Employee Guide to Cybersecurity and Cyber Threats

Author: Emily Y. Feliciano Cruz
Advisor: Jeffrey Duffany, Ph.D
Electrical and Computer Engineering and Computer Science Department

Abstract

Cybersecurity is a growing concern for companies and workers due to the growing threats posed by technology. The Covid-19 pandemic has highlighted the need for protective shields, with malware being a major threat. WannaCry, a $4 billion attack, cost businesses up to $4 billion.[1] While technical solutions like spam filters protect users, human error remains a risk factor that needs to be addressed to improve security across various systems and communications.
EFC Secure is committed to a modern approach to cybersecurity to prevent unauthorized access, disclosure, and damage to electronic information and critical infrastructure. This manual provides guidance on employees' roles and responsibilities to help prevent incidents that put at risk the information handled by EFC Secure and its customers. EFC Secure prioritizes information security, ensuring effective controls for customers and employees. They educate new and existing employees on their roles and responsibilities for information protection and cybersecurity matters.

Introduction

"The security of computer systems is such a sensitive issue today that even the companies that offer it must keep theirs under continuous evaluation. In addition, security testing and vulnerability remediation should be implemented by organizations from the beginning, to avoid falling victim to devastating attacks," said Mauricio Gómez, co-founder of Fluid Attacks, a company dedicated to ethical hacking in enterprise computer systems.
A cyberattack is an attack that is mounted against our digital equipment and services through cyberspace. This metaphorical place became a crucial element in understanding how digital weapons can reach us.
What is real is the intent of the attackers and the potential impact. While most attacks are a simple nuisance, some are serious and can be life-threatening. Cybersecurity threats can be divided into three main categories, according to intent: Financial Gain, Digital Disruption and Espionage (includes corporate, state, and patent espionage). Virtually all cyber threats can be divided into those three categories.

Problem

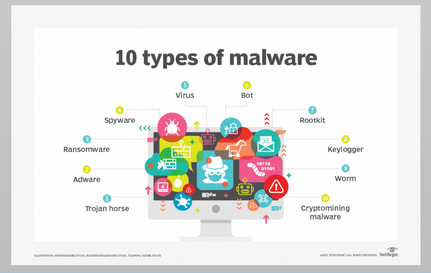
Cybersecurity extends to networks, applications, information, and operational processes. Elements that are necessarily executed for the continuity of a business.
Currently, the implementation of digital security measures is since there are more connected devices than people, and attackers are becoming more and more creative.
It is essential to learn how to detect possible cyber threats as a user, because today almost all companies develop in the digital field. For this reason, it is important to control their security and know how to act against them to avoid being potential victims of fraud.
Most of the drawbacks associated with cybersecurity are caused by human error. That's why businesses need to worry about their employees first and cybercriminals second. They should also prioritize having an IT security strategy in place that reduces the chances that attacks will be consciously caused by current and former employees.
When it comes to attack techniques, hackers have an abundance of options. The eight most common types are: Malware, Phishing, Ransomware, Business email Compromised (BEC), Man in the Middle (MitM), DDoS Attack, Piggybacking and Baiting attack.

Eight Most Common Types of Cyber Threats:

Malware

Malware is a type of software or application that intentionally damages a device, such as a computer or mobile phone, causing disruption, leakage of private information, unauthorized access, deprivation of access, or unknowingly interfering with a user's computer security and privacy. It comes from the English word "malicious software" and is derived from the union of the word's malicious software.[2]

Types of Malwares



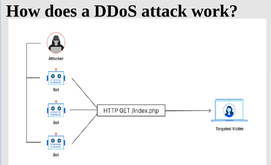
Symptoms of being affected by Malwares
Some of the most common symptoms include:
- Computer Slowdown and Errors
- Windows congratulating users on winning prizes.
- Operating system error messages, like Windows Blue Screen.
- Hard drive running out of space.
- Uninstalled utilities, applications, or toolbars.
- Sturdy or erratic running of computer fan.
- README file indicating encrypted information.

How to avoid being affected by malware
- Preventing Malware Downloads on P2P Networks
- Never open or execute files from unknown origins or senders.
- Avoid downloading on P2P networks.
- Beware of malware diffusion through cracks and free app promises.
- Keep device's operating system updated.
- Use antivirus on non-centralized download systems.

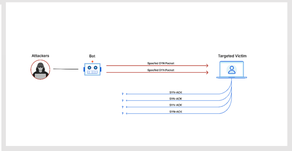
DDoS Attack

A distributed denial-of-service (DDoS) attack is a malicious attack that overwhelms a server or network with a flood of Internet traffic, resembling a traffic jam on a highway.

How does a DDoS attack work?



HTTP flood DDoS attack: multiple bot HTTP GET requests to victim.



