UNDERSTANDING CYBERSECURITY

ADRIANO, OGALINO, RAPAY, SANCHEZ

Introduction to Cybersecurity

"WHAT ARE WE TRYING TO PROTECT OURSELVES AGAINST? "

- Unauthorized Access
- Unauthorized Deletion
- Unauthorized Modification

Cybersecurity

- Cybersecurity is a subset of information security, which aims to protect the availability, confidentiality, and integrity of data.

THE CIA TRIAD

The Confidentiality, Integrity, and Availability (CIA) triangle is a design framework that helps businesses and organizations create their security policies.

Confidentiality

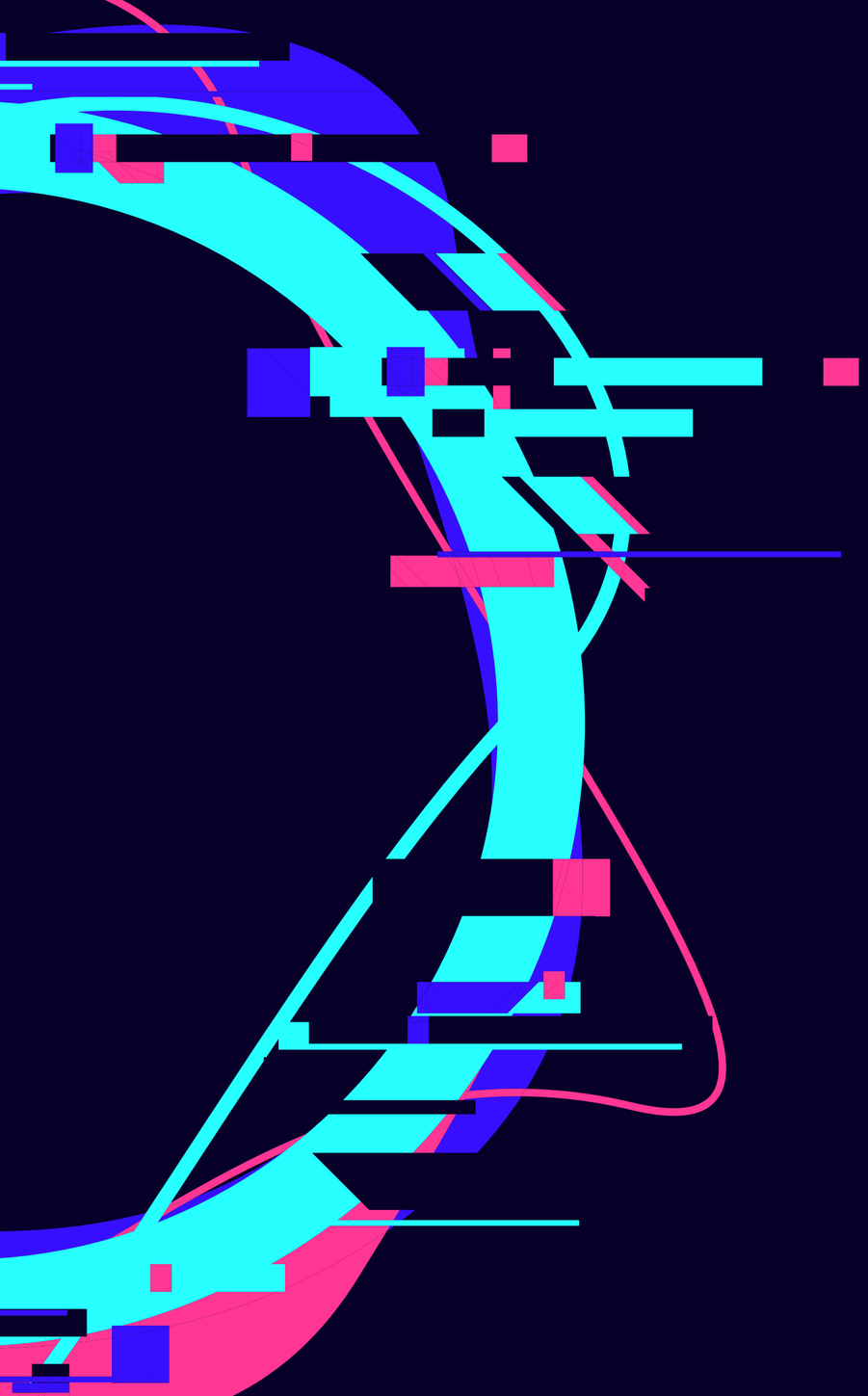
Protection of personal data is confidentiality. Confidentiality refers to not disclosing client information to anybody else, including coworkers, friends, family, etc.

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

01 to explain the importance of security and privacy for computer users in relation to computing devices, networks, and the Internet.

02 to discuss online theft, identity theft, spoofing, phishing, and other types of dot cons and detailed steps to protect against these threats.

