**UNDERSTANDING CYBERSECURITY: PROTECTING USERS AND COMPANIES AGAINST CYBER SECURITY THREATS**

**Group Leader:**

Adriano, Liam Andre

**Group Members:**

Ogalino, John Derick

Rapay, Regis

Sanchez, Jamaica Ann

**Submitted to:**

Amador, Peragrino B.

**A.Y. 2022 - 2023**

**INTRODUCTION AND BACKGROUND OF THE TECHNOLOGY**

The term "cybersecurity" describes a group of methods used to safeguard the integrity of networks, programs, and data against damage, assault, or illegal access.

Security from the perspective of computing includes both cybersecurity and physical security, both of which are employed by businesses to prevent illegal access to data centers and other computerized systems. Cybersecurity is a subset of information security, which aims to protect the availability, confidentiality, and integrity of data. Utilizing cyber security may assist manage risk and avoid cyberattacks, data breaches, and identity theft.

Therefore, one may ask "What are we trying to protect ourselves against? " while discussing cybersecurity.The three key areas we are attempting to govern are as follows:

* Unauthorized Access
* Unauthorized Deletion
* Unauthorized Modification

These three phrases are interchangeable with the well-known CIA triad, which stands for availability, confidentiality, and integrity. The majority of an organization's security policies are based on these three principles, which are also known as the CIA triad or the three pillars of security.

**THE CIA TRIAD**

The Confidentiality, Integrity, and Availability (CIA) triangle is a design framework that helps businesses and organizations create their security policies. To prevent confusion with the Central Intelligence Agency (CIA), it is alternatively referred to as the AIC trio. The triad's elements are seen to be the most crucial and essential parts of security. So allow me to give you a quick overview of the three parts.

**Confidentiality**

Protection of personal data is confidentiality. Confidentiality refers to not disclosing client information to anybody else, including coworkers, friends, family, etc.

**Integrity**

When referring to computer systems, the term "integrity" describes procedures for guaranteeing that data is authentic, correct, and protected against unauthorized user alteration.

**Availability**

In the context of a computer system, availability refers to a user's ability to access data or resources in the right place and format.

**OBJECTIVES OF THE TOPIC**

The topic assigned to the group aims to provide a comprehensive understanding of cybersecurity, especially it seeks:

* to explain the importance of security and privacy for computer users in relation to computing devices, networks, and the Internet.
* to discuss online theft, identity theft, spoofing, phishing, and other types of dot cons and detailed steps to protect against these threats.
* to identify personal safety risks associated with Internet use and list steps to protect against them.
* to describe privacy concerns regarding databases, electronic profiling, spam, and telemarketing and identify ways to protect privacy.
* to discuss types of electronic surveillance and monitoring and list ways to protect privacy.

**SCOPE OF THE TOPIC**

The arena of information technology has taken up and overwhelmed almost every component of our livelihood. Be it one’s social life or working space or personal life- everything has been taken over and is thus controlled by information technology.

This has also made our life a lot easier than it used to be. We do not have to remember numerous phone numbers or bank details anymore and rely on the system.

But with ease comes hand in hand, risk. The risk of our private information being compromised to people or groups with ill intentions stays. This is where the role of cyber security comes.

**Table of Contents**

[Pros of Cyber Security](https://thenextfind.com/pros-cons-of-cyber-security/#Pros_of_Cyber_Security)

·  [Protection from Unwanted Programs](https://thenextfind.com/pros-cons-of-cyber-security/#Protection_from_Unwanted_Programs)

·  [Denies Unauthorized Access](https://thenextfind.com/pros-cons-of-cyber-security/#Denies_Unauthorised_Access)

·  [Prevents Hacking](https://thenextfind.com/pros-cons-of-cyber-security/#Prevents_Hacking)

·  [Minimized Data Theft Hazard](https://thenextfind.com/pros-cons-of-cyber-security/#Minimized_Data_Theft_Hazard)

·  [Reduces Computer Crash](https://thenextfind.com/pros-cons-of-cyber-security/#Reduces_Computer_Crash)

·  [Increase in Cyber Defence](https://thenextfind.com/pros-cons-of-cyber-security/#Increase_in_Cyber_Defence)

·  [Detection and Deletion of Harmful Programs](https://thenextfind.com/pros-cons-of-cyber-security/#Detection_and_Deletion_of_Harmful_Programs)

·  [Deny Access from Possible Threat](https://thenextfind.com/pros-cons-of-cyber-security/#Deny_Access_from_Possible_Threat)

·  [Improves Stakeholder Confidence](https://thenextfind.com/pros-cons-of-cyber-security/#Improves_Stakeholder_Confidence)

·  [Faster Recovery](https://thenextfind.com/pros-cons-of-cyber-security/#Faster_Recovery)

[Cons of Cyber Security](https://thenextfind.com/pros-cons-of-cyber-security/#Cons_of_Cyber_Security)

·  [Difficult to Set Up](https://thenextfind.com/pros-cons-of-cyber-security/#Difficult_to_Set_Up)

·  [Constant Need to Update the Security](https://thenextfind.com/pros-cons-of-cyber-security/#Constant_Need_to_Update_the_Security)

