Employee Guide to Cybersecurity and Cyber Threats

Emily Y. Feliciano Cruz
Program: Master in Computer Science
Advisor: Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

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. By focusing on information security, EFC Secure ensures effective controls for its customers and employees.*

Key Terms *— Antivirus, Incident, Phishing, Ransomware.*

What is Cyberattack and What are the Various Cyber Threats?

A cyberattack is an attack that is mounted against our digital equipment and services through cyberspace [2]. 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 (including corporate, state, and patent espionage).

Virtually all cyber threats can be divided into those three categories. 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

The eight most common types of cyber threats are:

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 and malicious software [3].

Figure 1
Types of Malwares

Based on the premise that malware is any computer program designed to cause some damage, we can make the following classification, which, although it is not the only one, is the most common:

- Virus: Programs that replicate or spread through computers with the user’s help.
- Worms: Used to create botnets, networks of zombie computers, and launch various types of attacks.
- Trojan: A program that goes unnoticed, entering a computer as if it were using a Trojan Horse.
- RAT: Remote access Trojan.
- Backdoor: Programs that allow remote access or execution of commands.
- Downloader or dropper: Program that downloads and runs other malware.
- Hack tool: Programs used to carry out various types of attacks.
- Ransomware: Program that encrypts users' files and demands a ransom for decryption.
- Bot: Program that interacts automatically with another program.
- Rootkit: A hidden program allowing attackers to gain access with elevated privileges.
- Keylogger: Program that captures keystrokes to inform the attacker.
- Mining Software: Program to perform mining of cryptocurrencies.
- Info Stealer: Program that searches for passwords or personal information.
- Spyware: Software that collects user activity without their permission.
- PUPs/PUAs: Unwanted programs like browser bars.
- Adware: Malware that displays advertisements.

Symptoms of Being Affected by Malwares

The symptoms can be very varied and very different depending on the operating system, the type of device and, of course, the type of malware it is and what the purpose is. Some of the most common symptoms include:

- Computer Slowdown and Errors
- Slowing down of computer.
- 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.
- Change in file type or extension of photos.
- README file indicating encrypted information.

Any of these symptoms indicates that, most likely, your computer is affected by one of the types of malwares mentioned in the previous section.

How to Avoid Being Affected by Malware?

- Preventing Malware Downloads on P2P Networks
- Never open or execute files from unknown origins or senders.
- Extreme precautions are advised when downloading programs on P2P networks.
- Cracks and promises of free applications are common methods of malware diffusion.
- Keep device's operating system updated.
- Use antivirus, especially on operating systems without centralized download methods.

DDoS Attack

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic by overwhelming a targeted server or network with a flood of Internet traffic [4]. It uses multiple compromised computer systems, including computers and IoT devices, resembling an unexpected traffic jam clogging up a highway.

How Does a DDoS Attack Work?

DDoS attacks involve networks of infected Internet-connected machines, known as bots or zombies, controlled remotely by attackers. These bots, or botnets, send requests to a victim's IP address, potentially overwhelming the server or network and denial-of-service to normal traffic. The attacker can direct the attack by sending remote instructions to each bot, making it difficult to separate attack traffic from normal traffic due to each bot being a legitimate Internet device.

How to Identify a DDoS Attack?

DDoS attacks often cause sudden slowdowns or unavailable services, but further investigation is necessary due to potential traffic spikes [5]. 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.

What are Some Common Types of DDoS Attacks?

DDoS attacks target various network connections, which are made up of various layers. The OSI model, a conceptual framework, describes network connectivity in seven distinct layers: application, presentation, session, transport, network, data link, and physical. Attacks can be divided into three categories: application layer attacks, which exhaust the target's resources to create a denial-of-service, and layer 7 attacks, which target the server layer where web pages are generated and delivered in response to HTTP requests. These attacks are difficult to defend against as it can be difficult to differentiate malicious traffic from legitimate traffic. The OSI model provides a framework for understanding network connectivity and its various components.

- **HTTP flood-A:** A denial-of-service attack involves repeatedly refreshing a web browser on multiple computers, resulting in a flood of HTTP requests. This attack can be simple or complex, with simpler versions targeting one URL and using a range of IP addresses, referrers, and user agents.