03 to identify personal safety risks associated with Internet use and list steps to protect against them.

04 to describe privacy concerns regarding databases, electronic profiling, spam, and telemarketing and identify ways to protect privacy.

05 to discuss types of electronic surveillance and monitoring and list ways to protect privacy.

PROS

- Protection From Unwanted Programs
- Denies Unauthorized Access
- Prevents Hacking
- Minimized Data Theft Hazard
- Reduces Computer Crash
- Increase In Cyber Defence

PROS

- Detection And Deletion Of Harmful Programs
- Deny Access From Possible Threat
- Improves Stakeholder Confidence
- Faster Recovery

CONS

- Difficult To Set Up
- Constant Need To Update The Security
- Expense Of Setting Up The Whole System
- Security Patches May Back-Fire
- New Update Might Not Suit Your System
- Makes The System Slower

CONS

- **New Update Might Not Suit Your System**
- **Makes The System Slower**
- **Incorrectly Configured System Blocks Firewall**

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.

CYBERSECURITY

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

CYBERSECURITY

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.

TOP 5 CYBERSECURITY THREATS TO MANAGE

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.

PHISHING

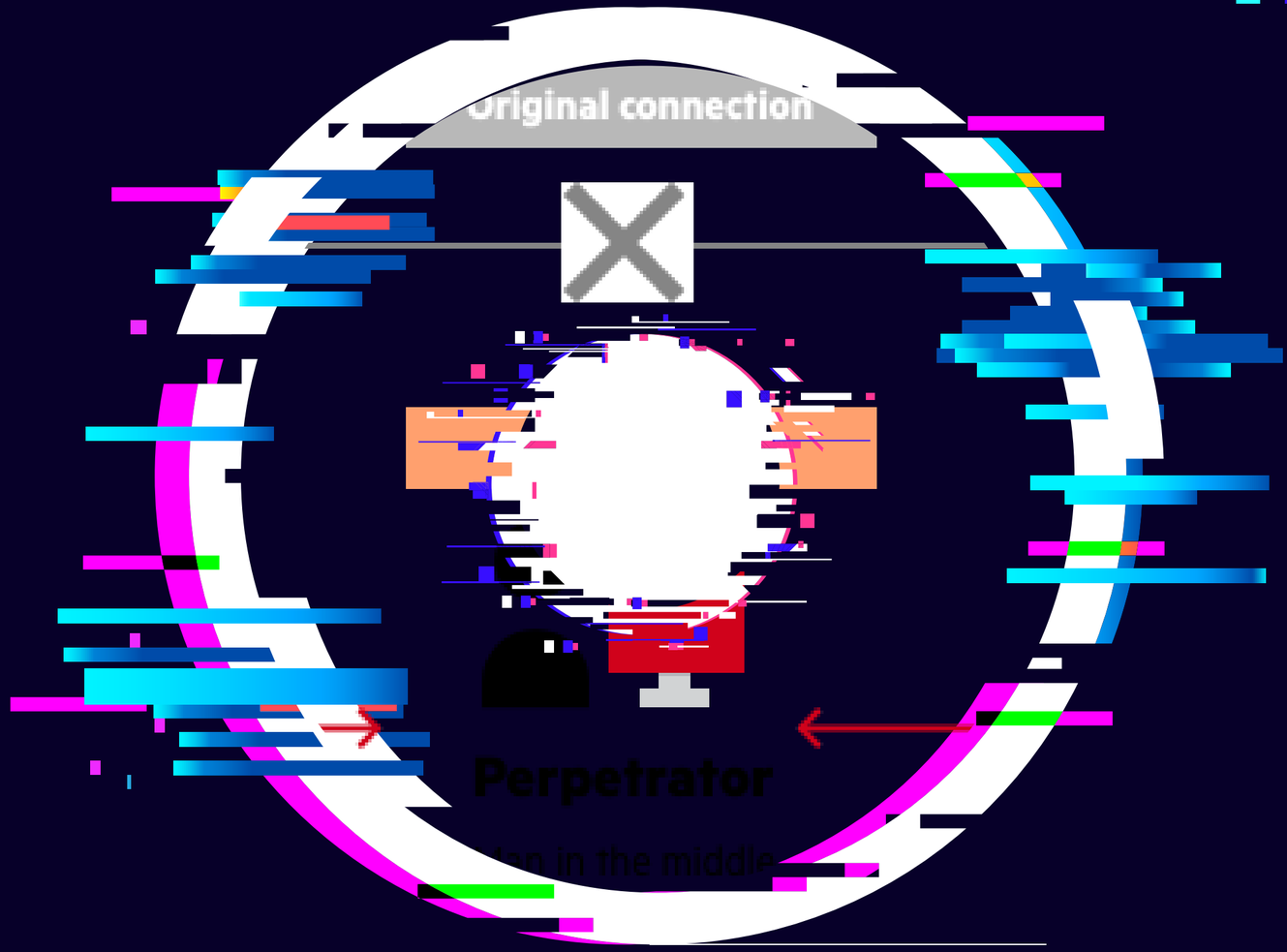
Phishing exploits human weaknesses whereas malware depends on technical aspects to do harm. These assaults entail deceiving a victim into disclosing private information or clicking on anything that may infect their device with malware. They frequently serve as the launch pad for more significant attacks.