·  [Expense of Setting up The Whole System](https://thenextfind.com/pros-cons-of-cyber-security/#Expense_of_Setting_up_The_Whole_System)

·  [Security Patches May Back-Fire](https://thenextfind.com/pros-cons-of-cyber-security/#Security_Patches_May_Back-Fire)

·  [New Update Might Not Suit Your System](https://thenextfind.com/pros-cons-of-cyber-security/#New_Update_Might_Not_Suit_Your_System)

·  [Makes the System Slower](https://thenextfind.com/pros-cons-of-cyber-security/#Makes_the_System_Slower)

·  [Incorrectly Configured System Blocks Firewall](https://thenextfind.com/pros-cons-of-cyber-security/#Incorrectly_Configured_System_Blocks_Firewall)

**Advantages of Cyber Security**

**Protection From Unwanted Programs**

The Internet is an open space where all kinds of programs go about, even the ones that are very harmful to our system. Cyber security provides protection against all these programs, viruses, malware, spyware that can make our gadgets compromise information.

**Denies Unauthorized Access**

No company or individual would want their strategy or exclusive plans to go into the hands of any other individual or organization who might use this information to their benefit and against the former party. Cybersecurity helps achieve this and denies access to anyone who might not be trying to access information through the front door.

**Prevents Hacking**

Hacking is one of the main vices of the internet and information technology combined. Though hacking is both ethically and legally unacceptable, the finest of hackers can break through the defenses of a system and exploit the weaknesses of the system. Cyber security puts up a strong defense against these hackers and protects the computer.

**Minimized Data Theft Hazard**

Cyber security ensures that no unauthorized or malicious user can gain access to the system. It implements such a high-security protocol that protects the user against any major data theft and makes the experience a lot more relieving.

**Reduces Computer Crash**

Crashing computers and freezing screens and two of the main hindrances of working with technology. Many times people working with tight deadlines face these problems that put their work-life at risk. Cyber security helps diminish these problems and lower the hindrance of working with technology.

**Increase In Cyber Defence**

Every organization or company tries its best to maximize the security of its exclusive data. The defense posed by mere antivirus or such software might be easy to breakthrough. Whereas a full-fledged defense of a cyber security program strengthens the defense and lets the user work from a safe space.

**Detection And Deletion Of Harmful Programs**

If the cyber security system finds any malware, spyware or virus in the files that were present even before the installation of the security system, it immediately takes it upon itself to detect them and ultimately delete them to remove any threat to the system.

**Deny Access From Possible Threat**

Cyber security does not allow any access that might pose even the slightest threat to the system. It not just denies access to a possible threat and saves the hazard, it also notifies the user of the possible threat so that the user can build the defenses to be stronger.

**Improves Stakeholder Confidence**

If your company can showcase greater cyber security and defense against malpractices, it is bound to give your company a boost about fulfilling stakeholders’ confidence in your company and hence, make them invest more.

**Faster Recovery**

In cases of disruption of the system, implementing a cyber security system ensures a faster recovery and stable continuity of the business operation, which is a savior as otherwise, it would result in total disruption and ultimately cessation of the business operation for the time being.

**Disadvantages of Cyber Security**

**Difficult To Set Up**

A cyber security system is difficult to set up for an average user. It requires professional technical knowledge and a professional to implement them and make them work. Thus, random installation of cyber security by regular people is not possible which makes it harder for the system to reach the masses.

**Constant Need To Update The Security**

Technology advances every minute and so does the security system. The user has to keep in mind to update his security system regularly to keep his device safe. Any missed update can put the whole system at a huge risk and compromise it.

**Expense Of Setting Up The Whole System**

Cyber security systems might be convenient to set up for the big farms, companies, and organizations, but not for individuals who might possess sensitive data that needs to be protected. The hindrance is the huge expense that is associated with it.

**Security Patches May Back-Fire**

When your content management system releases a new security update or patch, hackers can compare the patched and unpatched files to know the weaknesses that are mended in the patched file. Then they can attack the files that are unpatched. Hence, the security patches may backfire on the very system it was meant to secure.

**New Update Might Not Suit Your System**

When a new update is installed, a lot of the workings do not happen as they were meant to be. Thus, time is required to work around the system and make it function as it was intended to while complying to the security system.

**Makes The System Slower**

Better security is synonymous with a greater number of passwords and more and more checking of the files by the security system, all of which takes time and thus slows down both the system and the productivity of the person working.

**Incorrectly Configured System Blocks Firewall**

If the firewall is configured incorrectly, it blocks certain services and actions of the user. This stays until the firewall is configured correctly, which requires the intervention of a professional, thus making it hard to work with a person who is not familiar with the technology.

Cyber security might still have a lot of loopholes that are being constantly worked upon, but then it is our best bait at saving our information from hackers and other ill users of technology.

**PRESENTATION OF THE CHOSEN TECHNOLOGY**

**a.) Uses and Functions.**

Cybersecurity is a broad topic, covering many different disciplines, actions, threats and ideas. However, these parts come back to the same idea: protecting people’s digital lives and assets. Things like digital currency, data and access to some computers are valuable targets for criminals, so protecting them is crucial.