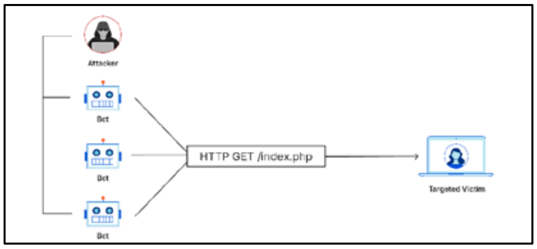

Figure 2

Application Layer Attack Example: HTTP Flood DDoS Attack – Multiple Bot HTTP GET Requests to Victim

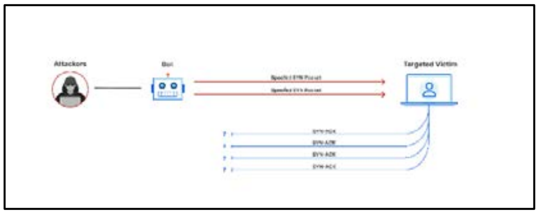

Figure 3

Protocol Attacks

Protocol attacks, also known as state-exhaustion attacks, disrupt services by over-consuming server resources or network equipment. They exploit weaknesses in layer 3 and 4 of the protocol stack, rendering the target inaccessible. An example is the SYN flood.

- **SYN flood:** A SYN Flood is a cyber-attack that uses the TCP handshake to send multiple spoofed SYN packets to a target machine, exhausting resources and leaving the target unanswered.
- **Volumetric attacks:** DDoS attacks cause congestion by consuming bandwidth between the target and the larger Internet. Mitigation requires distinguishing between attack and normal traffic. Multi-vector attacks use multiple pathways, distracting efforts. Layered solutions are effective, and indiscriminate traffic limiting may lead to attacks adapting to countermeasures.
- **Blackhole routing:** Network admins can create a blackhole route to funnel traffic, allowing both legitimate and malicious traffic to be routed and dropped. However, this is not ideal as it makes the network inaccessible, allowing attackers to gain their desired goal.
- **Rate limiting:** Rate limiting is a technique that restricts server requests over a specific time

frame, preventing web scrapers from stealing content and brute force login attempts.

- **Web application firewall:** A Web Application Firewall (WAF) acts as a reverse proxy between the internet and a server, protecting it from malicious traffic. It filters requests based on DDoS tools, enabling quick implementation of custom rules in response to attacks.
- **Anycast network diffusion:** Cloudflare uses a DDoS mitigation method using an Anycast network to spread attack traffic across distributed servers, whose effectiveness depends on network size and efficiency.

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. Once taken over, the malware encrypts user files, requiring a mathematical key known only to the attacker. Users are presented with a message stating their files are inaccessible and will only be decrypted if an untraceable Bitcoin payment is sent. Some forms may claim to be law enforcement agencies shutting down the victim's computer due to pornography or pirated software.

Who is the Target for Ransomware?

Attackers target organizations for ransomware in various ways [6]. Universities may be targeted due to their smaller security teams and file sharing capabilities, while government agencies, medical facilities, and law firms may be more likely to pay quickly for ransoms. However, organizations not listed above are not safe as ransomware can spread automatically and indiscriminately across the internet. It is crucial to be aware of these potential threats and protect yourself.

Ransomware Examples

Ransomware, a form of cybercrime, has gained popularity in the past five years due to the availability of untraceable payment methods like Bitcoin, with some of the most notorious offenders:

- CryptoLocker, a 2013 attack, infected up to 500,000 machines [6].
- WannaCry spread autonomously using EternalBlue.
- NotPetya used EternalBlue and may have been part of a Russian-directed cyberattack against Ukraine.
- Cerber, first appearing in 2016, netting attackers $200,000 in July.
- Maze, a new ransomware group known for releasing stolen data to the public.
- RobbinHood, another EternalBlue variant, caused significant damage in Baltimore, Maryland in 2019.
- Sodinokibi targets Microsoft Windows systems and encrypts all files except configuration files.
- Thanos, discovered in January 2020, uses the RIPlace technique to bypass most anti-ransomware methods.