INSIDER THREATS

An insider threat refers to a cyber security risk that originates from within an organization.

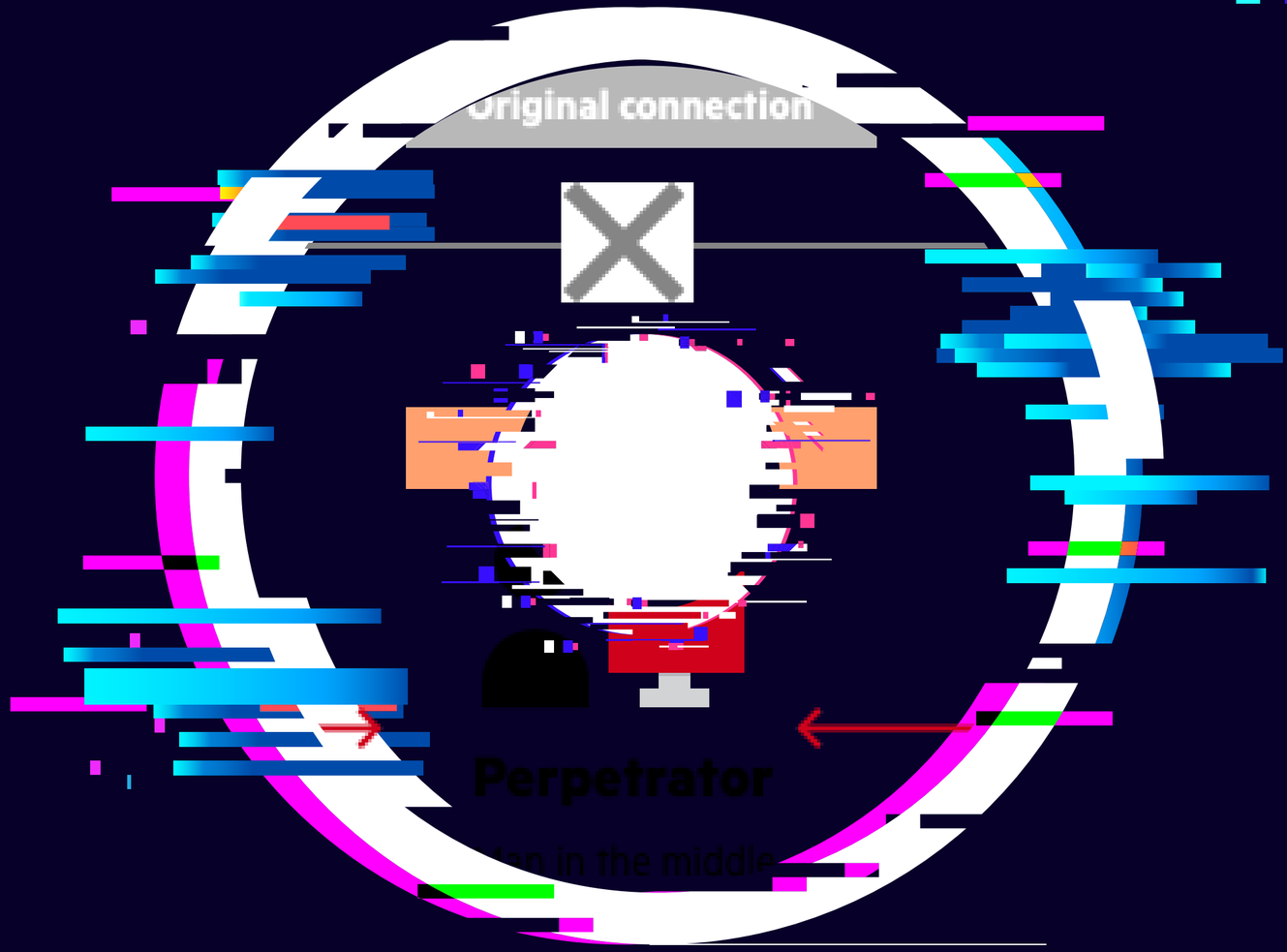
MAN-IN-THE-MIDDLE ATTACKS

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.



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.



BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

Use strong, varied passwords

Another crucial cybersecurity step is to use strong passwords. Most hacking-related data breaches stem from weak passwords, which are easy to avoid. Cracking a 12-character password takes 62 trillion times longer than a six-character one.

BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

Create backups of sensitive files

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

Stay informed and tell others

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.

BEST PRACTICES FOR CYBERSECURITY IN 2022

Review security steps regularly

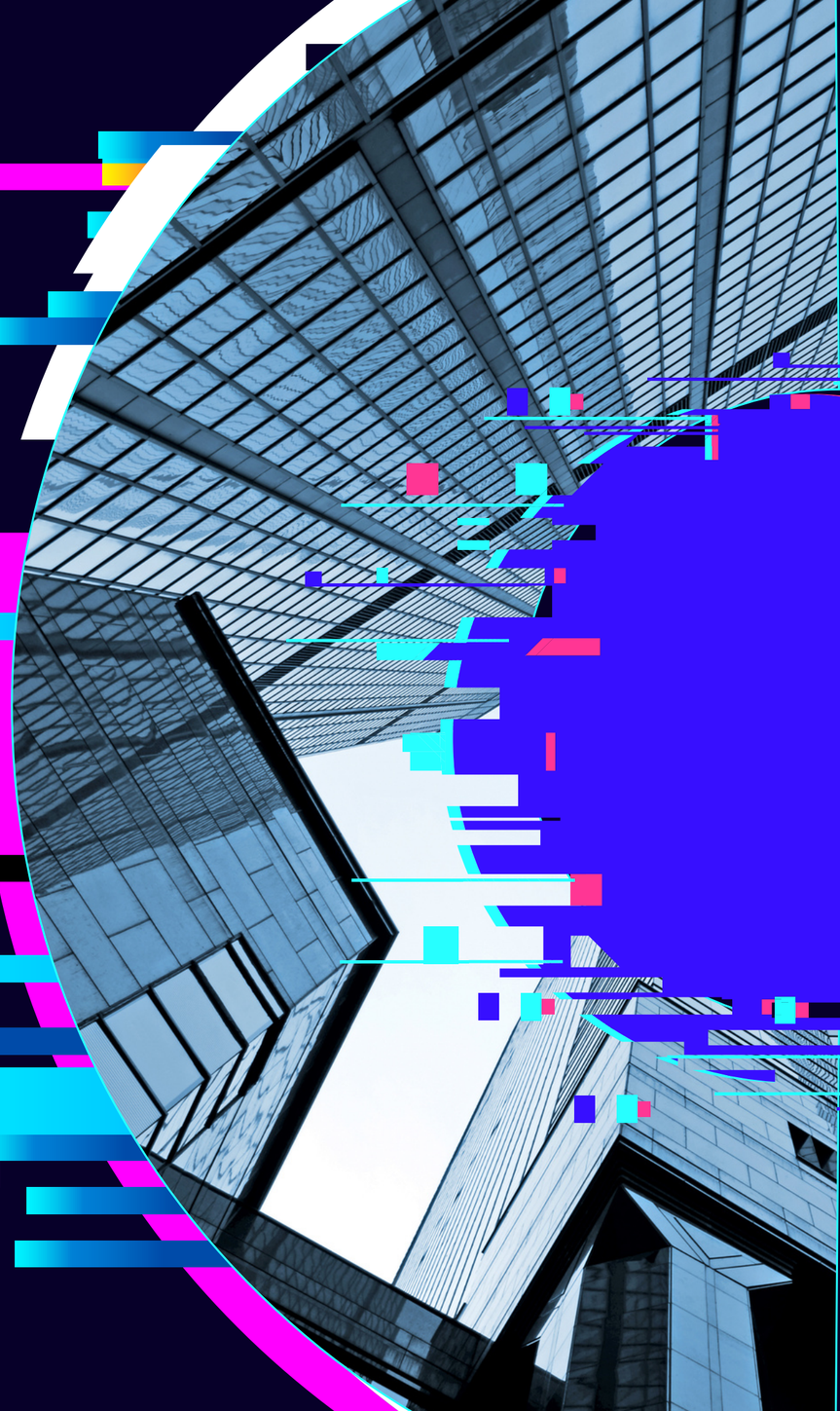
Every user and business should be aware that best practices today might not be applicable tomorrow. Since the subject of cybersecurity is always changing, it's crucial to assess defenses to make sure they remain effective. Without routine reviews, people can be exposed without realizing it.

Unauthorized Access

refers to the use of a computer or network without permission.

Unauthorized Use

refers to the use of a computer or its data for unapproved or possibly illegal activities.



UNAUTHORIZED ACCESS AND UNAUTHORIZED USE

Tailgating

Hacking

Illegal use/break of login and password

Total Amount :

$8 Trillion

According to a report by IBM’s X-Force, ransomware attacks were the most common cyberattack in 2021, accounting for 21% of attacks.