Consider the variety of modern uses for data and digital technology. There are many different kinds of cybersecurity because it is such a broad area. Here are a few illustrations:

* **Network security:** Protects computer networks like home Wi-Fi or a business’s network from threats
* **Application security**: Ensures programs and apps repel hackers and keep users’ data private
* **Cloud security:** Focuses on the cloud, where users and businesses store data and run apps online using remote data centers
* **Information security**: Focuses on keeping sensitive data safe and private
* **Endpoint security**: Secures devices like computers, phones or Internet of Things (IoT) gadgets to ensure they don’t become a way to get into other devices or data on a network.

These cybersecurity examples are far from the only types, but they’re some of the biggest. As the field grows, many smaller, more specialized subcategories emerge. All these smaller considerations combine to create an organization’s overall cybersecurity.

## **Top 5 cybersecurity threats to manage**

Just as there are many types of cybersecurity, there are multiple cybersecurity threats. Here’s a look at some of the most common and dangerous ones facing businesses and individuals today.

**1. Malware**

Despite a gradual drop over the past few years, malware remains one of the most prevalent categories of cybersecurity risks. It stands for "malicious software" and is a catch-all term for programs and lines of code that harm or grant illegal access.

Malware includes viruses, trojan horses, spyware, and ransomware, among others. These might be as little as installing annoying pop-up windows on a computer or as risky as collecting private information and transmitting it to another location.

**2. Phishing**

Phishing exploits human weaknesses whereas malware depends on technical aspects to do harm. These assaults entail deceiving a victim into disclosing private information or clicking on anything that may infect their device with malware. They frequently serve as the launch pad for more significant attacks.

Phishing frequently takes the form of emails in which fraudsters pretend to be high-ranking individuals or to have exciting news to share. These messages frequently make use of people's worries or wants to persuade them to behave hastily and mindlessly. For instance, many claim that the users have won awards or have run into legal issues.

### **3. Insider threats**

The majority of cybersecurity threats originate from the outside of a company, but some of the most serious ones do as well. Insider threats occur when a system is threatened, whether intentionally or not, by someone with authorized access, such as an employee.

Numerous insider dangers are benign. This occurs when a legitimate person unknowingly puts a system at risk by falling for phishing or posting on the wrong account. Some people may intentionally do something, such as a dissatisfied ex-employee who infects their former employer's computers with malware to exact revenge.

**4. Man-in-the-middle attacks**

Cybercriminals can eavesdrop on communications by using man-in-the-middle (MITM) attacks, which include intercepting data as it moves between two places. They duplicate the data so it gets to its desired location rather than stealing it in the classic sense. As a result, it can appear as though nothing happened at all.

Malware, bogus websites, and even hacked Wi-Fi networks may all be used in MITM assaults. Despite not being as frequent as some, they are harmful since they are difficult to spot. Before they know it, a user may have entered personal information onto a website form that has been compromised.

**5. Botnets**

Another prevalent sort of cybersecurity danger is botnets. These are networks of several compromised computers that enable a single threat actor to attack utilizing numerous devices simultaneously. Attackers frequently use distributed denial-of-service (DDoS) techniques to bring down a system by flooding it with requests.

Attacks using botnets have significantly increased recently. Up from 35% just six months earlier, 51% of enterprises had discovered botnet activity on their networks as of June 2021. Massive damage can also be done by large-scale DDoS assaults, which might bring down vital services for a number of hours or even days.

## **Best practices for cybersecurity in 2022**

**1. Use anti-malware software**

Installing anti-malware software is among the most crucial cybersecurity best practices. There are several antivirus products and services available that can benefit customers of any financial standing. The best part is that these tools automate malware detection and prevention, so staying secure doesn't need you to be an expert.

This program can thwart a variety of attacks because malware is the origin of many cybersecurity concerns. Additionally, they often update, which aids in keeping up with new assault strategies. There is no excuse to avoid using them, given how simple they are to use and how important they are.

**2. Use strong, varied passwords**

Another crucial cybersecurity step is to use strong [passwords](https://venturebeat.com/2021/09/14/encrypted-passwords-and-a-virtual-private-network-are-two-ways-to-protect-yourself-from-cyberattacks/). Most hacking-related data breaches stem from weak passwords, which are easy to avoid. Cracking a 12-character password takes [62 trillion times longer](https://www.digitalinformationworld.com/2021/06/password-statistics-show-dire-state-of.html) than a six-character one.

Passwords should be long and contain numbers, symbols and varying letter cases. It’s also important to avoid using the same one for multiple accounts, as that lets a hacker into more places with one breached password. Changing them every few months can also minimize risks.

### **3. Enable multi-factor authentication**

Sometimes, a strong password isn’t enough. That’s why enabling multifactor authentication (MFA) is another essential cybersecurity best practice for employees and general users. MFA is quick to set up, easy to use and can stop nearly all attacks, according to some experts.

MFA adds another step to the login process, most often a one-time code sent to a user’s phone. Some MFA options are more advanced, like facial recognition services or fingerprint scanners. While these features may not see as much use as they should, they’re available on most internet services.

