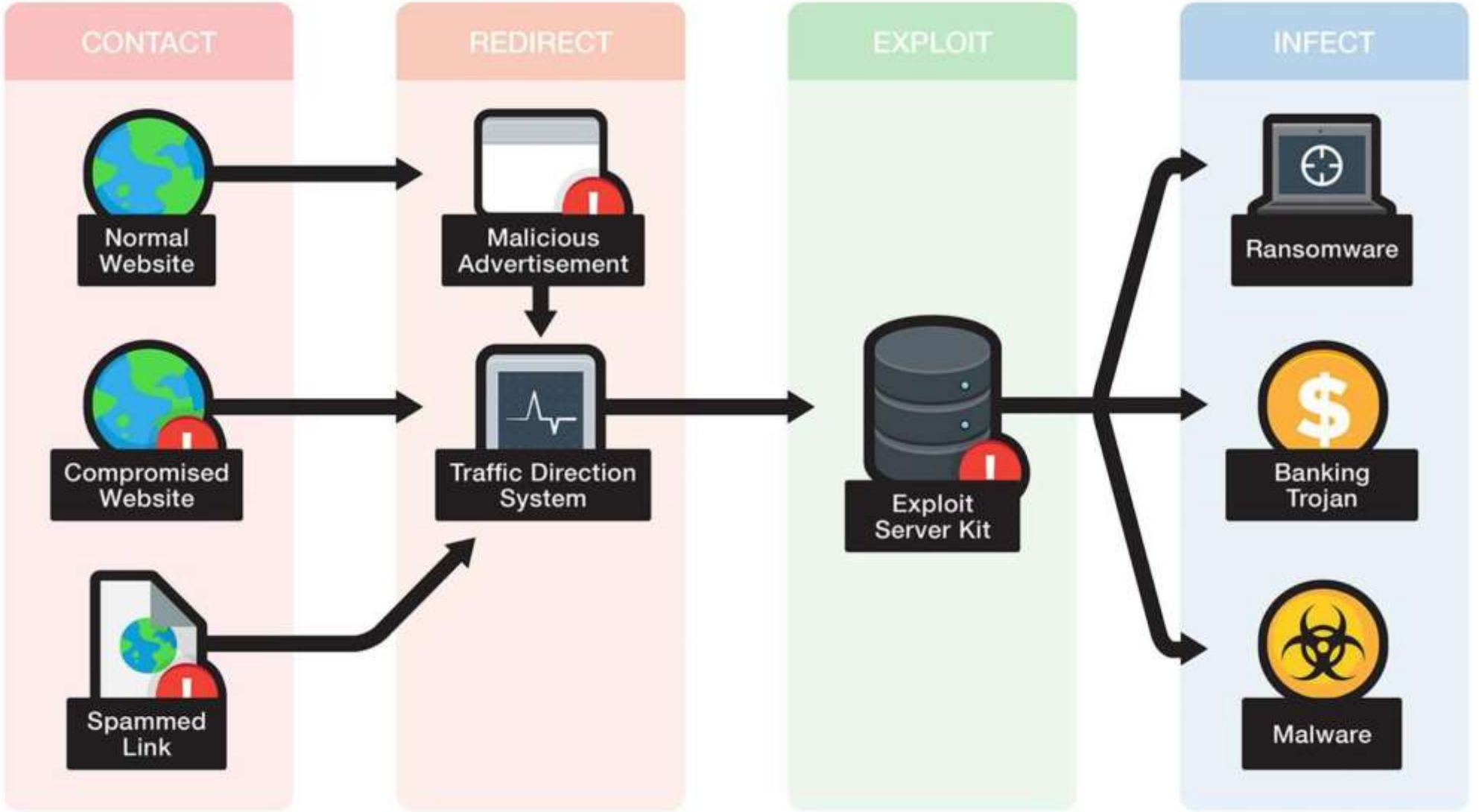
- Secretly takes over another networked computer by exploiting software flows
- Builds the compromised computers into a zombie network or botnet
- a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- Uses it to indirectly launch attacks
- E.g., DDoS, phishing, spamming, cra



Adware and Spyware

- Adware is a type of malware designed to display advertisements in the user's software.
- They can be designed to be harmless or harmful; the adware gathers information on what the user searches the World Wide Web for.
- With this gathered information it displays ads corresponding to information collected.
- Spyware is like adware it spies on the user to see what information it can collect off the user's computer to display pop ads on the user's computer.
- Spyware unlike adware likes to use memory from programs running in the background of the computer to keep close watch on the user.
- This most often clogs up the computer causing the program or computer to slow down and become un-functional.

Exploit Kit


CONTACT
REDIRECT
EXPLOIT
INFECT
Normal Website
Compromised Website
Spammed Link
Malicious Advertisement
Traffic Direction System
Exploit Server Kit
Ransomware
Banking Trojan
Malware