Cybersecurity Ventures predicts that the cost of these types of cybercrime will hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025

According to Microsoft, using multi-factor authentication (MFA) can prevent 99.9% of account attacks

WAYS TO PROTECT AGAINST UNAUTHORIZED ACCESS AND USE:

- Implement strict access control measures
- Monitor employee activity
- Educate employees
- Use strong passwords
- Keep software up to date
- Use antivirus and anti-malware software
- Backup data regularly
- Run system scans to check for vulnerabilities
- Know how to handle email
- Use a firewall:

ANTIVIRUS AND ANTI-MALWARE SOFTWARES

McAfee

Avast

Bitdefender

Norton

FIREWALL

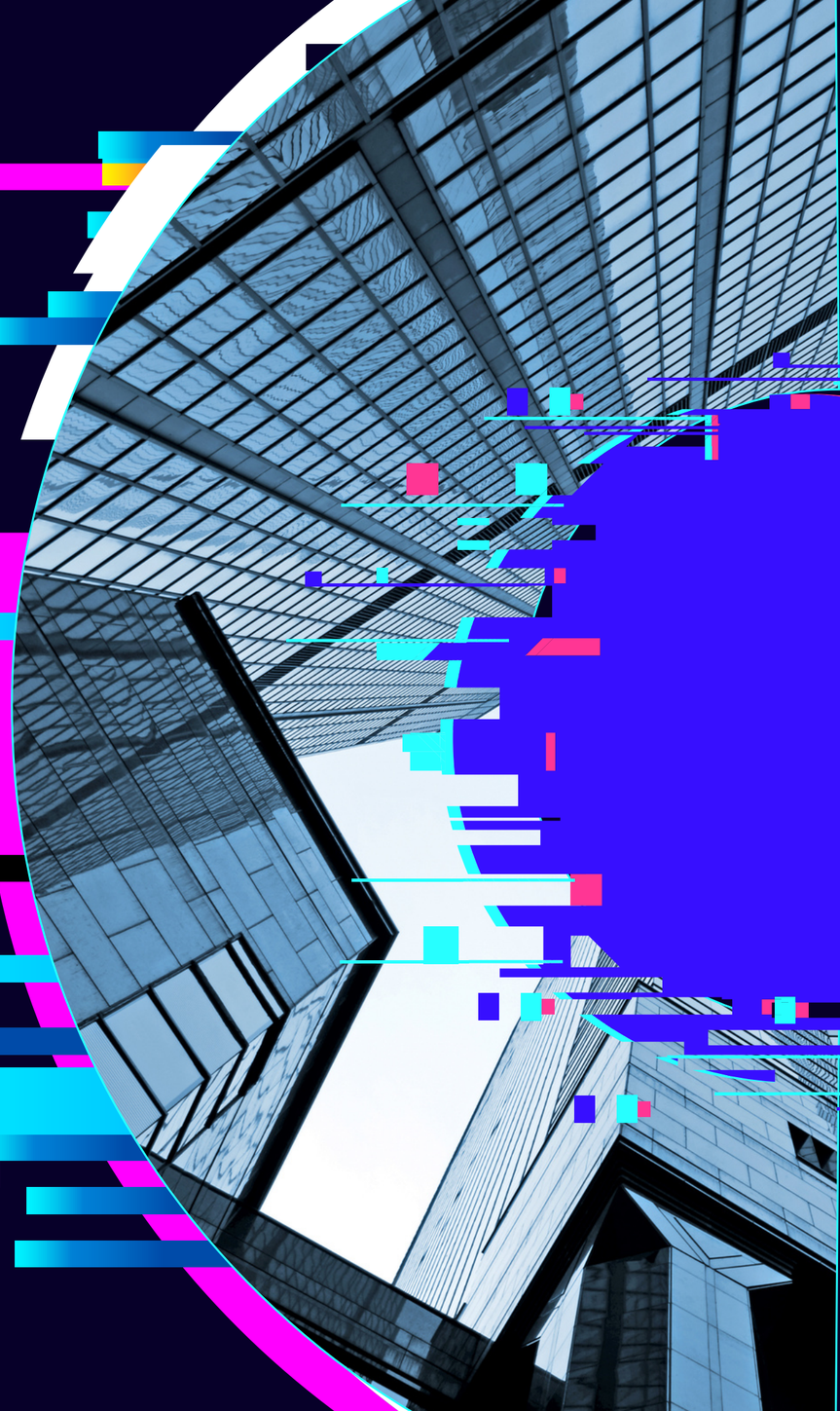
Windows Firewall

ZoneAlarm

Bitdefender

Computer Sabotage

is the act of intentionally destroying, altering, or disrupting computer systems or networks with malicious intent.



COMPUTER SABOTAGE

SolarWinds Attack

Attackers took advantage of multiple vulnerabilities within the network which is a method known as a supply chain attack

Accellion's Attack

Attackers infiltrated a company network through an affiliated partner, suppliers or any other party that would have access to the network

Oldsmar Water Supply Attack

Hackers were able to access the operating systems via remote-access system TeamViewer used by employees.