Protocol DDoS attack: SYN flood: spoofed SYN packets

How to identify a DDoS attack
Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:
- Suspicious traffic from a single IP address or range.
- Flood of traffic from users sharing a single behavioral profile.
- Unexplained surge in requests to a single page or endpoint.
- Odd traffic patterns, spikes at odd hours or unnatural patterns.
- Specific signs varying depending on the type of attack.[3]

What are some common types of DDoS attacks?
DDoS attacks target various network connections, which are made up of various layers. The OSI model provides a framework for understanding network connectivity and its various components.
*HTTP flood *SYN flood
*Volumetric attack *Blackhole
*Rate limiting *Web application firewall

Ransomware

Ransomware is malicious software that holds systems or data hostage until a ransom is paid. It can take various forms, such as phishing spam or aggressive forms like Not Petya.

Who is the target for ransomware?
*Universities *government agencies
*medical facilities *law firms
However, organizations not listed above are not safe as ransomware can spread automatically and indiscriminately across the internet.

Ransomware examples
• Thanos, discovered in 2020, uses RIPlace to bypass anti-ransomware methods.
• RobbinHood, another EternalBlue variant, caused significant damage in 2019.
• Cerber, first appearing in 2016, netting $200,000 in July.
• NotPetya, a Russian-directed cyberattack against Ukraine, used EternalBlue.
• Maze, a ransomware group releasing stolen data.

How to Identify Ransomware
Identifying an attacker's presence can be challenging due to their attempts to conceal their presence. [4] Common signs include:
*Odd or random file or folder names *Pop-ups or ads
*File or folder errors *Suspicious processes
*Operating system alert messages

How to prevent ransomware?
Cyber Hygiene and Ransomware Prevention:
*Backups *Risk Analysis *Staff Training *Vulnerability Patching
*Application Whitelisting *Business Continuity *Penetration Testing

Phishing

Phishing is an email-based scam where attackers deceive recipients into revealing sensitive information or downloading malware. In 2020 it was the most common type of cybercrime, with the FBI's Internet Crime Complaint Center reporting more incidents of phishing than any other type of computer crime. Phishing attacks have become increasingly sophisticated and mirror the targeted site, allowing attackers to observe and transverse security boundaries.

How to Prevent Phishing Attacks?[5]
*Identifying Phishing Emails *Avoiding Phishing Emails
*Avoiding Phishing Websites *Regularly Reviewing Accounts
*Recognizing Languages *Be Prudent and Don't Take Risks
*Regularly Informing Yourself *Using Official Contact Numbers

Business Email Compromised (BEC)

BEC, a social engineering tactic, involves impersonating trusted executives, causing significant financial losses and being harder to manage than ransomware, IC3 received 2,474 complaints in 2020.

Types of Business Email Compromise Scams:
The FBI reported a significant increase in Business Email Compromise complaints in 2020, resulting in reported losses of $1.86 billion, indicating a concerning trend in these scams. Some of the common BEC scams include:
- Account Compromise: Compromise of company email accounts for scams.
- Data Theft: Targeting sensitive data like HR for future attacks.
- CEO Fraud: Disguising as CEOs, instructing employees to send money, expose data, spoof emails, request payment, steal funds.

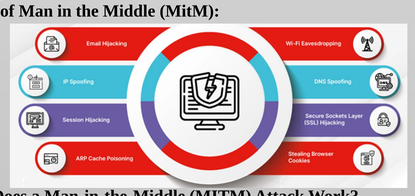
How do you detect Business Email Compromise?
- Spelling and grammar errors in emails, especially financial transactions.
- Suspicious emails from senior executives, seeking psychological advantage.
- Override routine procedures for large, time-sensitive transactions.
- Confirm email source and contact sender in person.

How to Protect Against Business Email Compromise Attacks?
- Implement anti-phishing solutions and machine learning for email analysis.
- Implement policies for high-risk actions requiring independent verification.
- Separate duties for actions requiring independent verification.
- Label emails from outside the organization as external.
- Ensure access to email accounts and use unique passcode or PIN.
- Use anti-spam software for phishing and ransomware protection.

Man in the Middle (MitM)

Man-in-the-middle (MITM) attacks involve attackers altering communication between two parties, targeting businesses, organizations, or individuals for financial gain, particularly in small and midsize businesses lacking robust security.

Types of Man in the Middle (MitM):



How Does a Man-in-the-Middle (MITM) Attack Work?
Person A sends a message to Person B.
MITM attacker intercepts the message without knowledge.
MITM attacker changes or removes the message without knowledge.
MITM attack exploits vulnerabilities in network or web, based security protocols.