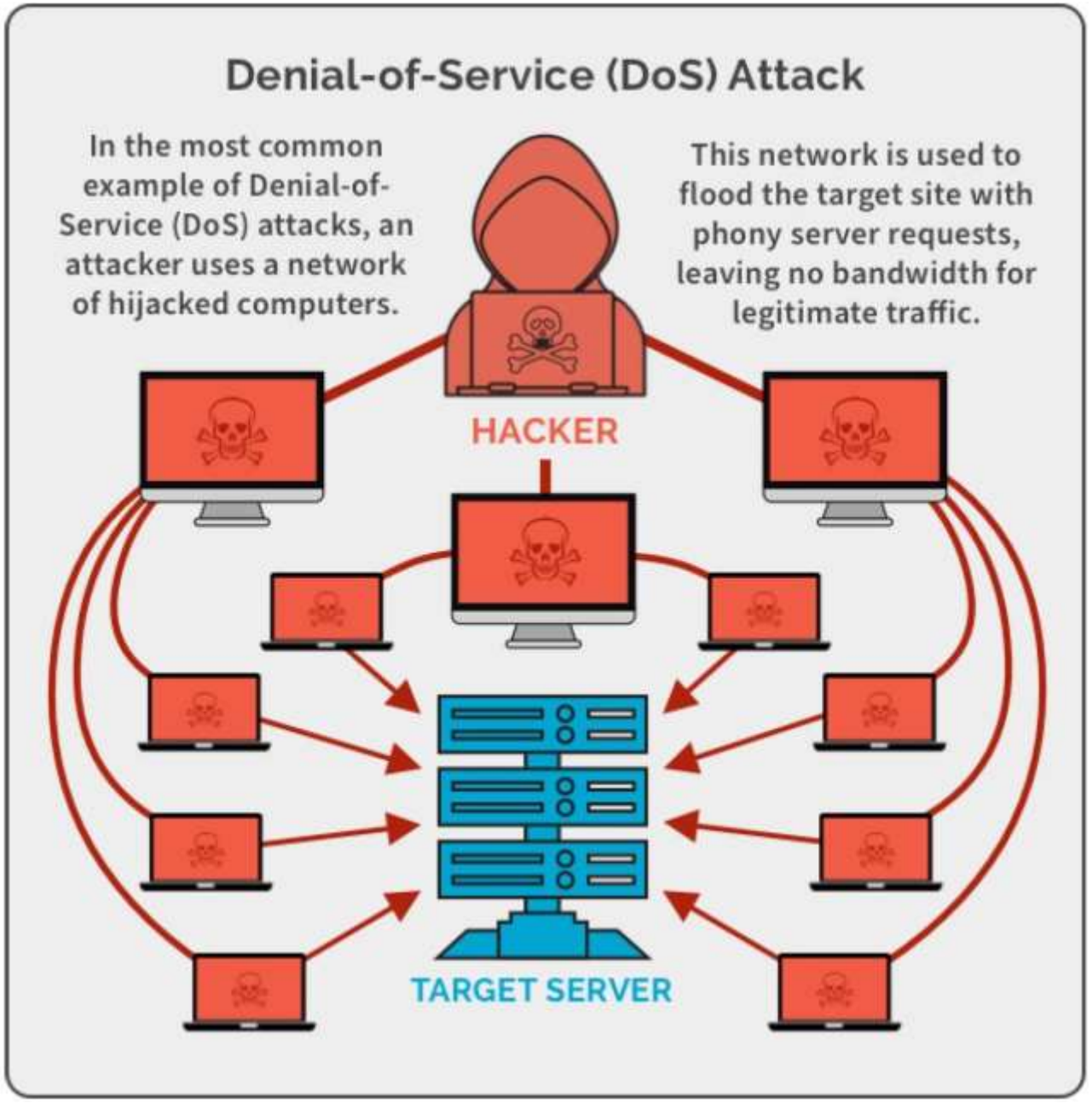
Identity Theft

- Identity Theft
  - Impersonation by private information
    - Thief can 'become' the victim
- Reported incidents rising
- Methods of stealing information
  - Shoulder surfing
  - Snagging
  - Dumpster diving
  - Social engineering
  - High-tech methods

Identity Theft

- Loss of privacy
  - Personal information is stored electronically
  - Purchases are stored in a database
    - Data is sold to other companies
  - Public records on the Internet
  - Internet use is monitored and logged
  - None of these techniques are illegal

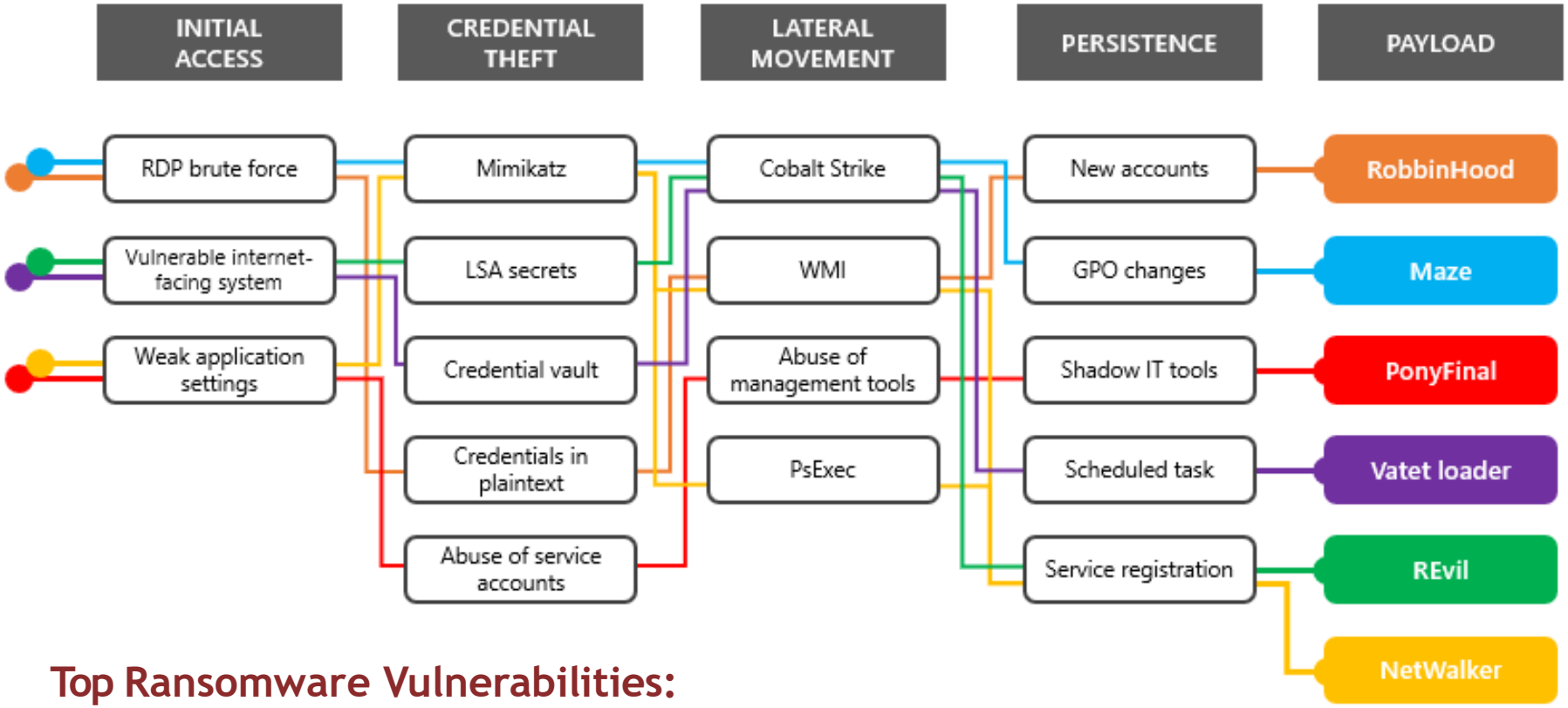
Denial of Service Attack



Ransomware

- Ransomware is a type of malware that restricts your access to systems and files, typically by encryption and then demands a ransom to restore access.
- Often, systems are infected by ransomware through a link in a malicious email. When the user clicks the link, the ransomware is downloaded to the user's computer, smartphone or other device. Ransomware may spread through connected networks.