How to Prevent Ransomware?

To prevent ransomware infection, follow these defensive steps, which are generally good security practices, to enhance your defenses against various attacks:

- Regularly patch and update operating systems.
- Avoid installing or granting administrative privileges to unknown software.
- Install antivirus and whitelisting software to detect malicious programs.
- Regularly and automatically back up files to reduce damage from malware attacks.

How to Identify Ransomware?

Identifying an attacker's presence can be challenging due to their attempts to conceal it [7]. Common signs include:

- Odd or random file or folder names: Ransomware-created files may have unusual names.
- Pop-ups or ads: Windows may display ransomware messages offering system unlocking assistance.

- File or folder errors: Encrypted files may display errors or appear corrupted.
- Suspicious processes: Background processes can indicate a ransomware attack.
- Operating system alert messages: Modern systems may display alert messages when a security threat is detected.

How Do I Protect My Networks?

Cyber Hygiene and Ransomware Prevention:

- Backups: Ensure all critical information is backed up and tested during incidents.
- Risk Analysis: Conduct a comprehensive cybersecurity risk analysis.
- Staff Training: Train staff on cybersecurity best practices.
- Vulnerability Patching: Implement appropriate patching of known system vulnerabilities.
- Application Whitelisting: Only allow approved programs on networks.
- Incident Response: Have an effective plan and exercise it.
- Business Continuity: Test the ability to sustain operations without system access.
- Penetration Testing: Test system security and defense against attacks.

Phishing

Phishing is an email-based scam where attackers deceive recipients into revealing sensitive information or downloading malware. As of 2020, it is 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.

Types of Phishing

- Phishing emails: Emails containing job offers, security warnings, or invoices that spread ransomware.
- Pharming: Cyber criminals create fake web pages, attacking domain name hosts and directing users to scam pages. Dropbox recently suffered such an attack.
- Malvertising: Cyber attackers buy ads on trusted websites and install malware inside them. Popular sites like The New York Times, Spotify, WordPress, The Atlantic, and Adobe have been victims.
- Spear phishing: Hackers trawl victims' social media accounts to gather personal information. The personal nature of the attack makes it harder to detect as fraudulent.
- Whaling: A variation of phishing that targets CEOs and other executives.
- Quid Pro Quo attack: The attacker requests sensitive information from the victim in exchange for a desirable service. The credentials are used to gain access to other sensitive data stored on the device and its applications.
- Data Breach: A security violation where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an unauthorized individual.

How to Recognize Phishing?

Phishing scammers use emails and text messages to steal passwords, account numbers, and Social Security numbers, potentially accessing your accounts or selling them to others. They use common tactics like telling a story, appearing as a trusted company, or using an unfamiliar website or app. These attacks are successful and often update their tactics. It's possible that it's a message from a scammer who might:

- Suggesting suspicious activity in accounts.
- Claiming payment issues.
- Suggesting confirmation of personal or financial information.
- Attaching fake invoices.
- Asking for payment links with malicious programs.
- Scams about government refund eligibility.
- Offering free coupons without verification.

How to Prevent Phishing Attacks?

- Identifying Phishing Emails: Use names and images of real companies, address by company or employee name, and include websites that resemble real companies [8].
- Avoiding Phishing Emails: Never send passwords or personal details via email, and only respond to questions about bank details [8].
- Avoiding Phishing Websites: Only enter confidential data on secure websites, starting with 'https://' and displaying a small, closed padlock icon [8].
- Regularly Reviewing Accounts: Regularly check bank accounts for irregularities in online transactions [8].
- Recognizing Languages: Phishing can target any language, and poorly written or translated communications can indicate a potential attack [8].
- Be Prudent and Don't Take Risks: Systematically reject emails or communications that require confidential data and contact your bank for clarification [8].
- Regularly Informing Yourself: Keep passwords up to date, avoid reusing them, and remember them easily [8].
- Using Official Contact Numbers: Use official company numbers and avoid unofficial numbers [8].
- Data Encryption: Encrypt sensitive data at rest and in transit to prevent unauthorized access [8].

