Cybersecurity at Home

HOMESCHOOL ACADEMICS LEARNING CENTER (SM)
WRITTEN BY CHERISA CHAPA

Printed by Recharge Consultants, LLC., in the United States of America.

First printing, 2024.

Recharge Consultants LLC
c/o Cherisa Chapa
PO Box 114
Burkburnett, TX 76354-0114

www.RechargeConsultants.com

Contents

Introduction

You may be concerned about cybersecurity protections due to increased online activity from remote work or schooling or simply wanting to protect personal information and devices from potential online threats. Your concerns could also stem from a recent data breach, a phishing scam, cyberbullying targeting a child, or identity theft.

This overview covers the cybersecurity threat landscape, recognizing threat actors, and identifying common vulnerabilities and exploits.

Cybersecurity Summary

Child safety concerns

If a child is being cyberbullied or exposed to inappropriate content online, parents may prioritize teaching them about online safety and implementing parental controls.

Financial concerns

Being notified that your information has been exposed in a breach or that you have experienced credit card fraud could prompt a family to take steps to secure their online accounts.

Sensitive data exposure

Growing awareness of data collection practices and sharing personal information like medical records or financial details online could motivate a family to improve their cybersecurity practices.

Increased online activity

If working remotely or spending more time online for education, the need for robust cybersecurity measures may become more apparent.

Smart home devices

Using connected devices like smart speakers, security systems, or other Internet of Things (IoT) devices can introduce additional vulnerabilities, prompting a family to review their network security.

Educating your children and older ones about cybersecurity can significantly reduce the chances of falling victim to cyberattacks. With cyber threats changing constantly, protecting your household from cyber threats is paramount.

Think cybersecurity is complicated?

Let’s simplify it.

Understanding the Threat Landscape

In cybersecurity, "threat landscape" refers to *the overall picture of potential cyber threats an individual might face, encompassing all known and emerging risks, vulnerabilities, attack vectors, and threat actors*. This landscape constantly evolves as new technologies emerge, cybercriminals develop new tactics, and vulnerabilities are discovered.

Safeguarding your family from cybersecurity threats involves learning about specific behaviors of threat actors, their motivations, the types of attacks they might use, any potential vulnerabilities in your home, and emerging trends in cybercrime.

Generational Attacks

Sadly, every family member is a potential target for cyber threats, from the youngest playing educational games on tablets to teenagers on social media to parents managing finances online while streaming reality television shows.

Another reality is that **threat actors tailor their attacks to exploit specific vulnerabilities within different age demographics.**

Boomers and the Silent Generation (57+ years old)

Less technologically advanced and socially isolated, older adults (over 60) are often targeted through traditional needs. A significant 24% of older adults (over 60) said their fraud began with a phone call. For those 80 and over, that figure rose to over 40%.

Baby boomers are especially likely to use technology to stay in touch with friends and family, which can make them vulnerable to social engineering attacks. Common scams involve winning the lottery or a prize, romantic partnerships, paying upfront fees, sharing personal information, or paying or sending money via gift cards.

Gen X (41 – 56 years old)

Gen Xers remember life before digital technology became ubiquitous, and they appreciate the value of balancing their digital and analog worlds. Due to their reliance on email communication, Gen X individuals may be more likely to fall victim to phishing scams, where attackers send convincing emails, especially those that mimic legitimate sources, to trick users into revealing sensitive information.

Caring for aging parents and young children, these adults are generally exploited through email scams related to technology support or healthcare. These middle-aged adults are more susceptible to phishing attacks that seem urgent or work-related.

Millennial (25-40 years old)

Although generally considered the most tech-savvy demographic, many Millennials are likelier to have cybersecurity liabilities. Millennials are often victims of cyberattacks because they are more likely to be online for education, entertainment, and work.

Millennials and Gen Z are often victims of phishing, identity theft, romance scams, and cyberbullying.

Millennials are the most significant security offenders. They are the most likely to use the same password across multiple online accounts (80%) and the most inclined to trust companies to keep their data secure (75%). Therefore, it's no surprise they're the most impacted generation regarding data breaches (60%).

Millennials often use multiple connected devices at once, which increases their risk of fraud and identity theft.