Ransomware



Top Ransomware Vulnerabilities:

- RDP or Virtual Desktop endpoints without MFA
- Citrix ADC systems affected by CVE-2019-19781
- Pulse Secure VPN systems affected by CVE-2019-11510
- Microsoft SharePoint servers affected by CVE-2019-0604
- Microsoft Exchange servers affected by CVE-2020-0688
- Zoho ManageEngine systems affected by CVE-2020-10189

https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

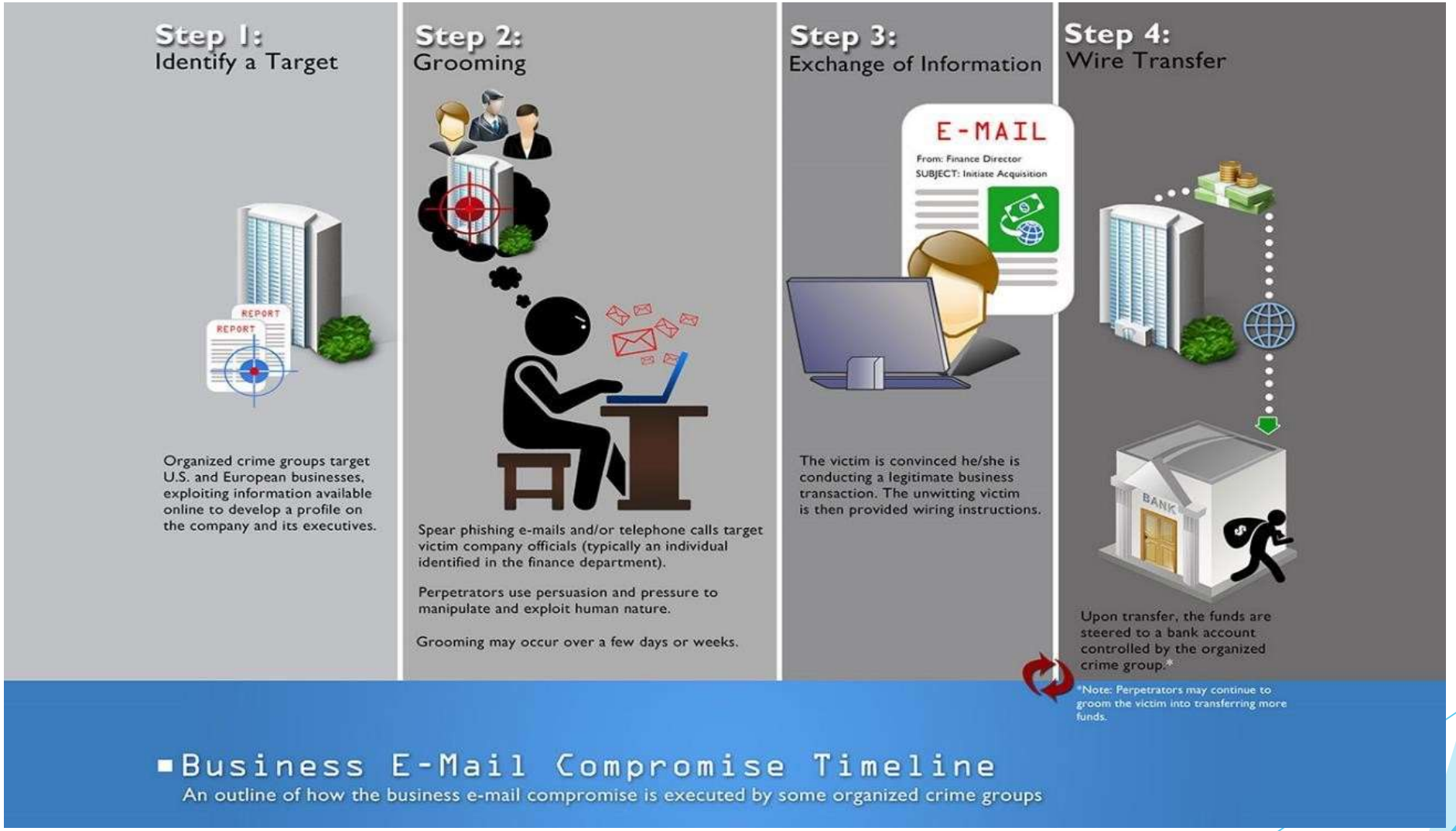
Ransomware Controls

- Weapons-Grade Data Backups
- Religious Patch Management
- Plan to Fail Well (Incident Response Plan)
  - Know who to call!
- Training and Testing Your People
- Don’t Open that Email Link/Attachment

Business/Official Email Compromise

- BEC is a big problem for you and your organization:
- Your email is compromised.
- Another employee of your organization is compromised
- Almost always, these emails fall into 2 categories:
  1. Downloading and spreading additional malware automatically
  2. Urging the customer to perform a financial transaction immediately
- Tips and Tricks to share with customers:
  - BEC made up half of cyber-crime losses in 2019; $75K per scam
  - Standard phishing email awareness – don't click links or download attachments
  - Pay attention to the email address
  - Enable MFA for business email accounts