### **4. Verify before trusting**

Since cybersecurity risks sometimes don't appear odd at first look, it's crucial to confirm security. Examine anything more thoroughly before replying to an email or clicking a link. If it has grammatical problems, uses bizarre language, is unusually urgent, or otherwise appears wrong, it may be a trap.

The same idea holds true for internet networks, hardware, and software. Never put your confidence in free WiFi since it might be used for MITM attacks by anyone. Similar to this, before downloading and installing an application, be sure the developer is reliable. This should be applied to commercial partners as well.

### **5. Update frequently**

Cybersecurity is a dynamic field. Criminals are always coming up with new ways to attack targets and cybersecurity tools adapt in response. That means it’s crucial to update all software regularly. Otherwise, users could be vulnerable to a weak point that app developers have already patched.

Some of the most infamous cybersecurity breach examples have happened because of outdated software. In 2019, the United Nations tried to [hide a data breach](https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack) that used a vulnerability a current software update would have patched. This is a critical cybersecurity best practice for businesses, which may be bigger targets.

**6. Wherever feasible, encrypt**

The encryption of sensitive data is a further technological cybersecurity measure. By encrypting data and providing a key to authorized users, encryption renders information unreadable to anybody but the intended audience. Although it doesn't stop data breaches, it lessens their damage.

Data that a cybercriminal cannot read or interpret is useless to them and is thus a less desirable target. Additionally, it guarantees that any private information that spills will remain that way. Information is kept extra safe by using numerous encryption techniques, such as end-to-end and at-rest encryption.

### **7. Segment networks**

Network segmentation is a crucial security best practice for enterprises. This entails using many networks to run devices and store data so that a compromise in one place won't provide access to everything else. Large IoT networks especially need to be careful with this stage.

Although this phase can also be used by individuals, it usually relates to organizations. It's a good idea to connect smart home gadgets to a different network than your home or office PCs. In this manner, a smart TV, which is simpler to hack into, won't end up being a gateway to more delicate data.

### **8. Create backups of sensitive files**

It’s also crucial to back up any sensitive data or programs. This won’t prevent a cyberattack, but it will minimize the damage. Stolen data or downed systems aren’t as pressing if you have extra copies you can use.

With cybercrime as rampant as it is, it’s unsafe to assume someone will never be the target of a successful breach. More than [half of all consumers](https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf) have been the victim of cybercrime. Since no defense is perfect, ensuring a hack won’t be crippling is essential.

### **9. Stay informed and tell others**

Despite how massive a problem cybercrime is, many people don’t know cybersecurity best practices. Many simple steps can be effective. It’s just a matter of knowing what risks are out there and what to do about them. Consequently, staying informed is half the battle.

This step is an important cybersecurity best practice for employees especially. Businesses should train all workers about things like strong password management and how to spot a phishing attempt. Holding these meetings regularly can help companies stay on top of emerging threats and remain safe despite a changing landscape.

### **10. Review security steps regularly**

Every user and business should be aware that best practices today might not be applicable tomorrow. Since the subject of cybersecurity is always changing, it's crucial to assess defenses to make sure they remain effective. Without routine reviews, people can be exposed without realizing it.

Businesses can engage in penetration testing, in which a cybersecurity professional attempts to hack their systems to identify any vulnerabilities. To find out what additional precautions they might need to take, consumers can keep up on the most recent cybersecurity news. Being complacent is the worst thing you can do.

**b.) Importance and Benefits**

**The Importance of Computer Security**

Computer security measures are frequently overlooked until a problem manifests, at which time a breach in security can have detrimental effects and could have a significant impact. We provide answers to some commonly asked concerns concerning potential security vulnerabilities and how you can stop them from happening to you since we all want to keep our systems and information secure.

Computer security is important because it keeps your information protected. It’s also important for your computer’s overall health; proper computer security helps prevent viruses and malware, which allows programs to run quicker and smoother.

**c.) Unauthorized Access and Unauthorized Use**

In cybersecurity, unauthorized access refers to the use of a computer or network without permission. On the other hand, unauthorized use refers to the use of a computer or its data for unapproved or possibly illegal activities.

**Examples:**

**Tailgating:** This is when an unauthorized person follows an authorized individual to enter/access a secured area/information. Unauthorized use could include accessing sensitive areas of a building or stealing sensitive information. The following are some of the examples:

* A person pretends to be an employee and claims that they have forgotten their ID so that you can grant them access.
* Someone walks behind you into a secure area and expects you to keep the door open for them to enter right after you.
* Service providers, delivery persons, or painters who request access to authorized spaces.

**Hacking:** This can include internet or online account takeover like hacking into financial or bank account-related information. Unauthorized use could include stealing money or sensitive financial information. According to a report by IBM’s X-Force, ransomware attacks were the most common cyberattack in 2021, accounting for 21% of attacks. Ransomware is where a hacker steals an individual's computer data and essentially holds it hostage; they only release the data when they receive a ransom payment. Cybersecurity Ventures predicts that the cost of cybercrime will hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

**Illegal use/break of login and password:** This can include illegally using or breaking the login and password of other users. Unauthorized use could include accessing sensitive information or performing actions without permission. According to a 2019 study conducted by Google in conjunction with Harris Poll, 75% of Americans find maintaining and keeping track of their passwords frustrating. An estimated 81% of data breaches are due to poor password security.