Gen Z (18-24 years old)

These younger adults, being digital natives, spend a significant amount of time online, making them prime targets for cyberattacks across various platforms like social media, online banking, and gaming. Hackers often exploit Gen Z's trust in online interactions by using social engineering techniques to manipulate them into sharing sensitive information.

Gen Z individuals will likely click on malicious links in phishing emails, unknowingly compromising their personal information. Gen Z is exposed to potential vulnerabilities within the Internet of Things (IoT) ecosystem with the widespread use of connected devices like smart home appliances.

Overall

According to a new AARP Fraud Watch Network report, an estimated 141.5 million adults (42%) have had money or sensitive information stolen through fraud. **It's a startling reality that, with the click of a link, anyone—from the tech-savvy to the average internet user—can unwittingly give cybercriminals access to their most private information.**

Notes:

_____

_____

_____

_____

_____

Threat Actors Come in Different Types

Anyone can become a target for a threat actor. Threat actors target specific individuals or entities. They can be trolls who spam social media posts on someone's account, employees who steal privileged information from their organization, or ransomware users who target large organizations or high-profile individuals for monetary gain. They can also use advanced persistent threats (APT) to steal sensitive data over a prolonged period.

There are many different types of threat actors. While most fall under the standard cybercriminal umbrella, some do not. A threat actor is *someone who harms a computer system or device, whether that's through malware or stealing sensitive data*.

There are many types of threat actors:

Type	Definition	Motivations	Status
Insider Threat	Individuals in the targeted organization intentionally harm their networks. Employees or contractors with malicious intent or accidental actions.	Job Dissatisfaction	On the rise.
Nation-State Actors	Well-resourced groups that pay cybercriminals to perform various malicious acts. They could be governments conducting espionage, sabotage, or warfare.	Geopolitical motivations	Elevated threat.

Cybercriminals	Any person or group that intentionally harms a digital system. Individuals or groups seeking financial gain.	Financial gain or profit	Social Engineering Strategies
Thrill Seekers	Anyone who damages a network for personal enjoyment	Fun and satisfaction	How much sensitive data they can steal or how “far” they can go.
Terrorists	Any group that forces another to act. Groups driven by political or social causes.	Political / Ideological	Intimidate or force a group of people into performing specific actions
Hackers (i.e., black hat)	Any person who attempts to break into a system with malicious intent. Including “script kiddies” who are amateur hackers using pre-made tools.	Various Reasons	Several techniques to reach their goals include hacking passwords, phreaking, or executing a distributed denial-of-service attack.

Cybersecurity Threats

Cybersecurity threats are potential dangers or malicious actions that aim to compromise the confidentiality, integrity, or availability of digital information, systems, or networks. These threats can come from various sources, including hackers, malicious software, insider threats, or even accidental human error.

Social engineering is a form of attack that exploits human nature and behavior. It exploits human characteristics such as trust in others, a desire to aid, or a propensity to show off.

Social engineering attacks take two primary forms: convincing someone to perform an unauthorized operation or revealing confidential information. In almost every case, the attacker tries to convince the victim to perform some activity or reveal information they shouldn’t.

These attacks work because we are human. They are designed to focus on various aspects of human nature and take advantage of them. Most of us are vulnerable to one or more common social engineering principles.

Social Engineering Principles

Authority

Authority is an effective technique because most people are likely to respond to authority with obedience. The trick is to convince the target that the attacker is someone with valid internal or external authority. Some attackers claim authority verbally, while others assume authority by wearing a costume or uniform.

Intimidation

Intimidation can sometimes be seen as a derivative of the principle of authority. It uses authority, confidence, or even the threat of harm to motivate someone to follow orders or instructions. Often, intimidation is focused on exploiting uncertainty in a situation where a clear directive of operation or response isn't defined. Intimidation carries a perceived penalty.

Consensus

Consensus or social proof is taking advantage of a person's natural tendency to mimic what others are doing or are perceived as having done in the past. The attacker attempts to convince the victim that a particular action or response must be consistent with social norms or previous occurrences.

Scarcity

Scarcity is a technique used to convince someone that an object has a higher value based on the object's scarcity. This could relate to only a few items produced, limited opportunities, or where most of the stock is sold, and only a few items remain. In other words, the opportunity will be lost if you don't grab the items now.