Business Email Compromise



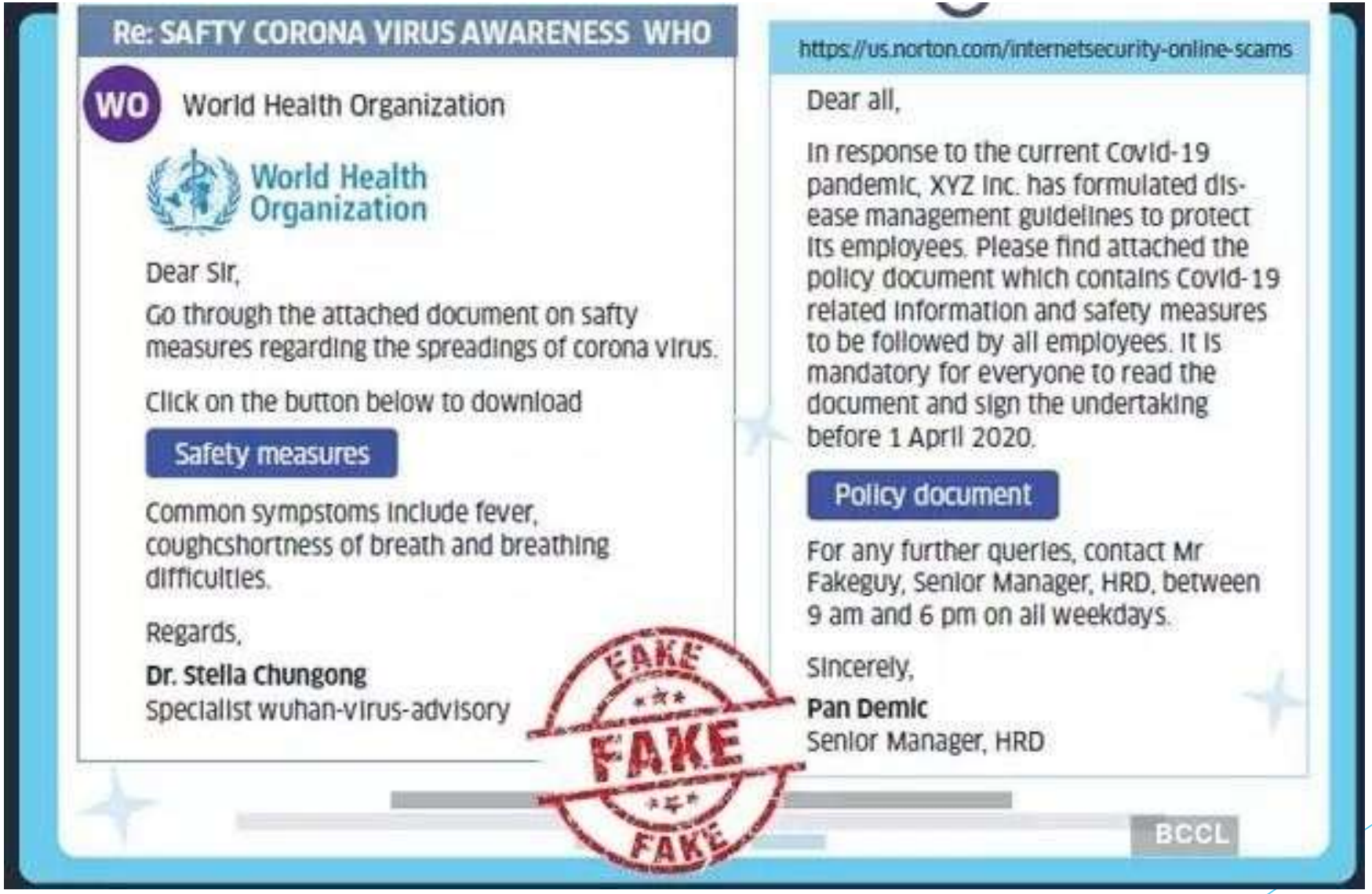
Business Email Compromise

COVID-19 Cyber Threats

COVID-19 Cyber Threats

COVID-19 Cyber Threats

COVID-19 Cyber Threats



COVID-19 Cyber Threats

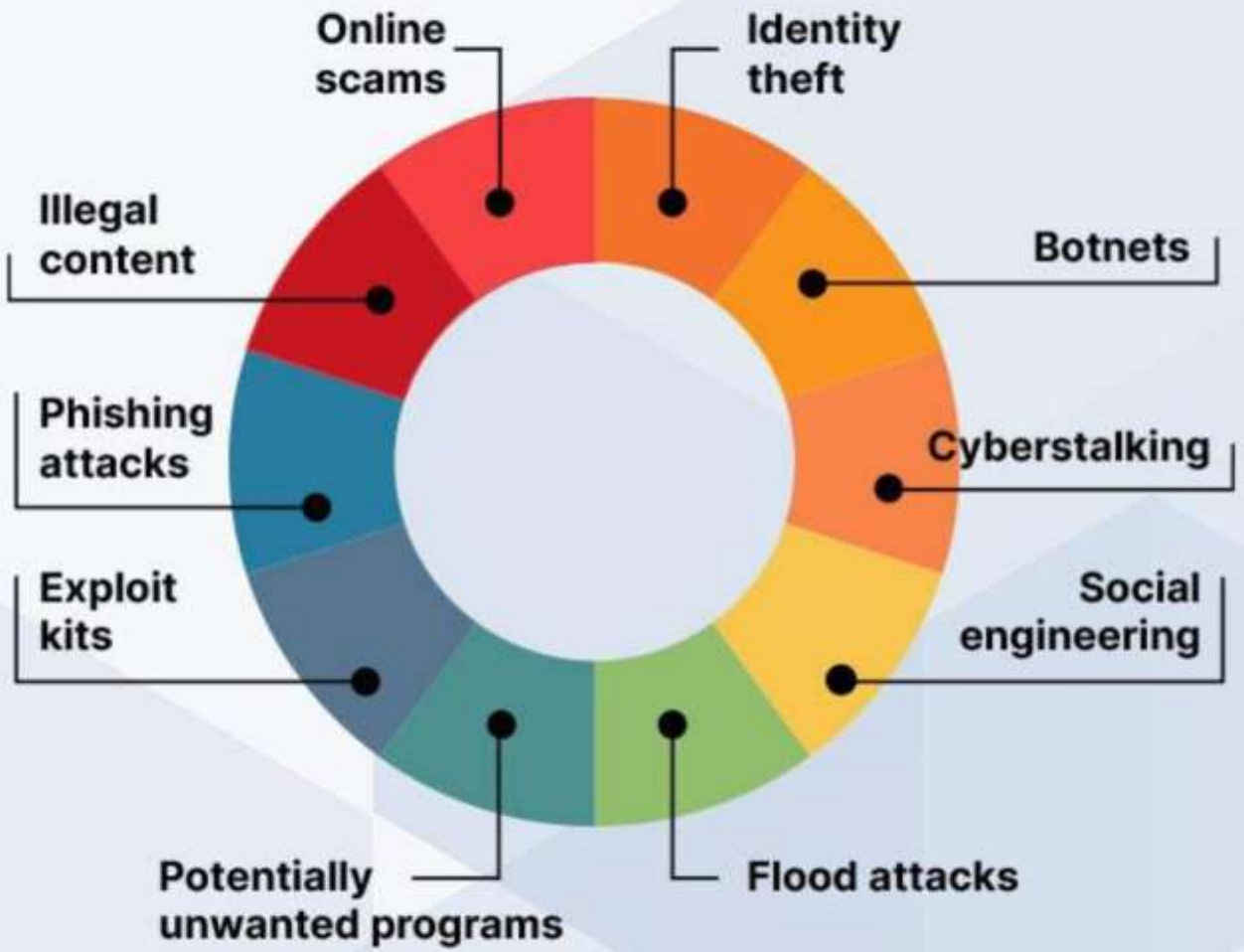
- Google: 18+ Million COVID-19 emails in just the one week, in addition to 240M daily COVID-19 spam messages
- Phishing up 667% right now
- FBI IC3: 4x complaints per day (1K before COVID-19, now 3k-4k per day)
- 148% spike in ransomware attacks due to COVID-19
- 30%-40% increase in attacker interest relating to RDP (as measured by Shodan)
- 26% increase in e-comm web skimming in March
- Healthcare, Financial Services, Medical Suppliers and Manufacturing, Government and Media Outlets all seeing a large increase in cyber threats

Cyber Crime

Cyber Crime is a generic term that refers to all criminal activities done using the medium of communication devices, computers, mobile phones, tablets etc. It can be categorized in three ways:

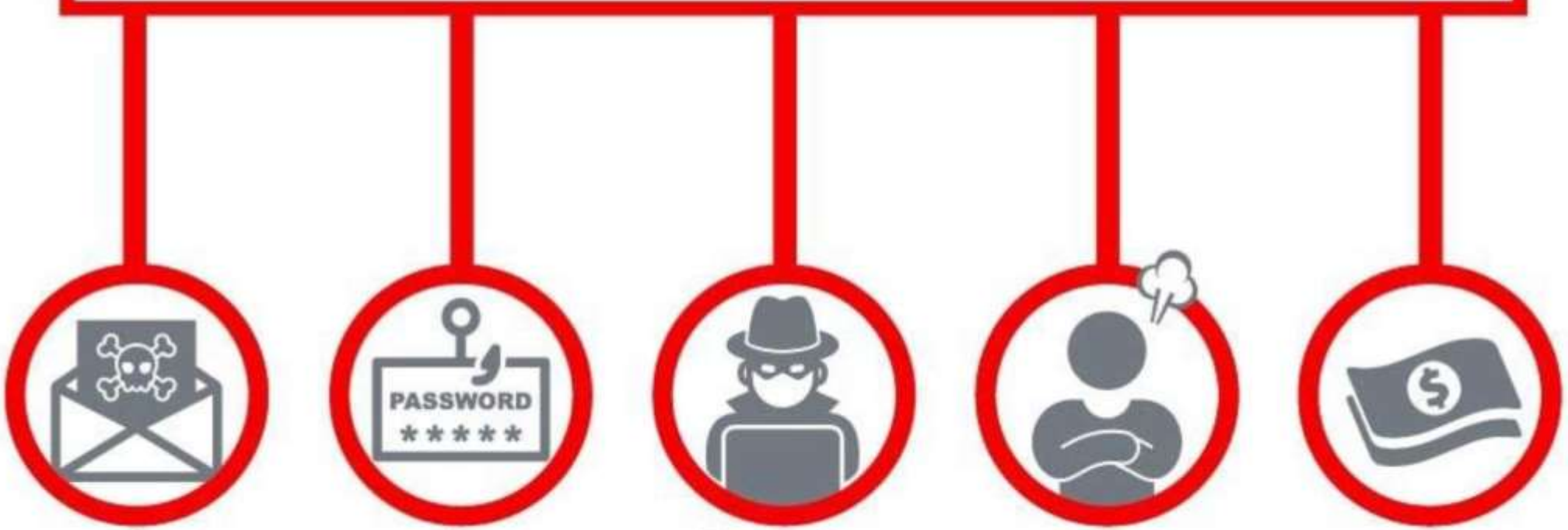
- **The computer as a target** – attacking the computers of others.
- **The computer as a weapon**- Using a computer to commit "traditional crime" that we see in the physical world.
- **The computer as an accessory**- Using a computer as a "fancy filing cabinet" to store illegal or stolen information.

Types of Cybercrime



SecurityTrails

5 Types of Cyber Criminals

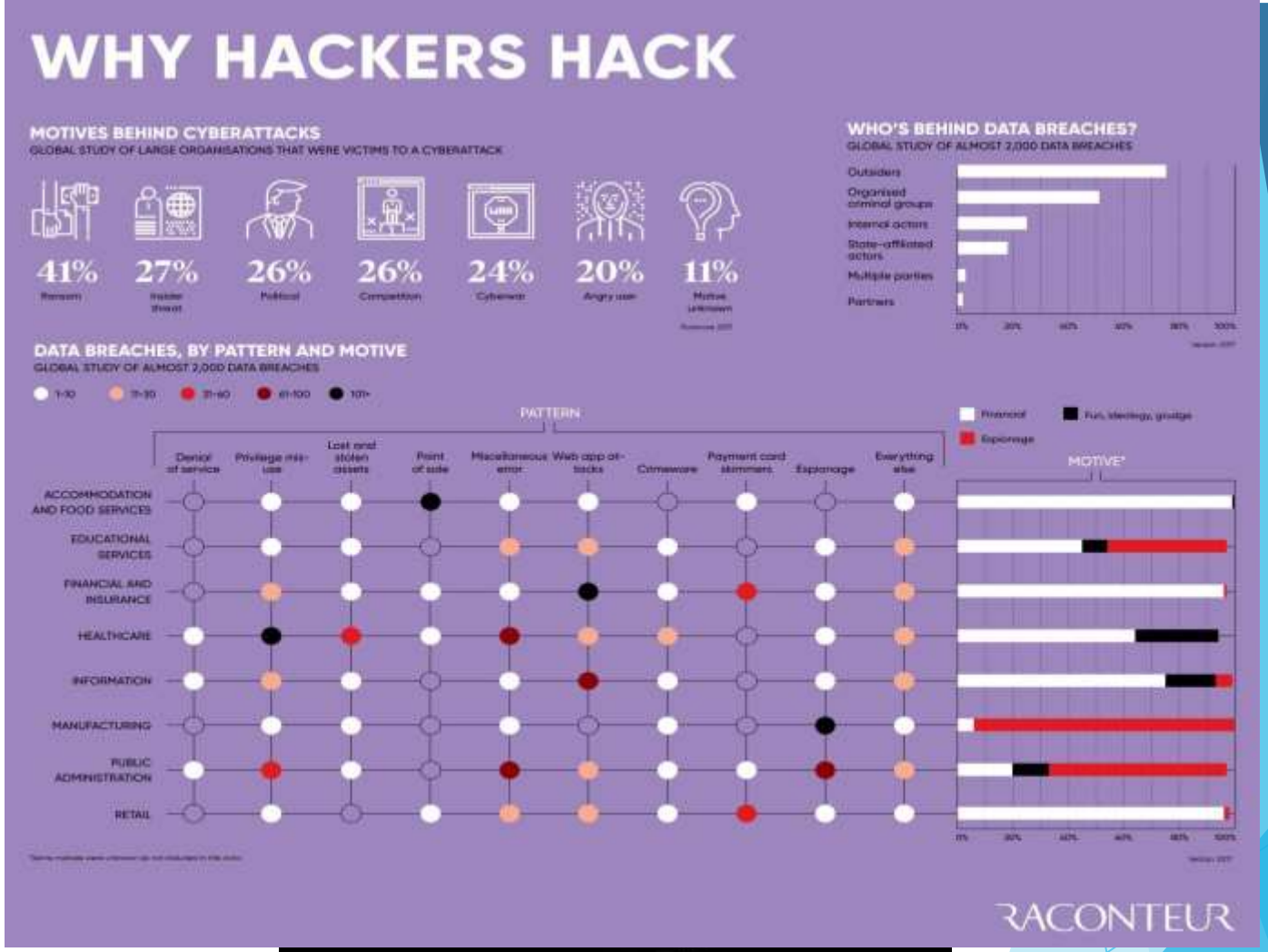


How do you look like to Bad guys?