COMPUTER SABOTAGE

Channel 9 News Attack

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

WAYS TO PROTECT AGAINST COMPUTER SABOTAGE

- Install quality antivirus and firewall software
- Use only reliable networks
- Don’t open spam
- Don’t download anything from dubious sites
- Monitor systems for unexpected behaviors

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.

What Is Identity Theft?

KEY TAKEAWAYS

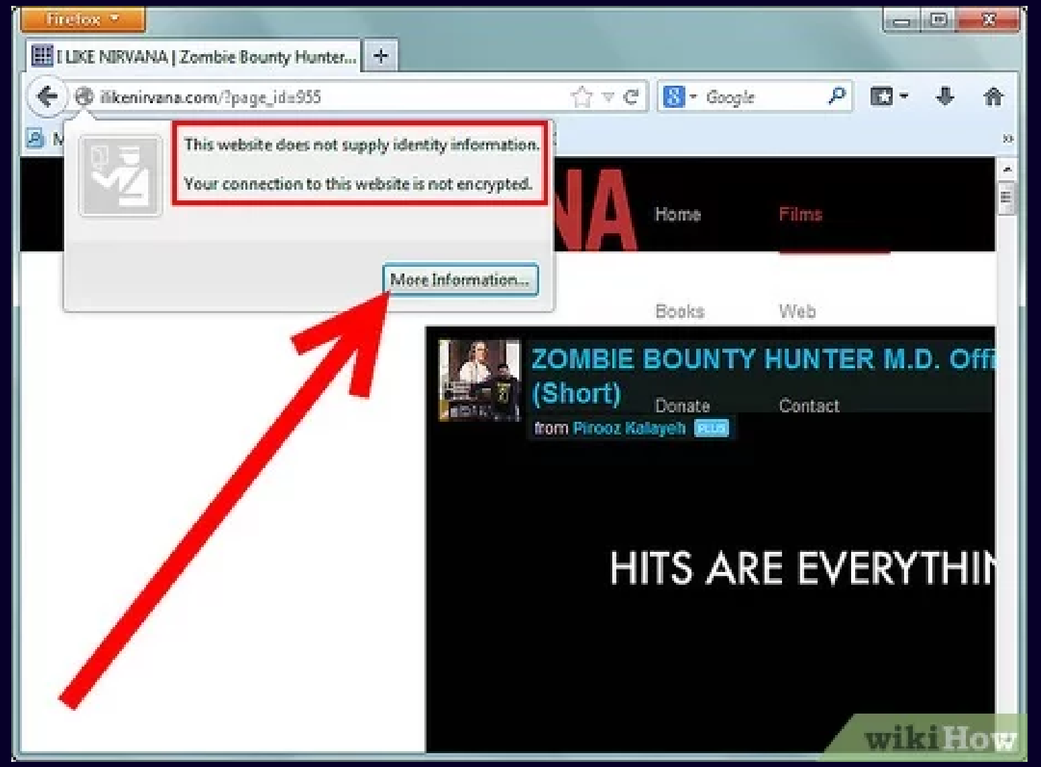
Identity theft occurs when someone steals your personal information and credentials to commit fraud.

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.

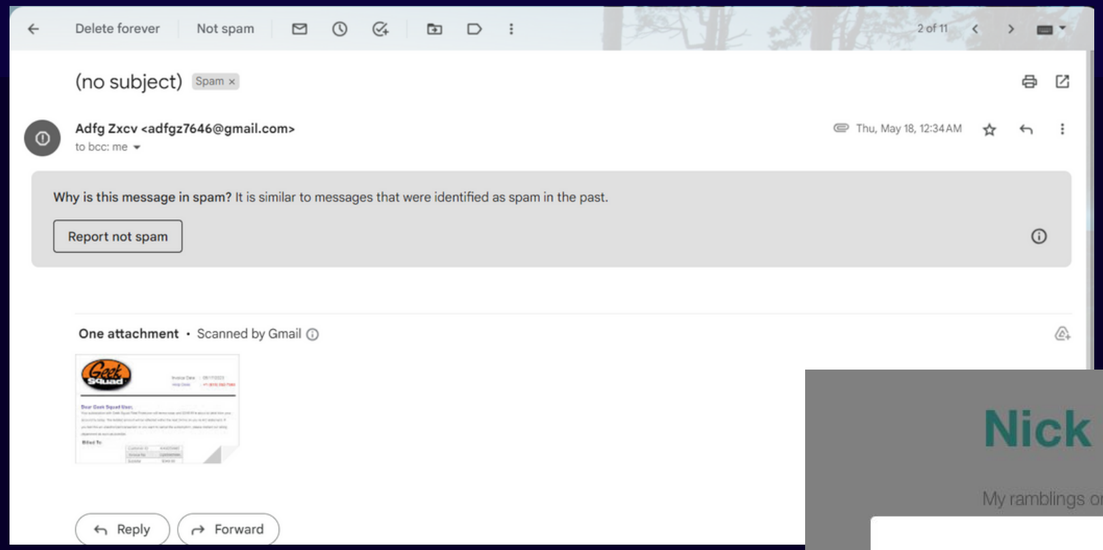
YOU CAN ENCOUNTER SPYWARE AND OTHER FORMS OF MALWARE IN MANY WAYS, INCLUDING:

Downloading files or software



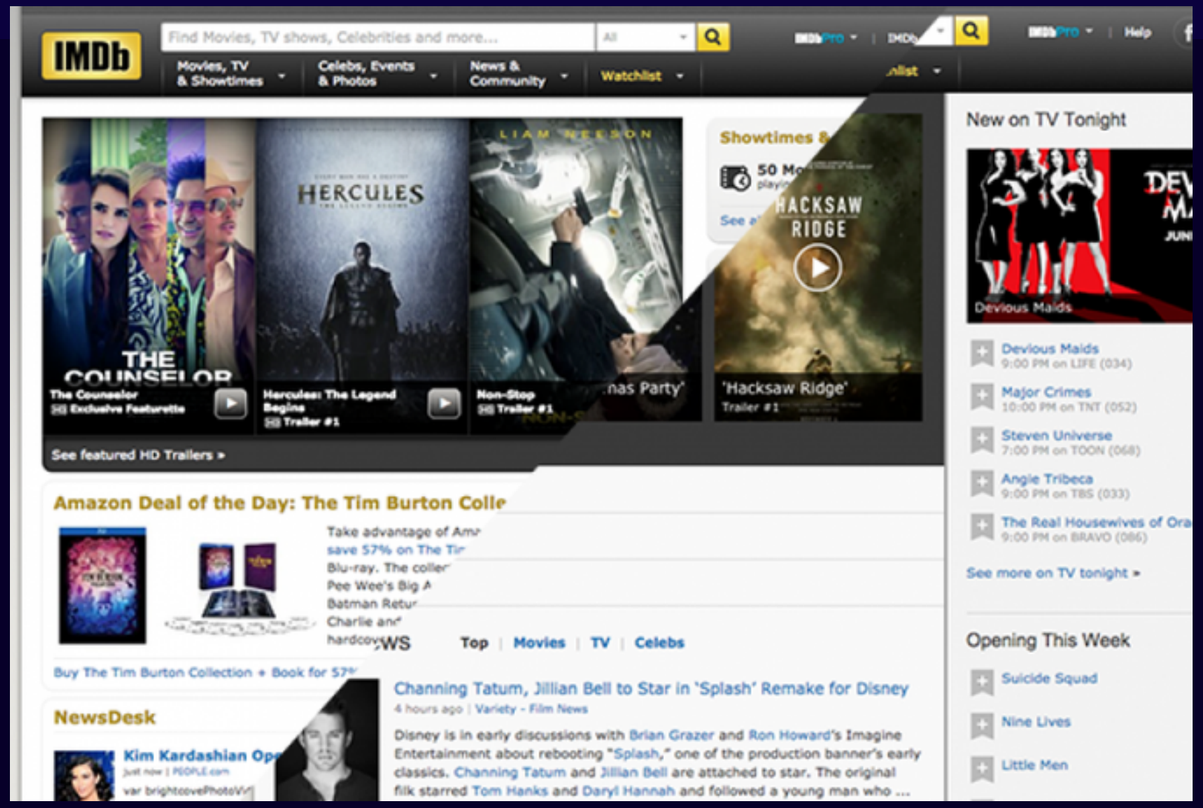
YOU CAN ENCOUNTER SPYWARE AND OTHER FORMS OF MALWARE IN MANY WAYS, INCLUDING:

Opening email attachments or clicking on pop-ups



YOU CAN ENCOUNTER SPYWARE AND OTHER FORMS OF MALWARE IN MANY WAYS, INCLUDING:

Visiting devious websites



SPYWARE TRANSMITS YOUR SENSITIVE DATA, USING YOUR OWN INTERNET CONNECTION.