Familiarity

Familiarity or liking, as a social engineering principle, attempts to exploit a person's native trust in that which is familiar. The attacker often tries to appear to have a common contact or relationship with the target, such as mutual friends or experiences or uses a facade to take on the identity of another person or business. If the target believes a message is from a known entity, such as a friend or their bank, they're much more likely to trust the content and even act or respond.

Trust

Trust is a social engineering principle that involves an attacker working to develop a relationship with the victim. This may take seconds or months, but eventually, the attacker

attempts to use the value of the relationship (the victim's trust in the attacker) to convince the victim to reveal information and perform an action.

> A *honeytrap* attack is a social engineering technique targeting individuals looking for love on online dating websites or social media. The criminal befriends the victim by creating a fictional persona and setting up a fake online profile. Over time, the criminal takes advantage of the relationship and tricks the victim into giving them money, extracting personal information, or installing malware.

Urgency

Urgency often deals with scarcity because the need to act quickly increases as scarcity indicates a greater risk of missing out. Urgency is frequently used to get a quick response from a target before they have time to consider or refuse compliance carefully.

Eliciting Information

Eliciting information is gathering or collecting information from systems or people. In the context of social engineering, it is used as a research method to craft a more effective pretext. A pretext is a false statement crafted to sound believable to convince you to act or respond in favor of the attacker.

Any of these social engineering techniques can be used as a weapon to harm the target victim and to obtain more information (or access). Any fact, truth, or detail collected, gathered, or gleaned from the target can form a complete and more believable pretext or false story. This increases the chance of success at the next level or stage of an attack.

Prepending

Prepending is adding a term, expression, or phrase to the beginning or header of some other communication. Often, prepending is used to refine or establish the pretext of a social engineering attack, such as spam, hoaxes, and phishing. An attacker can precede the subject of an attack message with RE: or FW: (which indicates "in regard to and forwarded," respectively) to make the receiver think the communication is the continuance of a previous conversation rather than the first contact of an attack.

These prepending attacks can also fool filters such as spam filters, antimalware, firewalls, and intrusion detection systems (IDSs).

Phishing

Phishing is a social engineering attack focused on stealing credentials or identifying information from any potential target. It is derived from "fishing" for information. Attackers indiscriminately send phishing emails as spam without knowing who will get them, but they hope some users

will respond. Phishing emails sometimes inform the user of a bogus problem and say that the company will lock the user's account if the user doesn't act.

Spear Phishing

Spear phishing is a more targeted form in which the message is crafted and explicitly directed to a group of individuals. Often, attackers use a stolen customer database to send false messages crafted to seem like communication from the compromised business but with falsified source addresses and incorrect URI/URLs. The attacker hopes that someone who already has an online or digital relationship with an organization is more likely to fall for fake communication.

Some abusive concepts to watch out for are requests to pay bills or invoices using prepared gift cards, changes to wiring details (especially at the last minute), or requests to purchase products that are atypical for the requester and needed in a rush.

Whaling

Whaling is a form of spear phishing that targets specific high-value individuals (by title, by industry, from media coverage, and so forth), such as the CEO or individuals with known high-paying positions. Whaling attacks require significantly more research, planning, and development by the attackers to fool the victim.

Smishing

Short Message Service (SMS) phishing or *smishing* (spam over instant message [SPIM]) is a social engineering attack that occurs over or through standard text messaging services. There are several smishing threats to watch out for, including these:

- Text messages asking for a response or reply. In some cases, replies could trigger a cramming event. Cramming is when a false or unauthorized charge is placed onto your mobile service plan.
- Text messages could include a hyperlink / URI / URL to a phishing or scam website or trigger the installation of malicious code.
- Text messages could contain pretexts to get you involved in a conversation.
- Text messages could include phone numbers. Always research a phone number before calling it, especially from an unknown source.

Although smishing refers to SMS-based attacks, it can sometimes be used to refer to similar attacks occurring through Multimedia Messaging Services (MSS), Rich Communication Services (RCS), Google Hangouts, Android Messenger, Facebook Messenger, WeChat, Apple / iPhone iMessage, WhatsApp, Slack, Discord, Microsoft Teams, and so on.

Vishing

Vishing (e.g., voice-based phishing) or SpIT (Spam over Internet Telephony) is done over any telephony or voice communication system. This includes traditional phone lines, voice-over-IP (VoIP) services, and mobile phones. Most social engineers waging vishing campaigns use VoIP technology to support their attacks. VoIP allows the attacker to be located anywhere in the world, make free phone calls to victims, and falsify or spoof their original caller ID.