66.233.160.64

Hacking

- Financial (theft, fraud, blackmail)
- Political/State (state level/military)
- Fame/Kudos (fun/status)
- Hacktivism (cause)
- Pen Testers (legal hacking)
- Police
- Insider
- Business



Which hat you want to wear?

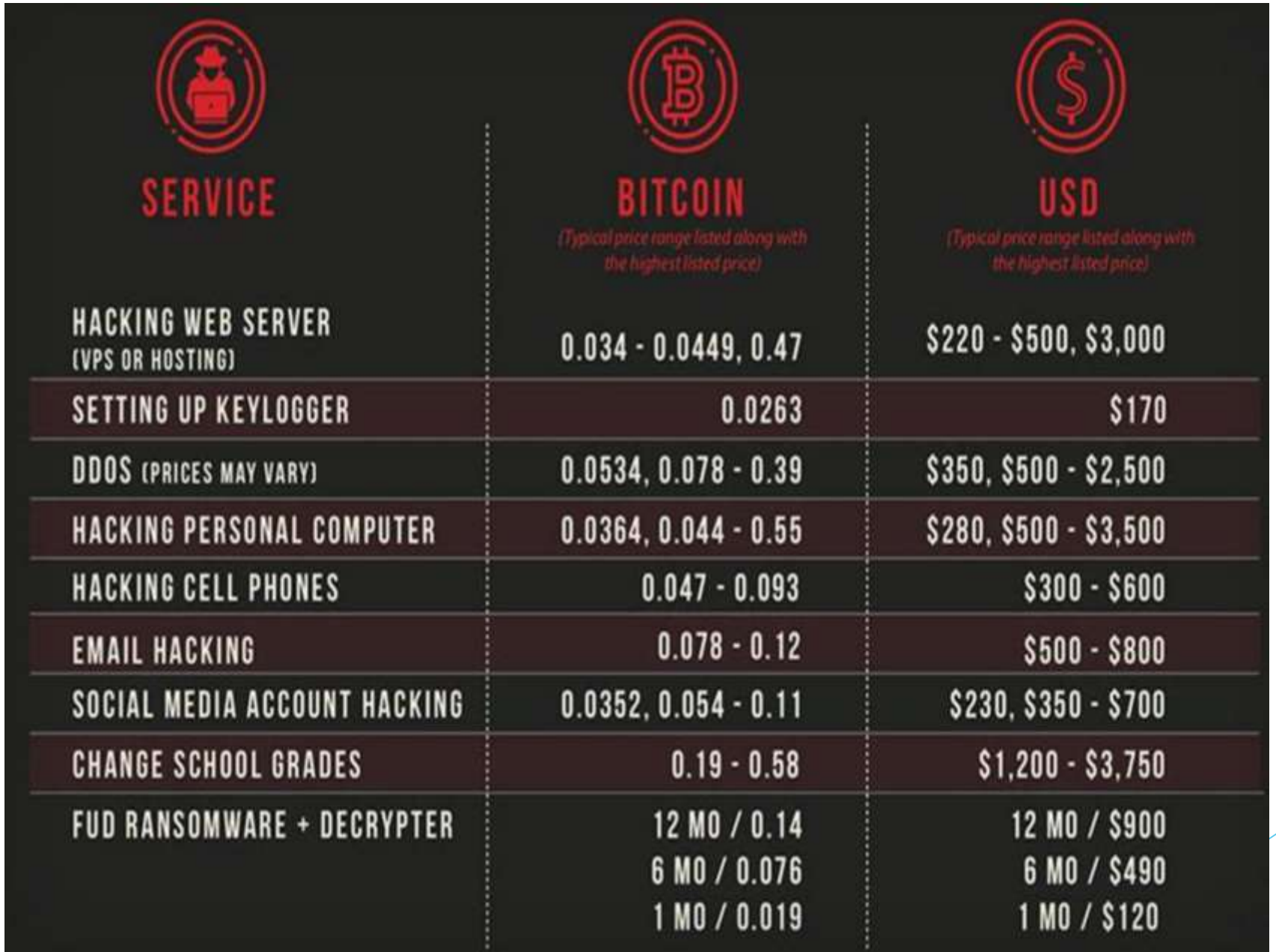
Ethical Hacking

System Hacking

- System hacking is a vast subject that consists of hacking the different software-based technological systems such as laptops, desktops, etc.
- **System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information.**
  - Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.
- Hackers generally use viruses, malware, Trojans, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, or port vulnerabilities to access any victim's system.