**Here are several ways to protect against unauthorized access and use:**

**Implement strict access control measures:** This can include measures such as requiring employees to use keycards or badges to enter certain areas of a building.

**Monitor employee activity:** This can include monitoring employee computer activity and access logs to identify any suspicious behavior.

**Educate employees:** It’s important to educate employees on the importance of data security and the potential consequences of unauthorized access and use.

**Use strong passwords:** Make sure to use a personal password for all your accounts to prevent unauthorized access. Also, change passwords often and use a combination of letters, numbers, and symbols. Because according to Microsoft, using multi-factor authentication (MFA) can prevent 99.9% of account attacks.

**Keep software up to date:** Ensure that all software, including operating systems and applications, are kept up to date with the latest security patches to protect against cyberattacks.

**Use antivirus and anti-malware software:** Use antivirus and anti-malware software to protect against malware, including ransomware.

**Backup data regularly:** Regularly backup important data to protect against data loss in the event of a ransomware attack or other security breach.

**Run system scans to check for vulnerabilities:** Regularly run system scans to check for vulnerabilities in your system

**Know how to handle email:** Be cautious when opening emails from unknown senders and do not click on suspicious links or download attachments from unknown sources.

**Use a firewall:** Use a hardware or software firewall to protect against unauthorized access

Unauthorized access to company data and resources is a major concern for businesses. According to a report conducted by Dimensional Research, 32% of enterprises experienced unauthorized access to cloud resources, and another 19% were unaware if unauthorized access occurred. This was found to be largely driven by poor enforcement of identity and access management (IAM) policies in the cloud.

**d.) Computer Sabotage**

Computer sabotage is the act of intentionally destroying, altering, or disrupting computer systems or networks with malicious intent. It can be done by individuals or groups with the intention of causing harm to an organization or individual. The damage caused by computer sabotage can range from minor disruptions to complete system failure (such as data theft, data corruption, and denial of service attacks).

**EXAMPLES:**

**SolarWinds Attack**

In the SolarWinds attack, attackers took advantage of multiple vulnerabilities within the network which is a method known as a supply chain attack. A supply chain attack works by targeting a third party with access to an organization’s systems rather than trying to hack the networks directly. Companies can sidestep this issue by ensuring that their network perimeter stays secure by employing a strong, automated patch management solution that finds vulnerabilities and patches them before they result in a breach.

**Accellion's Attack**

In the Accellion attack, attackers infiltrated a company network through an affiliated partner, suppliers or any other party that would have access to the network. A robust patch management software solution that automatically searches for and patches vulnerabilities is a must for most organizations.

**Oldsmar Water Supply Attack**

In the Oldsmar water supply attack, hackers were able to access the operating systems via remote-access system TeamViewer—used by employees—and poor password hygiene and out-of-date software were suspected as the cause of the issue. Making sure credentials don’t become compromised is a critical part of overall strong password hygiene. You can do this by making them hard to guess and having them regularly rotated and changed whenever there’s a detected breach, as well as through the deployment of a password manager.

**Channel 9 News Attack**

In March 2021, hackers were successfully able to disrupt Australia’s Channel 9 News live broadcast, preventing the channel from airing several other shows and affecting 9 News’ print production. The confirmed ransomware attack, in addition to successfully taking shows off the air, also locked staff out of their emails, blocked their internet access, and halted print production systems. At the time, it was the largest cyber-attack on an Australian media company.

In the Channel 9 News attack, it was never made public or discovered what the root cause was, but admins suspected it was probably either due to vulnerabilities that hadn’t been patched or from a phishing email. Having strong anti-phishing solutions in place can prevent your employees from inadvertently downloading malicious code that acts as a gateway for a ransomware attack.

**Here are several ways to protect against computer sabotage:**

* **Install quality antivirus and firewall software:** Antivirus software is vital in defending your computer, mobile devices and data against computer vandalism, viruses, worms, Trojans and other malware. Firewalls are also important as they can help prevent unauthorized access to your computer or network.
* **Use only reliable networks:** If you often use public and open wifi networks, this can be a problem for your security. Hackers can easily intercept your data and steal your personal information. Use only reliable networks that you trust.
* **Don’t open spam:** You may often receive spam mails. These mails can contain malicious links or attachments that can infect your computer with malware.
* **Don’t download anything from dubious sites:** Downloading files from dubious sites can be dangerous as they may contain malware that can harm your computer.
* **Monitor systems for unexpected behaviors:** This is one of the best ways to protect against computer sabotage. Monitor systems for unexpected behaviors such as unusual network traffic or unauthorized access attempts.

**e.) Online Theft, Identity Theft, Spoofing, Phishing, and Other Types of Dot Cons**

**How Malicious Hackers Use Spyware to Steal Your Identity**

Even normal browsing activities like clicking on an enticing ad or filling out a form for downloadable content can lead to online identity theft when users don't know what to look for. Keyloggers can be overlaid on seemingly legitimate banking or investment apps and intrusive tracking procedures can be signed off on by users who fail to read terms and conditions notices carefully.