Vishing calls can display a caller ID or phone number from any source the attacker thinks might cause the victim to answer the call. Some attackers just duplicate your area code and prefix to trick the victims into thinking the call is from a neighbor or other local entity. Vishing is simply another form of phishing attack. It involves pretexting the displayed caller ID and the story of the attacker spouts. Always assume caller ID is false or at least incorrect.

Spam

Spam is any undesired and unsolicited email. However, spam is not just unwanted advertisements; it can also include malicious content and attack vectors. Spam is often used as the carrier of social engineering attacks.

Spam is a problem for numerous reasons:

- Some spam carries malicious codes such as viruses, logical bombs, ransomware, or Trojan horses.
- Some spam carries social engineering attacks (hoax messages).
- Unwanted email wastes time while you sort through it, looking for legitimate messages.
- Spam wastes internet resources: storage capacity, computing cycles, and throughput.

The primary countermeasure against spam is an email spam filter. These email filters can examine a message's header, subject, and contents to look for keywords or phrases that identify it as a known type of spam and then take the appropriate actions to discard, quarantine, or block the message.

> *Baiting* is a social engineering attack wherein scammers make false promises to users to lure them into revealing personal information or installing malware on the system.
>
> Baiting scams can involve tempting ads or online promotions, such as free games or movie downloads, music streaming, or phone upgrades. The attacker hopes the target's password to claim the offer is one they have used on other sites. This can allow the hacker to access the victim's data or sell the information to other criminals on the dark web.

Invoice Scams

Invoice scams are social engineering attacks that often attempt to steal funds from an individual by presenting a false invoice, usually followed by strong inducements to pay. Attackers try to target members of financial departments or accounting groups. Some invoice scams are spear phishing scams in disguise. It is also possible for a social engineer to use an invoice scam approach over a voice connection.

Hoax

A *hoax* is a form of social engineering designed to convince targets to perform an action that will cause problems or reduce their IT security. A hoax can be an email proclaiming that an imminent threat is spreading across the internet and that you must perform specific tasks to protect yourself.

Impersonation and Masquerading

Impersonation is the act of taking on someone else's identity. It can occur in person, over the phone, through email, logging into someone's account, or any other means of communication. Impersonation can also be masquerading, spoofing, and even identity fraud. In some circumstances, impersonation is defined as a more sophisticated and complex attack, whereas masquerading is amateurish and simpler.

Dumpster Diving

Dumpster diving involves digging through trash, discarded equipment, or abandoned locations to obtain information about a target organization or individual. Items typically collected include old calendars, calling lists, handwritten meeting notes, discarded forms, product boxes, user manuals, sticky notes, printed reports, or test sheets from a printer.

Identity Fraud

Identity fraud and identity theft are terms that are often used interchangeably.

Identity *theft* is the act of stealing someone's identity. Specifically, this can refer to the initial act of information gathering or elicitation where usernames, emails, passwords, answers to secret questions, credit card numbers, Social Security numbers, healthcare services numbers, and other related and relevant facts are stolen or otherwise obtained by the attacker. Identity theft is the actual theft of the credentials and information for someone's accounts or financial positions.

A second definition of identity theft is when credentials and details are used to take over someone's account. This could include logging into their account on an online service, making false charges to their credit card, ATM card, or debit card, writing false checks against their checking accounts, or opening a new line of credit in the victim's name using their Social

Security number. When an attacker steals and uses a victim's credentials, this is known as credential hijacking.

This second definition of identity theft is very similar to the definition of identity fraud. Identity fraud is when you claim something false to be accurate, falsely claiming to be someone else by using stolen information from the victim. It is criminal impersonation or intentional deception for personal or financial gain.

Identity theft and fraud are forms of spoofing. Spoofing is any action to hide a valid identity, often by taking on someone else's identity. In addition to human-focused spoofing (i.e., identity fraud), spoofing is a common tactic for hackers against technology. Hackers often spoof email addresses, IP addresses, media access control (MAC) addresses, Address Resolution Protocol (ARP) communications, Wi-Fi networks, websites, mobile phone apps, and more.

Identity theft and identity fraud are also related to impersonation. Impersonation is the act of taking on someone's identity. This might be accomplished by logging into their account with stolen credentials or claiming to be someone else when using the phone.