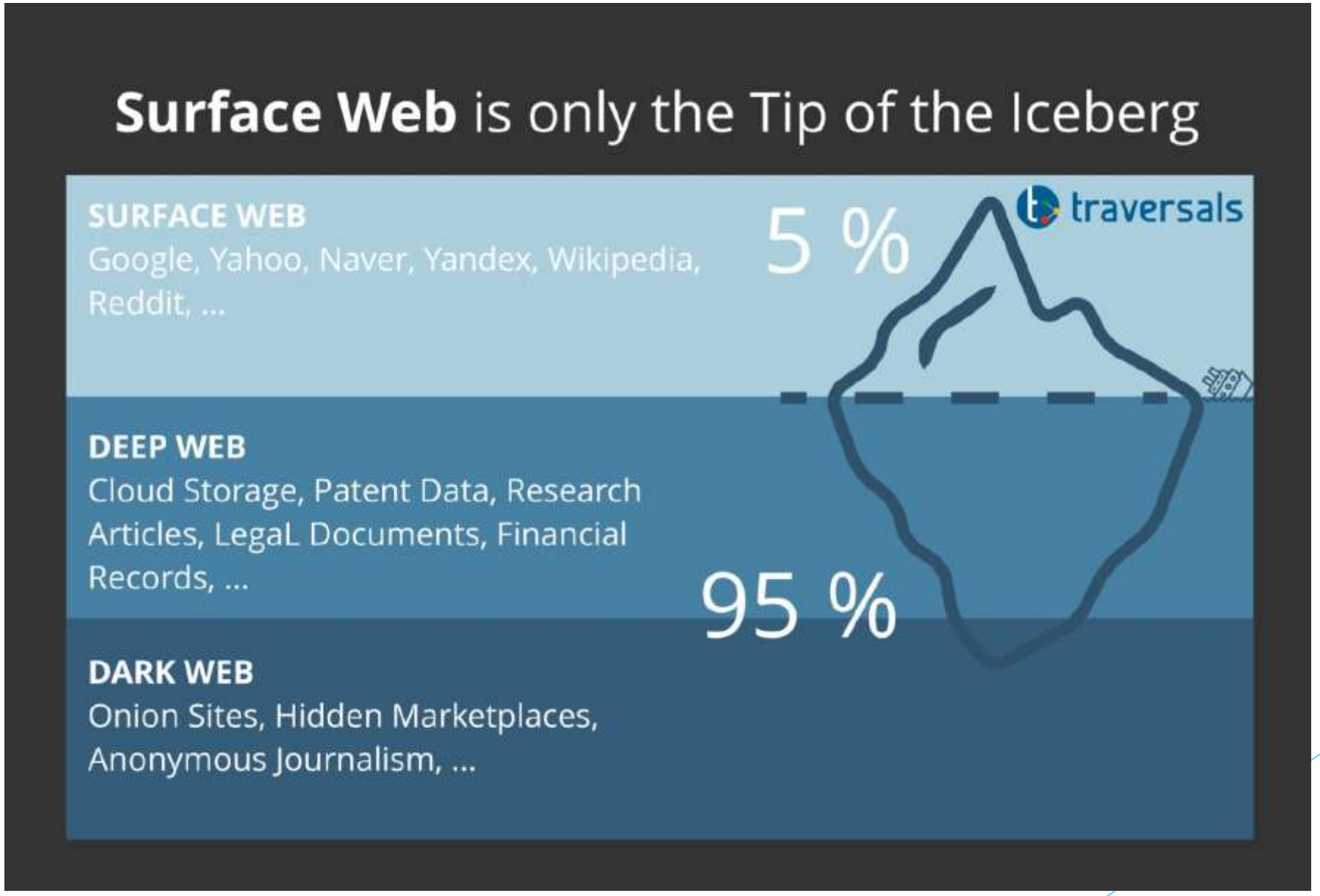
Cybercrime as a Service

Cybercrime as a Service



SERVICE	BITCOIN (Typical price range listed along with the highest listed price)	USD (Typical price range listed along with the highest listed price)
HACKING WEB SERVER (VPS OR HOSTING)	0.034 - 0.0449, 0.47	$220 - $500, $3,000
SETTING UP KEYLOGGER	0.0263	$170
DDOS (PRICES MAY VARY)	0.0534, 0.078 - 0.39	$350, $500 - $2,500
HACKING PERSONAL COMPUTER	0.0364, 0.044 - 0.55	$280, $500 - $3,500
HACKING CELL PHONES	0.047 - 0.093	$300 - $600
EMAIL HACKING	0.078 - 0.12	$500 - $800
SOCIAL MEDIA ACCOUNT HACKING	0.0352, 0.054 - 0.11	$230, $350 - $700
CHANGE SCHOOL GRADES	0.19 - 0.58	$1,200 - $3,750
FUD RANSOMWARE + DECRYPTER	12 MO / 0.14 6 MO / 0.076 1 MO / 0.019	12 MO / $900 6 MO / $490 1 MO / $120

Web, Deep Web & Dark Web



Global Cyber Security Trends – The next wave

Recent studies reveal three major findings:

- **Growing threat to national security** - web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organized operations aimed at not only financial, but also political or technical gain
- **Increasing threat to online services** – affecting individuals and industry because of growth of sophistication of attack techniques
- **Emergence of a sophisticated market for software flaws** – that can be used to carry out espionage and attacks on Govt. and Critical information infrastructure. Findings indicate a blurred line between legal and illegal sales of software vulnerabilities

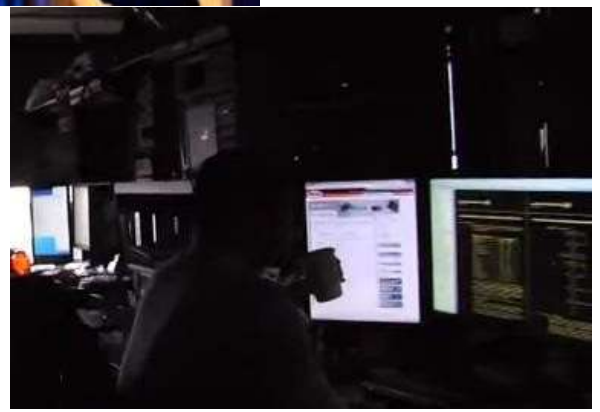
Mischievous activities in cyber space have expanded from novice geeks to organized criminal gangs that are going Hi-tech

Attacks today are AUTOMATED!

It’s not some dude sitting at his hacker desk all day typing out ping commands to IP addresses via the command prompt manually…

What does a Cyber Security Professional look like?

What does a Cyber Security Professional look like?



In reality…

Eugene Kaspersky, CEO Kaspersky Labs, £1.1bn

David Ulevitch, Founder OpenDNS

Katie Moussouris, Microsoft Bug Bounty creator

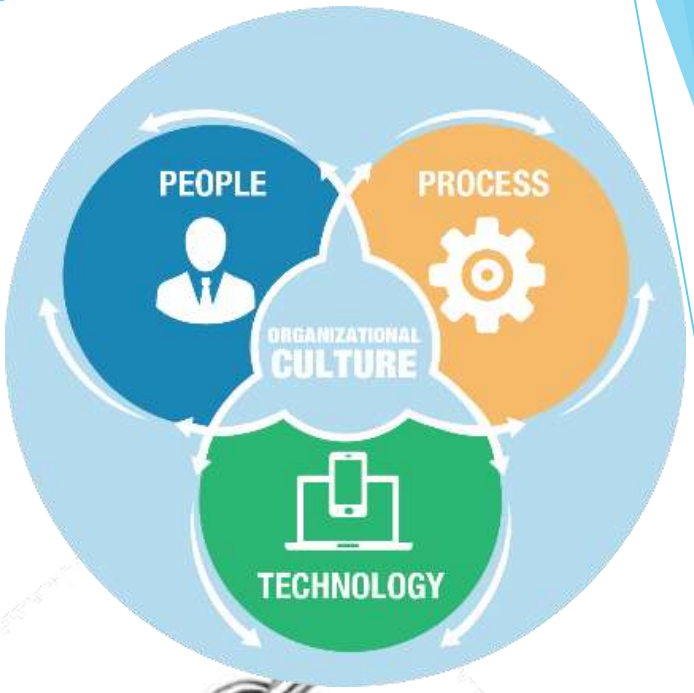
James Lyne, CTO, SANS

Erin Jacobs, CSO at UCB Financial Services

Dr Laura Toogood, MD Digitalis Reputation

How We Protect Information?