Business Email Compromised (BEC)

Business Email Compromise (BEC) is a social engineering tactic where an attacker impersonates a trusted executive to handle financial matters within an organization. They send emails requesting wire transfers, banking details, and other money-related tasks, resulting in significant financial losses. BEC attacks are harder to monitor and manage than ransomware, which encrypts data and holds it hostage until a ransom is paid. In 2020, the IC3 received 2,474 complaints related to ransomware.

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 [9]. Some of the common Business Email Compromise scams include:

- Account Compromise: Employees' company email accounts can be compromised, used for scams. Attackers may impersonate attorneys, accountants, or IRS representatives to pressure employees into quick action.
- Data Theft: Attackers may target employees with access to sensitive data, such as HR, to plan future attacks.
- CEO Fraud: Attackers pose as CEOs and direct employees to send money or expose private company data. Attackers spoof emails from different organizations or vendors, requesting payment to a controlled account, stealing funds.

How Do You Detect Business Email Compromise?

Common signs of Business Email Compromise attacks include:

- Spelling mistakes: Emails filled with spelling or grammar errors should be suspicious, especially when dealing with requests for financial transactions.
- Suspicious emails from senior executives: Attackers may pretend to be senior executives to gain psychological advantage. Employees should reflect on the character of the senior executive when receiving urgent instructions.
- Requests to bypass set procedures: Employees should be wary of requests to bypass routine procedures, especially for large and time-sensitive transactions.

Before submitting similar requests, employees should confirm the email source and, if unsure, contact the sender in person.

How to Protect Against Business Email Compromise Attacks?

- Implement anti-phishing solutions and machine learning for email analysis.
- Train employees on identifying and responding to Business Email Compromise attacks.
- 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 senior executives' email accounts and use a unique passcode or PIN.
- Use anti-spam software to guard against sophisticated phishing and ransomware attacks.

Man in the Middle (MitM)

Man-in-the-middle (MITM) attacks are cyberattacking where an attacker secretly relays and alters communications between two parties who believe they are directly communicating. Examples include active eavesdropping, where the attacker makes independent connections and relays messages to make victims believe they are talking directly. MITM attacks can succeed only when the attacker impersonates each endpoint sufficiently well. Most cryptographic protocols include endpoint authentication to prevent MITM attacks. MITM attacks target businesses, organizations, or individuals if there is a perceived chance of financial gain by cyber criminals. Popular industries for MITM attacks include banks, financial companies, healthcare systems, and IoT-connected businesses. Small and midsize businesses face greater risks due to their lack of robust security.

Types of Man-in-the-Middle (MITM) Attacks

1. **Email Hijacking:** Cybercriminals exploit email accounts of trusted companies, accessing sensitive data and money [10].
2. **Wi-Fi Eavesdropping:** Attackers connect victims to malicious networks, monitoring online activity and scraping sensitive data [10].
3. **DNS Spoofing:** DNS spoofing is a method where manipulated DNS records redirect legitimate traffic to a fake website, prompting users to take specific actions, stealing data, and posing a threat [10].
4. **Session Hijacking:** Session hijacking is a MITM attack where an attacker steals a session cookie from a victim's account, allowing them to log in from their browser [10].
5. **Secure Sockets Layer (SSL) Hijacking:** HTTPS, SSL, and TLS are secure server protocols used by websites to display status and protect data, but SSL hijacking can intercept data [10].
6. **ARP Cache Poisoning:** The Address Resolution Protocol (ARP) is a crucial communication protocol used by cybercriminals to identify link layer addresses and translate them to local network IP addresses [10].
7. **IP Spoofing:** IP spoofing is a cyber-attack where an attacker modifies a legitimate website's IP address to resemble the intended user's, redirecting internet traffic [10].
8. **Stealing Browser Cookies:** Browser cookies enhance the browsing experience, but cybercriminals can steal them through MITM attack techniques like Wi-Fi eavesdropping or session hijacking, allowing access to sensitive information [10].

How Does a Man-in-the-Middle (MITM) Attack Work?

MITM Attack Work Order:

- 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, web, or browser-based security protocols.

How to Detect a Man-in-the Middle (MITM) Attack?