Typo Squatting

Typo squatting captures and redirects traffic when a user mistypes an intended resource's domain name or IP address. This social engineering attack takes advantage of a person's potential to mistype a fully qualified domain name (FQDN) or address. A malicious site squatter predicts URL typos and then registers those domain names to direct traffic to their site. This can be done for competition or malicious intent.

URL hijacking can also refer to displaying a link or advertisement that looks like that of a well-known product, service, or site but, when clicked, redirects the user to an alternate location, service, or product. This may be accomplished by posting sites and pages and exploiting search engine optimization (SEO) to increase your content in search results or using adware that replaces legitimate ads and links with those leading to alternate or malicious locations.

Clickjacking redirects a user's click or selection on a web page to an alternate, often malicious, target instead of the intended and desired location. This can be accomplished through several techniques. Some alter the code of the original web page to include a script that will automatically replace the valid URL with an alternate URL when the mouse clicks or selection occurs.

Another method is to add an invisible or hidden overlay, frame, or image map over the displayed page. The user sees the original page, but any mouse clicks or selections will be captured by the floating frame and redirected to the malicious target. Clickjacking can be used to perform phishing attacks, hijacking, and on-path attacks.

Influence Campaigns

Influence campaigns are social engineering attacks that attempt to guide, adjust, or change public opinion. Although hackers might undertake such attacks against individuals or organizations, most influence campaigns are waged by nation-states against their actual or perceived foreign enemies.

Influence campaigns are linked to the distribution of disinformation, propaganda, false information, “fake news,” and even the activity of doxing. Misleading, incomplete, crafted, and altered information can be used in an influence campaign to adjust readers' and viewers' perceptions of the influencer's concepts, thoughts, and ideologies.

Doxing is the collection of information about an individual or an organization (which can also include governments and the military) and the disclosure of the collected data publicly to change the perception of the target. Doxing can consist of withholding information that contradicts the attacker's intended narrative. It can also fabricate or alter information to place false accusations against the target.

Cybersecurity Attacks

A cyberattack is an individual or organization's malicious and deliberate attempt to breach another individual's information system. Usually, the attacker seeks some benefit from disrupting the victim’s network.

Cyberattacks can take many forms. Cybercriminals use various methods to gain unauthorized access to computers, data, and networks and steal sensitive information.

Here's an overview of common cybersecurity threats:

Malware (Malicious Software)

Malware is malicious software designed to disrupt, damage, or gain unauthorized access to a system. Different forms of malware exist, including Trojans, viruses, and worms, and they all reproduce and spread through a computer or network. This allows the hacker to gain deeper access to the target network to steal data, damage devices, render networks inoperable, or take control of systems.

- Worms: Self-replicating malware that spreads without user interaction.
- Trojan Horses: Disguised as legitimate software to steal data or harm systems.
- Ransomware: Encrypts data and demands payment for decryption.
- Spyware: Secretly gathers user information.
- Adware: Displays unwanted ads and can collect user data.

Wiper malware (i.e., wipers) damages organizations by wiping as much data (if not all) as possible. Unlike ransomware, which has financial motives, wiper attacks are purely disruptive. Criminals may also use wiper attacks to cover the tracks of separate data thefts.

Wipers often target files, backups, and the system boot section. Commonly, hackers override files to destroy them, but they don't do this in wiper attacks because it's time-consuming. Instead, hackers write a certain amount of data at intervals, randomly destroying files.

Phishing

Phishing attacks are deceptive attempts to steal sensitive information, such as passwords or credit card numbers, often via fraudulent emails or websites. A phishing attack tricks a target into downloading malware or entering sensitive information into spoofed websites. These cyber-attack methods are typically launched via email, with the attacker creating legitimate messages that may appear to be from a trusted sender. However, they will contain malware within an attachment or a malicious hyperlink that takes the recipient to a fake website that asks them to enter their login credentials or banking details.

Some phishing attacks take a blanket approach to try and catch as many victims as possible, but others are highly targeted and carefully researched to steal data from valuable individuals. Phishing is not restricted to email, however, as attacks increasingly target mobile devices.

- Description: Spear phishing (targeted attacks)
- Whaling (targeting high-profile individuals)

Ransomware

Ransomware attacks are a financially motivated form of malware. Attackers send messages containing a malicious attachment that, when downloaded, encrypts specific data and files or entire computers. The attacker then demands a ransom fee from the victim and will only release or restore access to the data upon payment.