**You can encounter spyware and other forms of malware in many ways, including:**

* Downloading files or software
* Opening email attachments or clicking on pop-ups
* Visiting devious websites

**They use spyware to record and collect your personal information.**

Without your knowledge, spyware runs in the background while it records your Internet browsing habits and keystrokes, monitors the programs you use and collects your personal information, which can lead to credit card fraud and online identity theft.

**Spyware transmits your sensitive data, using your own internet connection.**

While your computer is connected to the Internet, spyware quietly transmits your personal information to cybercriminals, which can include:

* Credit card numbers
* Bank account numbers
* Social Security numbers
* Usernames and passwords
* Address books, including email addresses

**Cybercriminals use your information for illicit or illegal activities.**

Once your personal information is received by the hacker who placed spyware on your computer, they can now:

* Steal money and open credit card and bank accounts in your name
* Sell it to other parties who will use it for illicit or illegal purposes
* Pummel your PC with pop-ups, spam and unwanted messages as well as direct you to websites you never intended to visit

**How to Prevent Identity Theft**

Spyware used for online identity theft can be the most harmful and difficult to remove of any type of malware. Here are a few things that can help you improve your level of online identity theft security:

Continually check the accuracy of personal accounts and deal with any discrepancies immediately.

Avoid questionable websites.

Practice safe email protocol:

* Don't open messages from unknown senders
* Immediately delete messages you suspect to be spam

Only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them.

Get the latest Windows® patches.

Use public computers with extreme caution.

Use antivirus protection and a firewall.

The best identity theft protection begins by avoiding spyware infection in the first place. Virus protection products guard against spyware entering your computer and prevent it from exposing your personal data and slowing your computer through damage to your files and programs. A good anti spyware program searches every place on your PC where spyware can hide and removes every trace to boost your PC performance and keep you safe from intrusion. While free anti spyware downloads are available, they just can’t keep up with the continuous onslaught of new spyware strains. Previously undetected forms of spyware can often do the most damage to your computer, so it’s critical to have up-to-the-minute online identity theft protection.

**KEY TAKEAWAYS**

* Identity theft occurs when someone steals your personal information and credentials to commit fraud.
* There are various forms of identity theft, but the most common is financial.
* Identity theft protection is a growing industry that keeps track of people's credit reports, financial activity, and Social Security Number use.

**Spoofing and Phishing**

Remaining vigilant against cybersecurity threats such as phishing and spoofing attacks is crucial — no one is immune. Phishing and spoofing attacks are similar, but they are two distinct cybersecurity threats. Understanding the difference between phishing and spoofing and the dangers they pose can boost your cybersecurity awareness and help you protect your business.

**Spoofing vs Phishing**

Spoofing attacks resemble identity theft while phishing attacks attempt to steal sensitive information. Notably, a phishing attempt may begin with a spoofing attack. Phishing, however, is never part of spoofing.

**Definition of Spoofing**

In spoofing attacks, threat actors disguise themselves as legitimate sources to gain the victim’s trust. The intention behind a spoofing attack is to install malware and orchestrate further crimes with the information or access gained. Spoofing attacks can take many forms, including the following:

Email spoofing: The attacker creates an email address resembling that of a trusted sender by altering the “from” field to match a trusted contact or mimicking the name and email address of a known contact.

Domain or website spoofing: An attacker creates a fake website or email domain designed to impersonate a known business or person.

IP spoofing: Attackers alter their IP address in order to hide their real identity or impersonate another user via IP spoofing.

GPS spoofing: An attacker alters a device’s GPS to register in a location different from the user’s actual physical location.

Caller ID spoofing: The attacker disguises their phone number with one that is familiar to the victim, similar to the method in email spoofing.

**Definition of Phishing**

A phishing attack is a scam in which a threat actor sends generic messages in mass quantities, usually via email, in hopes of getting anyone to click on malicious links. The intent is usually to steal credentials or personal information, such as your social security number. Four of the most common types of phishing attacks are outlined below.

Spear phishing: This phishing attempt targets specific individuals or organizations with personal communication, typically through malicious emails, with the intent to steal sensitive information.

Whale phishing: A whaling attack is a social engineering attack specifically targeting senior or C-level executives in an attempt to steal money or information or gain access to the victim’s computer in order to execute further cyberattacks.

Voice phishing (vishing): Vishing is a phishing attack conducted by telephone.

SMS phishing (smishing): Smishing refers to phishing scams conducted through SMS messages, usually with the goal of luring the user to visit a website that entices them to download malicious apps or content.

**Differences Between Spoofing and Phishing**

It’s easy to see that spoofing attacks and phishing attacks are related yet distinct cybersecurity threats. Further examining the characteristics of each threat clarifies their differences.

**Purpose:** The goal of spoofing is to impersonate someone’s identity while the purpose of phishing attacks is to steal information.

**Nature:** Spoofing is not considered fraud because the victim’s email address or phone number are not stolen but rather imitated. Phishing scams are fraud because they involve information theft.