MITM attacks, involving phishing or spoofing, are difficult to detect due to their sophistication. Prevention is crucial, and signs include unusual disconnections, strange URLs, and public, unsecured Wi-Fi. Attackers scrape usernames and passwords, create bogus websites, intercept messages, and collect data through DNS hijacks. Avoiding public, unsecured Wi-Fi is essential to prevent malicious code eavesdropping.

Impact of Man-in-the-Middle Attacks on Enterprises

MITM attacks pose significant risks to enterprises due to mobility, remote workers, IoT vulnerabilities, and unsecured Wi-Fi connections. The 2022 Cybersecurity Almanac reported $6 trillion in damage in 2021, expected to reach $10 trillion annually by 2025. Small businesses experience average losses of $55,000.

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 servers.
- Enable end-to-end encryption for communication channels.
- Employees responsible for patch installation and security software updates.
- Encourage the use of strong passwords and password managers.
- Implement multi-factor authentication (MFA) for defense against threats.
- Connect only to secure websites.
- Encrypt DNS traffic for authentication.
- Adopt a zero-trust philosophy for continuous verification.
- Utilize the User and Entity Behavior Analytics Solution to detect anomalies.

Piggybacking

Piggybacking 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.

Piggybacking Definitions and Types

- Password Sharing: Unauthorized individuals share login credentials, allowing unauthorized access.
- Physical Access: Unauthorized individuals gain secure areas by following or using physical access cards or keys.
- Remote Access: Unauthorized individuals gain access using stolen or leaked credentials.
- Wi-Fi Piggybacking: Unauthorized access exploits security vulnerabilities, affecting unprotected businesses, passwords, personal hotspots, and routers.

What is Piggybacking in Computer Networks?

Piggybacking is a technique in computer networks that enhances efficiency and reduces overhead by combining multiple information in a single transmission, with two main types:

1. Piggybacking Acknowledgments: In TCP, the receiver acknowledges the receipt of data, reducing the number of separate packets and associated overhead.
2. Piggybacking Data: The receiver can include its data along with the acknowledgment message, minimizing the number of separate packets.

Piggybacking reduces packets and improves network performance, especially in limited resources or latency optimization. Careful protocol design is necessary to avoid issues like message collisions or excessive delays.

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 [11]. However, most Wi-Fi networks are now encrypted and secured with passwords, making these attacks less common. Threat actors can still access networks if they have the password or can crack the encryption.

How to Prevent Piggybacking Attacks?

Follow these steps to protect your Wi-Fi from unwanted intruders.

- Use strong passwords: Long, complex strings of random letters, symbols, and numbers, with at least ten characters.
- Regularly change passwords: Regularly change your network key to prevent future reconnections.
- Monitor connected devices: Check network settings to identify devices currently connected to the Wi-Fi.
- Remove and block unknown users: Remove and block them immediately if they are found on the network.

Baiting Attack

Baiting attacks are social engineering techniques that use bait to lure victims into a trap, aiming to steal login credentials, distribute malware, or achieve other nefarious goals [12]. They exploit human curiosity by making false promises and are popular among cybercriminals due to their lack of advanced technical skills.

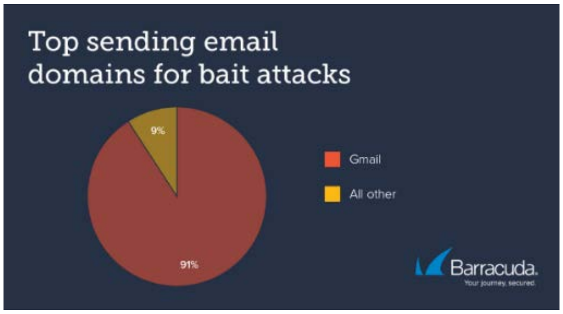

Figure 4
Top Sending Email Domains for Bait Attacks

According to a report from Barracuda, 35% of organizations were targeted and had an average of three employee email accounts impacted by bait attacks; also, 91% of all bait attacks were conducted over Gmail.