Impact: This can cause significant financial loss and operational disruption.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

A *denial-of-service (DoS) or brute-force attack* is designed to prevent online services from working efficiently. It is typically caused by an attacker flooding a website with vast amounts of traffic or requests to overwhelm its systems and take them offline. A more advanced DoS form is a distributed denial-of-service (DDoS) attack, through which an attacker takes control of several computers to overload its target.

Target: Often aimed at websites, servers, or online services.

Man-in-the-Middle (MITM) Attacks

Man-in-the-middle attacks intercept communication between two parties to steal data or inject malicious content. An example is an attacker creating a spoofed, free-to-access Wi-Fi network. When the user connects to or signs in to the network, the attacker can steal the login credentials and data they use while on it.

Common Targets: Public Wi-Fi networks and unencrypted connections.

SQL Injection

Attackers use *Structured Query Language (SQL) injections* to exploit vulnerabilities and seize database control. Many websites and web applications store data in SQL to share user data with databases. If an attacker spots a vulnerability in a webpage, they can perform an SQL injection to discover user credentials and mount a cyber-attack.

These are attacks where malicious SQL code is inserted into a database query, allowing attackers to manipulate or steal data. In some cases, they may be able to alter and add data within a database, delete records, transfer money, and even attack internal networks.

Zero-Day Exploits

Zero-day attacks target unknown vulnerabilities in software or hardware that developers have not yet discovered and have not been able to fix or patch. Once an attacker spots a code vulnerability, they create an exploit that enables them to infiltrate the business before it realizes a problem. They are then free to collect data, steal user credentials, and enhance their access rights within an organization.

Attackers can often remain active within business systems for months and even years without being noticed. Zero-day vulnerability exploit techniques are commonly available on the Dark Web, often for purchase by government agencies for hacking purposes.

Impact: This can be challenging to detect and defend against.

DNS Tunneling

DNS tunneling is a cyber-attack method that targets the Domain Name System (DNS), a protocol that translates web addresses into Internet Protocol (IP) addresses. DNS is widely trusted, and because it is not intended for transferring data, it is often not monitored for malicious activity. This makes it a compelling target to launch cyber-attacks against corporate networks.

One such method is DNS tunneling, which exploits the DNS to tunnel malicious data and malware. It begins with an attacker registering a domain with the name server pointing to the attacker's server, which has a tunneling malware program installed. The attacker infiltrates a

computer and is free to send DNS requests through their server, which establishes a tunnel they can use to steal data and other malicious activities.

Cryptojacking

A *cryptojacking* attack occurs when a bad actor takes control of a computer, mobile device, or server to mine for online currency or cryptocurrency. The attack either begins with malware being installed on a computer or by running code in JavaScript to infiltrate the user's browser.

Cryptojacking is financially motivated, and the method is designed to remain hidden from the target while using their computing resources to mine cryptocurrency. The only sign of cryptojacking is often a loss or reduction in computer performance or overactive cooling fans.

Impact: Slows down systems and increases energy consumption.

Trending Cybersecurity Attacks

Information Stealer

Information stealers are malicious programs designed to collect personal and financial information from an infected system. They can capture keystrokes, extract files, and steal browser data like passwords and cookies. Information stealers generate large amounts of DNS traffic because they exfiltrate data from a compromised organization.

It is typically delivered via email and malvertising campaigns, either directly or via exploit kits and loader malware; recent research suggests that some cybercriminal groups are targeting the gaming community, leveraging fake Web3 gaming lures to deliver malware capable of stealing sensitive information from macOS and Windows users.

Impact: Harvest a wealth of sensitive data highly valued on the black market.

Trojans

Trojans are a type of malware that misleads users of their true intent. They are often disguised as legitimate software. Another common installation tactic is when a user gets a malicious link, like an email attachment disguised as an invoice, that, once clicked on, can silently install a Trojan. Once activated, Trojans can enable cybercriminals to spy on you, steal sensitive data, and gain backdoor access to your system.

Trojans remain a common threat due to their deceptive nature and ability to hide in the background while performing malicious activities. They are an effective means for attackers to gain unauthorized access to systems, deliver additional malware, and create backdoors. The ease with which Trojans can be spread through social engineering and software vulnerabilities contributes to their ongoing prevalence in our threat reports.