**Method:** Malicious software is installed on the victim’s computer in a spoofing attack. Phishing attacks are conducted using social engineering techniques.

**How to Prevent and Address Spoofing**

Protecting yourself from spoofing attempts is integral to responsible online behavior. In many cases spoofing attacks are easy to detect and prevent through cybersecurity awareness. Follow these tips on what to do and what not to do to protect yourself from spoofing:

· Do log into accounts through new browser tabs or official apps.

· Do use a password manager.

· Do use a spam filter for email security.

· Do invest in cybersecurity software.

· Do confirm if unexpected phone numbers or email addresses have been associated with scams.

· Do enable two-way authentication whenever possible.

· Do not click on unsolicited links.

· Do not download unexpected attachments.

· Do not share personal information.

· Do not access URLs that don’t begin with HTTPS.

· Do not log into accounts through links in emails or text messages.

If you suspect you’ve received a spoofed email, verify the message’s validity by contacting the sender using another mode of communication; do not reply to the suspicious email. Remain aware of any further damage and take steps to secure your personal information.

**How to Prevent and Address Phishing**

Minimizing the risk of phishing attacks is crucial to your organization’s cybersecurity strategy. Conduct security awareness training with employees to ensure they know how to identify and report suspected phishing attacks. Below are a few simple strategies to help defend against the many types of phishing:

·  **Use antivirus software:** Antimalware tools scan devices to prevent, detect and remove malware that enter the system through a phishing scam.

·  **Use an anti spam filter:** Anti Spam filters automatically move phishing emails to your junk folder.

·  **Update browsers and software:** Running the latest version of a web browser, app or other software ensures you have the best defense against the latest phishing attacks.

· **Activate multi factor authentication (MFA):** Even if your credentials have been compromised in a phishing attack, this extra authentication provides an extra layer of defense, and threat actors won’t necessarily be able to access your personal information.

·  **Do not open and do not reply:** Ignore spam emails! Delete them without opening. Responding to phishing emails prompts threat actors to retarget you.

·  **Security awareness training:** Train employees to recognize and report phishing attempts. Conducting phishing simulations allows employees to practice what they learn as well.

·  **Validate URLs and files:** Double-check links, files and senders for validity before clicking on links or downloading files.

If you experience a phishing attack, don’t panic. Simply reading a phishing email is normally not a problem. Phishing attacks require the victim to click a malicious link or download files to activate the malicious activity. Monitor your accounts and personal information and remain vigilant.

**f.) Personal Safety Risks Associated with Internet Use**

**The Risks Associated with the Internet and Online Social Networking**

The internet, with its endless access to information, is a valuable tool but also a potential risk to safety and security. It is important to monitor or be aware of what a child sees and shares, or could become exposed to. There is a high risk of being exposed to sexual predators (for example, in chat rooms), pornography or radicalisation.

Using e-technology to bully people has become an increasing problem in recent years with over a third of young people having been affected at least once. There has been a massive increase in online bullying due to the use of social media such as Twitter or Facebook, which is easily accessible through mobile devices as well as computers.

**Examples include:**

· Posting negative comments on someone’s Facebook/Twitter site

· Taking on someone’s identity on the web to humiliate them

· Harassing someone via their mobile phone/social media.

· Staff should be aware of the risks and check that any technological devices children use are secure and have the relevant security installed. Children may be enticed to access certain websites with the offer of special offers and prizes. They should report any concerns to a line manager immediately.

**The Risks Associated with the Internet and Online Social Networking**

**Inappropriate content** – Children may see illegal or unsuitable content such as pornography, child abuse images, dangerous advice on eating disorders, self harm or suicide, radicalisation, excessive violence or race hate materials.

**Ignoring age restrictions** – Some websites and games use age restrictions and checks to make sure that children don’t see unsuitable content. Children must be at least 13 to register on most social networking websites and therefore such companies do not provide safety advice for children under the age of 13.

**Friending or communicating with people they don’t know** – Children and young people may chat or become ‘friends’ with people on social networks or online games. They may not actually know anything about the person they are communicating with, having never met them in person. This makes children vulnerable to bullying, grooming and sharing personal information

**Sharing personal information** – Privacy controls can limit who can see your child’s details, like their name, age and where they live. But when your child connects to someone as a ‘friend’, that person will have access to your child’s personal information, including their GPS location on some devices. Some ‘free’ games might ask your child to fill out lots of details before they can play and then illegally rent or sell this data to others. Children and young people can also reveal their location by tagging photos, such as on Instagram, or checking in on Facebook or Foursquare. This enables people to find out where a child lives, socializes and studies.

**Gambling or running up debts** – Many online games are free but offer the chance to buy items such as extra lives or new levels. So children may run up big bills without realizing. Gambling sites have strict measures to make sure that their users are adults, but young people aged 18 and over could be enticed by offers and prizes and try to access these sites with the temptation to win money etc.

**7 Tips for Protecting Yourself Online**

Though the internet has many advantages, it can also make users vulnerable to fraud, identity theft, and other scams. According to Symantec, 12 adults become a victim of cybercrime every second.