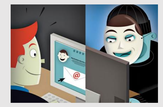
How to Prevent Man-in-the-Middle Attacks?
Regular firmware updates and security settings for home Wi-Fi routers.
Use of VPNs for data encryption between devices and server.
Enable end-to-end encryption for communication channels, Encrypt DNS traffic.
Employees responsible for patch installation and security software updates.
Encourage use of strong passwords and password managers.
Implement multi-factor authentication and connect only to secure websites.

Piggybacking attack

Is a cybersecurity attack where an unauthorized user gains access to a secure system or network by exploiting the privileges of an authorized user, leading to security breaches and slower internet speeds.

Types of Piggybacking include:
- Piggybacking Acknowledgments: Recipient acknowledges data receipt.
- Piggybacking Data: Includes data with acknowledgement message.

How Does Piggybacking Work?
Piggybacking attacks were once easier due to unencrypted Wi-Fi networks, allowing anyone within the signal's range to access a network without a security password. However, most Wi-Fi networks are now encrypted and secured with passwords, making these attacks less common. [7] Threat actors can still access networks if they have the password or can crack the encryption.



How to prevent piggybacking attacks
- Use strong passwords: long, complex strings.
- Regularly change network keys.
- Monitor connected devices.
- Remove and block unknown users immediately.

Baiting attack

Baiting attacks are social engineering tactics that use bait to lure victims into traps, aiming to steal login credentials, distribute malware, or achieve other nefarious goals.

Examples of Baiting Attacks
- Tempting Offers: Cybercriminals use free content or iPhones as baits. Victims provide personal information or create accounts.
- Online Downloads: Websites selling paid content distribute malware.
- Malware-infected Devices: USB flash drives and external hard drives used in baiting attacks.

How to detect a baiting attack?
Identifying legitimate baiting and malicious baiting can be challenging due to sophisticated cybercriminals' tactics. Some signs to look out for include:
*Overly attractive or generous offers.*Requests for personal or banking information.
*Spelling and/or grammatical errors. *Prompts to download or run something.

How to Avoid Baiting Attacks
- Regular training sessions to dispel baiting attack misconceptions.
- Baiting simulations to assess cybersecurity awareness.
- Reliable antivirus software like Microsoft's Safe Links.
- Partnerships with managed IT service providers.

Prevent Baiting Attacks with Education
- Regular cybersecurity awareness training can reduce baiting attacks by teaching employees to detect and respond to these threats using psychological manipulation.

Cases of Cyberattacks

FBI Springfield, "FBI Springfield Warns of Constant Barrage of Cyberattacks", fbi.gov, (2023). [Online] Available: https://www.fbi.gov/contact-us/field-offices/springfield/news/fbi-springfield-warns-of-constant-barrage-of-cyberattacks.
Kyle Alspach, "10 Major Cyberattacks And Data Breaches In 2023", TheChannelCo.CRN, (2023). [Online] Available: https://www.crn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023?page=1

Conclusions and Future Works

Regular employee cybersecurity training enhances threat identification, reduces damage, and increases safety awareness, boosting IT system engagement and promoting a more capable approach to compute-intensive tasks.
Highlights importance of cybersecurity for data protection:
• Teaches effective password management to minimize compromised passwords.
• Educates on phishing and cyber threats.
• Regularly updates operating systems, anti-malware programs, and applications.
• Uses secure file transfer systems for personal information protection.
• Locks computers and devices, employees handle screen locking, IT handles physical lockouts,reports lost/stolen devices immediately and secure portable media.
• Applies privacy settings and limits personal information visibility.
• Uses authorized software downloads to prevent data breaches.

Blog

https://efcsecure2024.blogspot.com/

References

[1] Usecure. (2022). La Guía Completa Para la Formación en Materia de Seguridad [Online]. Available: https://www.usecure.io/hubfs/Partner%20Sales%20+%20Marketing%20Resources/La%20gu%C3%ADa%20completa%20para%20la%20formaci%C3%B3n%20en%20materia%20de%20seguridad.pdf.
[2] Fernández, Y. (2020, June 2). Malware: Qué Es, Qué Tipos Hay y Cómo Evitarlos. [Online] Available: https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos
[3] Cloudflare. (2024) What Is a DDoS Attack? [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[4] Comunicación, C. (2024). La Guía Esencial Sobre el Ransomware: Qué Es, Cómo Identificarlo y Proteger Mis Datos. [Online] Available: https://www.grupocibernos.com/blog/guia-esencial-ransomware
[5] Panda. (2016, February 21). 10 Consejos Para Evitar Ataques de Phishing [Online]. Available: https://www.pandasecurity. com/es/mediacenter/10-consejos-para-evitar-ataques-de-phishing/.
[6] Higgins, M. (2023, April 23). Piggybacking: Meaning, Types and Prevention. [Online] Available: https://nordvpn.com/es-mx/blog/what-is-piggybacking/