Ransomware

Ransomware is malware that encrypts files on a victim's computer or network, making them inaccessible and demanding a ransom payment to decrypt them. Victims are often threatened with permanent data loss or exposure to stolen data if the ransom isn't paid.

> Ransomware as a service (RaaS) is a growing cybercrime business model in which ransomware developers sell ransomware code or malware to other hackers, called "affiliates," who then use the code to initiate ransomware attacks. RaaS arrangements are popular with cybercriminals.

Remote Access Trojans (RAT)

Remote access trojans (RATs) are malware that provides a back door for administrative control over the targeted computer. RATs enable intruders to do almost anything on the targeted computer, such as monitoring user behavior, accessing confidential information, activating the system's webcam, and distributing more malware.

RATs are favored tools for cybercriminals and espionage because they provide deep access to compromised systems. They enable stealthy surveillance, data exfiltration, and complete control over victim machines, often remaining undetected for extended periods. The difficulty in detecting RATs and their multifunctional use in targeted attacks ensure their persistence in threat landscapes.

Advanced Persistent Threats (APTs)

Advanced persistent threats are complex, sophisticated threats that target specific entities (like organizations or nations) intending to steal information or disrupt operations. These threats are persistent, often remaining undetected in a network for a long time, and are carried out by well-funded cybercriminals or state-sponsored groups.

APTs remain prevalent because they are sophisticated, targeted, and stealthy, often backed by nation-states or well-funded entities. Their long-term focus on espionage and intellectual property theft, combined with their ability to remain undetected within networks for months or years, makes them a continually evolving and persistent threat in cybersecurity.

Botnet

A botnet is a network of infected computers, known as bots, controlled by a threat actor (often called a "botmaster"). These compromised computers can be controlled remotely to perform malicious activities such as launching Distributed Denial-of-Service (DDoS) attacks, sending spam emails, stealing data, or spreading malware without the owners' knowledge.

Botnets remain a prevalent cyber threat due to their ability to rapidly propagate across many devices, including insecure Internet of Things (IoT) devices, and their versatility in executing

various malicious activities, such as DDoS attacks and data theft. Because of their decentralized command and control structures and stealthy operation, botnets are challenging to detect and dismantle.

Impact: Exploiting weakly secured connected devices like smart home gadgets, cameras, or industrial controls.

Dropper

A dropper is a malware designed to install other malware onto a target system. It does not typically harm the system; instead, it aims to evade detection and establish a foothold from which it can discreetly download and execute other malicious programs.

Droppers are still commonly reported as they play a crucial role in multi-stage malware attacks by facilitating the discreet delivery of payloads. Their ability to bypass initial security measures and install more destructive malware makes them a persistent tool in the cybercriminal arsenal. As droppers evolve to evade detection, their use in facilitating complex malware infections keeps them relevant.

Backdoor

A backdoor is a method by which unauthorized users bypass standard authentication and gain remote access to a computer or network. It may be an installed software or a built-in feature of the hardware or software.

Backdoors remain a significant threat, providing attackers with ongoing, unauthorized access to compromised systems. Their stealth and persistence enable long-term exploitation of data breaches, surveillance, or malicious activities. The strategic placement of backdoors within software or systems, often through supply chain compromises, makes them a challenging threat to eliminate and a consistent concern for organizations.

Emerging Cybersecurity Threats

Third-party Exposure

Cybercriminals can get around security systems by hacking less-protected networks belonging to third parties with privileged access to the hacker's primary target. This type of cyberattack is hazardous as many third parties tend to be much less secure than the major companies they work with.

Artificial intelligence (AI) and Machine Learning

AI has undoubtedly changed the game when it comes to cyber threats. Attackers increasingly leverage artificial intelligence (AI) and machine learning (ML) to enhance their capabilities. These technologies automate attacks, create more convincing phishing emails, and even identify vulnerabilities in target systems.

With all this said, artificial intelligence hasn't been bad news for cybersecurity; it has improved capabilities in recent years. Security systems that utilize AI have improved threat detection, are more automated, and can even point out weak points in the system.

As AI and ML advance, their role in digital threats will likely grow.