**1. Keep your computers and mobile devices up to date.**

Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

**2. Set strong passwords.**

A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.

**3. Watch out for phishing scams.**

Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with.

**4. Keep personal information personal.**

Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lockdown your privacy settings and avoid posting things like birthdays, addresses, mother’s maiden name, etc. Be wary of requests to connect with people you do not know.

**5. Secure your internet connection.**

Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it.

**6. Shop safely.**

Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with https. Also, check to see if a tiny locked padlock symbol appears on the page.

**7. Read the site’s privacy policies.**

Though long and complex, privacy policies tell you how the site protects the personal information it collects. If you don’t see or understand a site’s privacy policy, consider doing business elsewhere.

**g.) Privacy Concerns Regarding Databases, Electronic Profiling, Spam, and Telemarketing**

* Concerning Information privacy such as databases, electronic profiling, spam, and telemarketing is really important. Knowing privacy is a state of being concealed or free from unauthorized intrusion and intruders. Information privacy is the right of individuals and companies to control how information about them is collected and used. As well, computers add additional privacy challenges wherein many data breaches recently due to lost or stolen hardware, carelessness with documents containing sensitive data, database breaches, and many more. To protect your privacy as well as your protection, you should use anti spyware software to detect if someone is monitoring your computer usage. Every user has the responsibility to keep their information private and secured.

**h.) Types of Electronic Surveillance and Monitoring**

* Listed below are the types of Electronic Surveillance and Monitoring,
* Wiretapping
* Bugging
* Videotaping
* Geolocation (RFID, GPS, data)
* Social media mapping
* Proximity cards

**SUMMARY**

**To protect a company’s computer system and data and an individual's personal data and devices from cyber threats and attacks one must do the following:**

* Keep your software up to date. This includes operating systems, applications, and firmware.
* Use strong passwords and two-factor authentication (2FA) wherever possible.
* Use a Virtual Private Network (VPN) when connecting to public Wi-Fi networks.
* Be wary of phishing emails and other social engineering tactics.
* Use antivirus software and keep it up to date.
* Use firewalls to block unauthorized access to your computer or network.
* Backup your data regularly.
* Use encryption to protect sensitive data.
* Limit access to sensitive data.
* Educate yourself and your employees about cybersecurity best practices.

**CONCLUSION AND RECOMMENDATION**

**a.) Discuss the current state of network and Internet security and privacy legislation (in the Philippines).**

* In 2012 the Philippines passed the Data Privacy Act 2012, comprehensive and strict privacy legislation “to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth.” According to Microsoft Philippines National Technology and Security officer Mr. Dale Jose, The Philippines ranked 61st out of 194 countries in the ITU Global Cybersecurity Index.

**REFERENCE**

Computer Hope (2020). How to Prevent Unauthorized Computer Access. Retrieved from: https://www.computerhope.com/issues/ch000464.htm

Cypress Data Defense (2020). How to Protect Your Data from Unauthorized Access. Retrieved from: https://cypressdatadefense.com/blog/unauthorized-data-access/

Lightfoot L. (2023). The Top 10 Biggest Cyber Attacks Of 2021. Retrieved from: https://expertinsights.com/insights/10-high-profile-attacks-2021/

*What is online identity theft? how to*. Webroot. (n.d.). https://www.webroot.com/us/en/resources/tips-articles/malware-identity-theft?fbclid=IwAR0C50z0-d18feSUJ4ymRl2J\_RAncNrGbCDhwsG\_zWCMTFtHqE9PzV9wj-A

Panchal“Business, R. (2023, May 4). *20+ pros and cons of Cyber Security (explained)*. List of Pros and Cons to make you a sensible decision. https://thenextfind.com/pros-cons-of-cyber-security/?fbclid=IwAR0P\_xt1gcBCxAak5uyBoBve-q0sSfjO3U89s4rG1Vjif3l\_kiS7jKIfky4

*Spoofing vs phishing: Definition & differences - crowdstrike*. crowdstrike.com. (2023, April 27). https://www.crowdstrike.com/cybersecurity-101/attack-types/spoofing-vs-phishing/?fbclid=IwAR2873YGi5C5ubMOz5UZ4HXgHRKvgCklryszKM2XX9E1sSuHM6FM2wdBFSA#:~:text=Differences%20Between%20Spoofing%20and%20Phishing&text=Purpose%3A%20The%20goal%20of%20spoofing,not%20stolen%20but%20rather%20imitated

*Active social care*. activesocialcare.com. (n.d.). https://activesocialcare.com/handbook/safeguarding-children/the-risks-associated-with-the-internet-and-online-social-networking/?fbclid=IwAR2M\_sSIjCCv0tk5r4rlad9VlIqW3LhwRNWSuZDenVfjrNKYZ3zZaU3CtUI

*Weststar Bank*. 7 Tips for Protecting Yourself Online ’ WestStar Bank. (n.d.). https://www.weststarbank.com/tools-and-resources/7-tips-for-protecting-yourself-online?fbclid=IwAR02qRGfWmRd2UW1zY3CgLSJSK0tDaipbUVaROs6VR\_n6WM8AYnOFxnhUN8