Examples of Baiting Attacks

- Tempting Offers: Cybercriminals use emails offering free content or iPhones as baits. Victims provide personal information or create accounts [13].
- Online Downloads: Websites selling paid content distribute malware, enabling remote control and DDoS attacks [13].
- Malware-infected devices: USB flash drives and external hard drives are used in baiting attacks. In 2018, a malware-infected CD was used in a significant attack [13].

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.
- Urgency or artificial shortages.
- Spelling and/or grammatical errors.
- Requests for personal or banking information.
- Prompts to download or run something.
- Potential for malware or malicious code.

How to Avoid Baiting Attacks

Baiting attacks are often successful due to weak security protocols and insufficient cybersecurity awareness. Organizations can implement multiple security practices to reduce the risk of employees revealing sensitive information. Here are those you should know about:

- Regular cybersecurity awareness training sessions to dispel misconceptions about baiting attacks.
- Baiting simulations to assess cybersecurity awareness and remind employees of threats.
- Reliable antivirus software and features like Microsoft’s Safe Links or Safe Attachments to protect against baiting attacks.
- Partnering with managed IT service providers for affordable, enterprise-level security if maintaining an effective cybersecurity program is challenging.

Prevent Baiting Attacks with Education

Baiting in cybersecurity is a severe threat that uses psychological manipulation to bypass security defenses. Regular cybersecurity awareness training can reduce the success rate of baiting attacks, allowing organizations to teach employees to detect and respond to them.

CYBERSECURITY MEASURE FOR EMPLOYEES

Regular employee cybersecurity training improves threat identification, reduces damage, and increases safety awareness, boosting engagement with IT systems and promoting a more capable approach to compute-intensive tasks [14]. Here are the main cybersecurity measures for employees:

- Highlight the importance of cybersecurity for protecting customer and employee data.
- Teach effective password management to reduce the impact of compromised passwords.
- Educate employees on phishing and scams.
- Regularly update operating systems, anti-malware programs, and applications.
- Protect personal information using secure file transfer systems.
- Lock computers and devices, with employees responsible for locking screens and the IT department for physical lockouts.
- Secure portable media, including screen locks and malware scans.
- Report lost or stolen devices immediately to prevent IT from remotely wiping devices.
- Actively contribute to safety by reporting suspicious activity to the IT administrator.
- Apply privacy settings and limit personal information visibility.
- Use authorized software downloads to prevent data breaches and disruptions.
- Manage documents securely and understand how to share sensitive data and intellectual property.
- Implement rigid mobile device management policies to secure personal devices.

EMPLOYEE RESPONSIBILITIES

All employees will be responsible for:

1. Use information systems with caution to prevent unauthorized disclosure of sensitive information.
2. Be wary of suspicious messages and technologies.
3. Use company's information systems only for official tasks.
4. Keep passwords secret and secure.
5. Take precautions to prevent damage, loss, or theft of government devices or equipment.
6. Inform supervisor and information systems personnel immediately of any device or equipment loss, theft, or compromise.

CASES OF CYBERATTACKS

In the next section, some cases of cyberattacks will be presented.

Case #1: Florida Man Is Sentenced For Money Laundering Stemming From A Business Email Compromise Scheme [15]

U.S. Attorney's Office, Western District of North Carolina, "Florida Man Is Sentenced For Money Laundering Stemming From A Business Email Compromise Scheme", justice.gov, 2024. https://www.justice.gov/usao-wdnc/pr/florida-man-sentenced-money-laundering-stemming-business-email-compromise-scheme.

Case #2: 10 Major Cyberattacks And Data Breaches In 2023 [16]

Kyle Alspach, "10 Major Cyberattacks and Data Breaches In 2023", TheChannelCo.CRN, 2023. https://www.crn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023?page=1.

Case #3: FBI Springfield Warns of Constant Barrage of Cyberattacks [17]

FBI Springfield, "FBI Springfield Warns of Constant Barrage of Cyberattacks", fbi.gov, 2023. https://www.fbi.gov/contact-us/field-offices/springfield/news/fbi-springfield-warns-of-constant-barrage-of-cyberattacks.