- People
  - Training, education, awareness, repetition
- Process
  - Governance, oversight, policy, reporting
- Technology
  - Firewalls, IDS/ISP, SIEM, anti-malware
  - Strong passwords, Logging/monitoring
- **Which is the weakest link?**



Social Engineering Best Practices

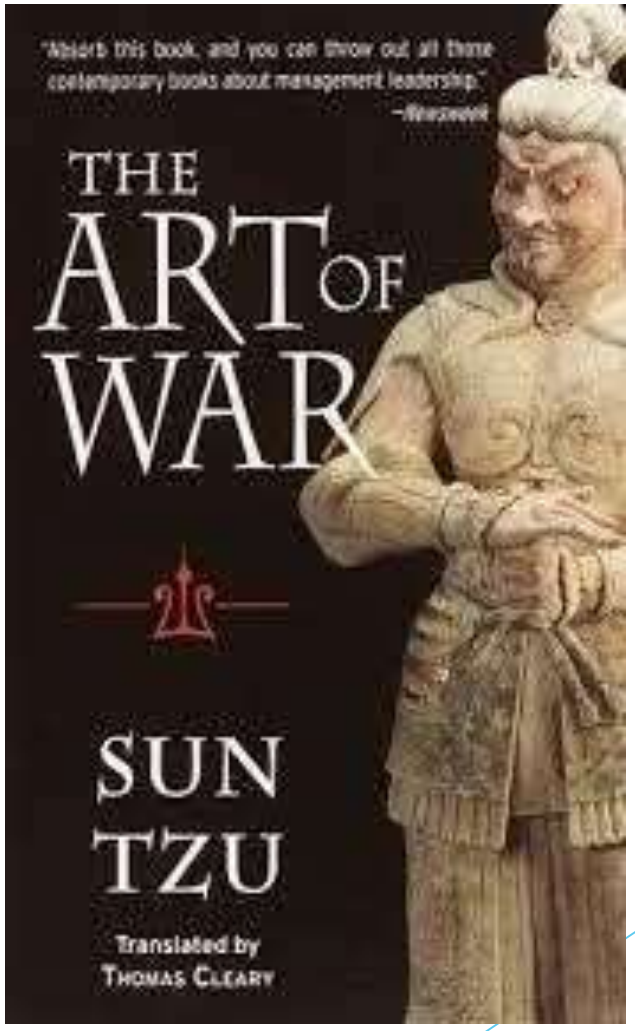
- USE YOUR **SECURITY SPIDER SENSE**!
- ALWAYS validate requests for information if you're not **100000%** sure
  - Call a number YOU know
  - Google it…
- **ALWAYS ASK QUESTIONS!**
  - Is this who I think it is FOR SURE?
  - Did someone mention this to me personally, or was it discussed at a staff meeting?
  - Is this the FIRST I'm hearing about this?

BEC Best Practices

- Avoid using free web-based email for business
- Not only less-professional, but easier to hack, typosquat, or spoof
- Domains and email addresses are cheap, especially compared to BEC
- Register similar domains to yours to prevent typosquatting e.g. delaplex.com vs. delapelx.com
- Be careful about the information you share on your website or Social Media (LinkedIn, Facebook) about job duties or positions, especially for positions with transactional or purchasing authority
- Think through Out of Office email responders

Sun Tzu on the Art of War

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
- If you know neither the enemy nor yourself, you will succumb in every battle.

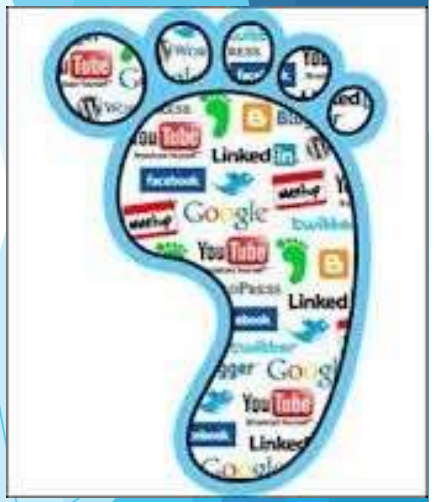


WHAT IS FOOTPRINTING?

- Definition: the gathering of information about a potential system or network (the fine art of gathering target information)
- a.k.a. fingerprinting
- Attacker's point of view
- Identify potential target systems
- Identify which types of attacks may be useful on target systems
- Defender's point of view
- Know available tools
- May be able to tell if system is being footprinted, be more prepared for possible attack
- Vulnerability analysis: know what information you're giving away, what weaknesses you have

WHAT IS FOOTPRINTING?

- System (Local or Remote)
- IP Address, Name and Domain
- Operating System
- Type (Windows, Linux, Solaris, Mac)
- Version (XP/Vista/7/10, Redhat, Fedora, SuSe, Ubuntu, OS X)
- Usernames (and their passwords)
- File structure
- Open Ports (what services/programs are running on the system)
- Networks / Enterprises
- System information for all hosts
- Network topology
- Gateways
- Firewalls
- Overall topology
- Network traffic information
- Specialized servers
- Web, Database, FTP, Email, etc.
- Social Media



Vulnerability Scanner

- Functions of Vulnerability Scanner are far different from firewall or intrusion detection system.
- Vulnerability scanning tools helps you in protecting your organization from any kind of security risks or threats by scanning with deep inspection of endpoints to ensure that they are configured securely and correctly.
- The prime aim of running a vulnerability scanner is to identify the devices that are open for vulnerabilities.

Types of Vulnerability Scanner

- Port scanner
- Network vulnerability scanner
- Web application security scanner
- Database security scanner.
- Host based vulnerability scanner
- ERP security scanner.
- Single vulnerability tests.

Virus Detection

- Simple Anti-virus Scanners
  - Look for signatures (fragments of known virus code)
  - Heuristics for recognizing code associated with viruses
    - Example: polymorphic viruses often use decryption loops
  - Integrity checking to detect file modifications
  - Keep track of file sizes, checksums, keyed HMACs of contents
- Generic decryption and emulation
  - Emulate CPU execution for a few hundred instructions, recognize known virus body after it has been decrypted
  - Does not work very well against viruses with mutating bodies and viruses

not located near beginning of infected executable

Virus Detection

- Simple Anti-virus Scanners
  - Look for signatures (fragments of known virus code)
  - Heuristics for recognizing code associated with viruses
    - Example: polymorphic viruses often use decryption loops
  - Integrity checking to detect file modifications
  - Keep track of file sizes, checksums, keyed HMACs of contents
- Generic decryption and emulation
  - Emulate CPU execution for a few hundred instructions, recognize known virus body after it has been decrypted
  - Does not work very well against viruses with mutating bodies and viruses

not located near beginning of infected executable

Cyber Security and Privacy Starts and Ends with Us!

Commit to a disciplined practice of information security and continue to refresh yourself so you don't become a point of vulnerability in our security defenses.

Summary

- Cybersecurity will require a significant workforce with deep domain knowledge.
- Almost everything is hooked up to the internet in some sort of form.
- Recent events have widened the eyes of many security experts.
- The ability to gain access to high security organizations, infrastructures or mainframes has frightened many people.
- Could one click of the mouse start World War III?

Thank you!