Drive-By Cyber Attacks

Another significant cybersecurity threat is "drive-by" attacks. These occur when you navigate to a compromised webpage that silently downloads malicious software onto your device. Hackers can do this by compromising weak site security and introducing malware code. The malware is downloaded without the user's knowledge; generally, the user won't need to authorize anything for the download to occur.

Some drive-by cyberattacks disguise themselves as fake advertisement pop-ups. When a user attempts to click on the X to close the pop-up, the malware is authorized to download onto the device.

Internet of Things (IoT)

The Internet of Things (IoT) is one of the significant technological revolutions of the 21st century. It is a network of interconnected "things," including appliances, vehicles, devices, and sensors.

The expansion of IoT gadgets has ushered in fresh susceptibilities within the digital threat environment. Numerous IoT devices exhibit insufficient security capabilities, rendering them susceptible to exploitation by malicious actors. These IoT devices can be harnessed when compromised to initiate extensive Distributed Denial of Service (DDoS) assaults or breach home networks.

The proliferation of 5G networks ushers in a new era of interconnectedness, particularly with the Internet of Things (IoT). While offering unprecedented connectivity, this also exposes IoT devices to vulnerabilities from external threats and software bugs. The nascent nature of 5G architecture necessitates extensive research to identify and address potential security loopholes.

While the connectivity of IoT allows for unthinkable automation and control of these devices, it also opens the door to new unforeseen cyber threats. As Internet of Things (IoT) devices grow, ensuring robust security measures becomes increasingly important.

Supply Chain Attacks

Another emerging trend is the rise of supply chain attacks, where attackers target supply chains to compromise the integrity of products and services. Recent incidents, such as the SolarWinds hack, have demonstrated the devastating impact of supply chain attacks, as they can affect organizations and their customers.

Safeguard and Preventative Measures

Cyber threats will continue to grow in sophistication, but with awareness and proactive measures, you can significantly reduce your family's risk. Protecting your digital life starts with adopting good cybersecurity practices that become habits or are performed regularly.

One way almost every family member can help maintain proper cyber hygiene is to mitigate risk.

How to Protect Your Family

- **Educate Family Members**: Teach family members about safe online practices, such as strong password management, phishing awareness, and not sharing personal information readily.
- **Use Strong Passwords**: Combine letters, numbers, and symbols and store them securely in a password manager.
- **Enable Multi-Factor Authentication (MFA)**: Add an extra layer of security to accounts.
- **Update Software Regularly**: Install updates on all devices, primarily operating systems, browsers, and apps, promptly to fix vulnerabilities.
- **Install Security Software**: Use reputable antivirus, anti-malware, and firewall programs on all devices.
- **Secure Your Wi-Fi Network**: Change default router settings, enable WPA3 encryption, and create a strong password. Consider using a guest network for visitors.
- **Monitor Children's Online Activity**: Use parental controls with appropriate restrictions and educate children on recognizing scams.
- **Be Skeptical**: Teach family members to verify links and emails before clicking or providing information. The refrain “trust but verify” is a good refrain.
- **Back Up Data**: Regularly back up essential files to an external drive or secure cloud storage.
- **Avoid Public Wi-Fi for Sensitive Tasks**: Use a VPN to access sensitive information on public networks.
- **Consider Cybersecurity Insurance**: Explore insurance options that may cover losses related to cybercrime.

Glossary of Terms

An ***attack*** occurs when a threat agent exploits a vulnerability to damage, lose, or disclose assets.

An ***exploit*** (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware, such as spyware, ransomware, Trojan horses, worms, or viruses.

Exposure is susceptible to asset loss because of a threat; there is the possibility that a vulnerability can or will be exploited by a threat agent or event. It doesn't mean that a realized threat (an event that results in loss) is occurring, just that *there is the potential for harm to occur*.

Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset and the severity of damage that could result.

A ***safeguard***, security control, protection mechanism, or countermeasure removes or reduces a vulnerability or protects against one or more specific threats.

Threats are any potential occurrence that may cause an undesirable or unwanted outcome.

Threat actors, or threat agents, intentionally exploit vulnerability. They are generally people but could be programs, hardware, or systems.

Threat events are accidental occurrences and intentional exploitations of vulnerability.

An ***attack vector*** is a method that cybercriminals use to gain unauthorized access to a network, system, or application.

Vulnerability is a flaw, loophole, oversight, error, limitation, frailty, or susceptibility that enables a threat to cause harm.