COMPUTER SECURITY SURVEY [18] [19]

1. What is cybersecurity?
2. What is a cyberattack?
3. What are the various cyber threats?
4. Who poses the biggest threat to your organization's cybersecurity?
5. Who is responsible for installing and maintaining the security software on your computer?
6. What version of Windows is installed on the computer you normally use to connect to the Internet?
7. What web browser do you typically use?
8. Are your devices protected against malware (e.g. antivirus, spam filter)?
9. What anti-spyware software do you use?
10. Do you use firewall software on your computer?
11. Is your firewall updated regularly?
12. Is management monitoring your computer all the time?
13. Has a cybersecurity officer been appointed in your company?
14. Are there guidelines for the safe use of computer equipment and data by employees?
15. Are these cybersecurity guidelines or measures applied consistently and systematically applied and regularly monitored?
16. Do you discuss cybersecurity with customers, other employees, and suppliers?
17. Is the data encrypted on your systems (digital files, storage media, terminals, servers)?
18. Do you hold or process personal data in electronic form?
19. Is your wireless network encrypted and secure?
20. Is the wireless network available to guests separate from that of employees?

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] Cisco. (2024). *¿Qué es la Ciberseguridad?* [Online]. Available: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html.

[3] Y. Fernández. (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.

[4] Kaspersky. (2024). *Cómo Prevenir Ciberataques* [Online]. Available: https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks.

[5] Cloudflare. (2024) What Is a DDoS Attack? [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[6] J. Fruhlinger. (2020, June 19). *Ransomware Explained: How it works and how to remove it* [Online]. Available: https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[7] C. Comunicación. (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.

[8] 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/.

[9] T. Mann. (2022, March 10). *What is Business Email Compromise and How Do You Detect it?* [Online]. Available: https://www.lepide.com/blog/what-is-business-email-compromise-and-how-do-you-detect-it/#:~:text=How%20do%20you%20detect%20Business%20Email%20Compromise%201,...%203%20Requests%20to%20bypass%20set%20procedures%20.

[10] Fortinet. (2024). *Man-in-the-Middle Attack: Types and Examples* [Online]. Available: https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack#:~:text=A%20man-in-the-middle%20%28MITM%29%20attack%20is%20a%20form%20of,entities%20in%20a%20communication%20channel%20to%20steal%20data.

[11] M. Higgins. (2023, April 23). *Piggybacking: Meaning, Types and Prevention* [Online]. Available: https://nordvpn.com/es-mx/blog/what-is-piggybacking/.

[12] B. Lenaerts Bergmans. (2023, November 8). *10 Types of Social Engineering Attacks and How to Prevent Them* [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/.

[13] Teal. (2023, September 19). *What Are Baiting Attacks and How Can You Prevent Them?* [Online]. Available: https://tealtech.com/blog/it-services/cybersecurity/how-to-prevent-baiting-attacks/.

[14] Ciberseguridad. (2024). *Ciberseguridad Para Empleados* [Online]. Available: https://ciberseguridad.com/guias/empleados/.

[15] U.S. Attorney's Office. (2024, January 4). *Florida Man Is Sentenced for Money Laundering Stemming From A Business Email Compromise Scheme* [Online]. Available: https://www.justice.gov/usao-wdnc/pr/florida-man-sentenced-money-laundering-stemming-business-email-compromise-scheme.

[16] K. Alspach. (2023, December 13). *10 Major Cyberattacks and Data Breaches in 2023* [Online]. Available: https://www.crn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023.

[17] FBI Springfield. (2023). *FBI Springfield Warns of Constant Barrage of Cyberattacks* [Online]. Available: https://www.fbi.gov/contact-us/field-offices/springfield/news/fbi-springfield-warns-of-constant-barrage-of-cyberattacks.

[18] A. Velázquez. (2024). *10 Preguntas para una Encuesta de Seguridad Informática* [Online]. Available: https://www.questionpro.com/blog/es/encuesta-de-seguridad-informatica/.

[19] Ciset. (2022, December 14). *¿Cómo Realizar Una Encuesta de Ciberseguridad?* [Online]. Available: https://www.ciset.es/publicaciones/blog/851-como-realizar-una-encuesta-de-ciberseguridad?dt=1704836314928.