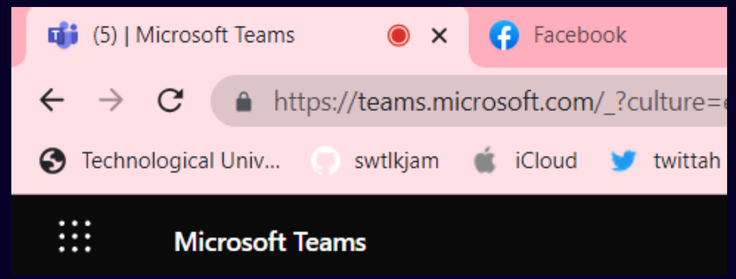
- Credit card numbers
- Bank account numbers
- Social Security numbers
- Usernames and passwords
- Address books, including email addresses

HOW TO PREVENT IDENTITY THEFT

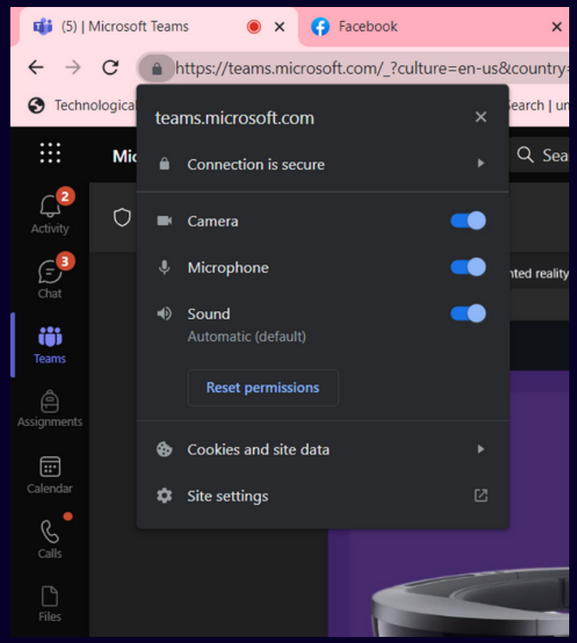
1.Continually check the accuracy of personal accounts and deal with any discrepancies immediately.
2. Avoid questionable websites.
3. Practice safe email protocol:
    - Don't open messages from unknown senders
    - Immediately delete messages you suspect to be spam

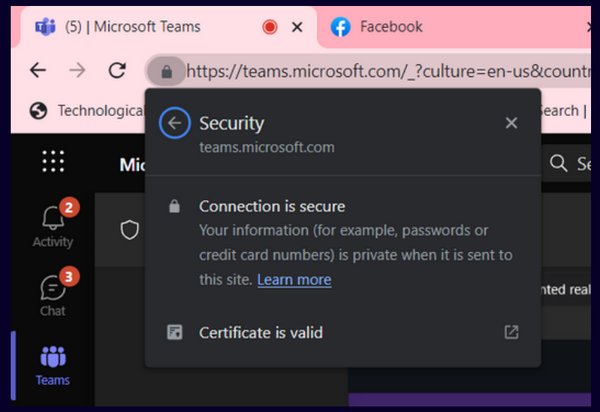
HOW TO PREVENT IDENTITY THEFT

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



Hypertext Transfer Protocol Secure (https)





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
- Domain or website spoofing
- IP spoofing
- GPS spoofing
- Caller ID spoofing

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. Four of the most common types of phishing attacks are outlined below:

- Spear phishing
- Whale phishing
- Voice phishing (vishing)
- SMS phishing (smishing)

DIFFERENCES BETWEEN SPOOFING AND PHISHING

- 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

- · 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.

HOW TO PREVENT AND ADDRESS 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.

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.

- 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.
- Ignoring age restrictions
- Friending or communicating with people they don’t know
- Sharing personal information
- Gambling or running up debts

7 TIPS FOR PROTECTING YOURSELF ONLINE

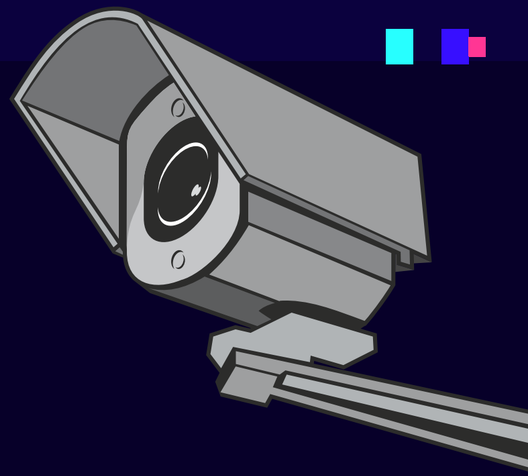
1. Keep your computers and mobile devices up to date.
2. Set strong passwords.
3. Watch out for phishing scams.
4. Keep personal information personal.
5. Secure your internet connection.
6. Shop safely.
7. Read the site’s privacy policies.

PRIVACY CONCERNS REGARDING DATABASES, ELECTRONIC PROFILING, SPAM, AND TELEMARKETING

Concerning Information privacy such as databases, electronic profiling, spam, and telemarketing is really important. 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.

TYPES OF ELECTRONIC SURVEILLANCE AND MONITORING

1. Wiretapping
2. Bugging
3. Videotaping
4. Geolocation (RFID, GPS, data)
5. Social media mapping
6. Proximity cards



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.

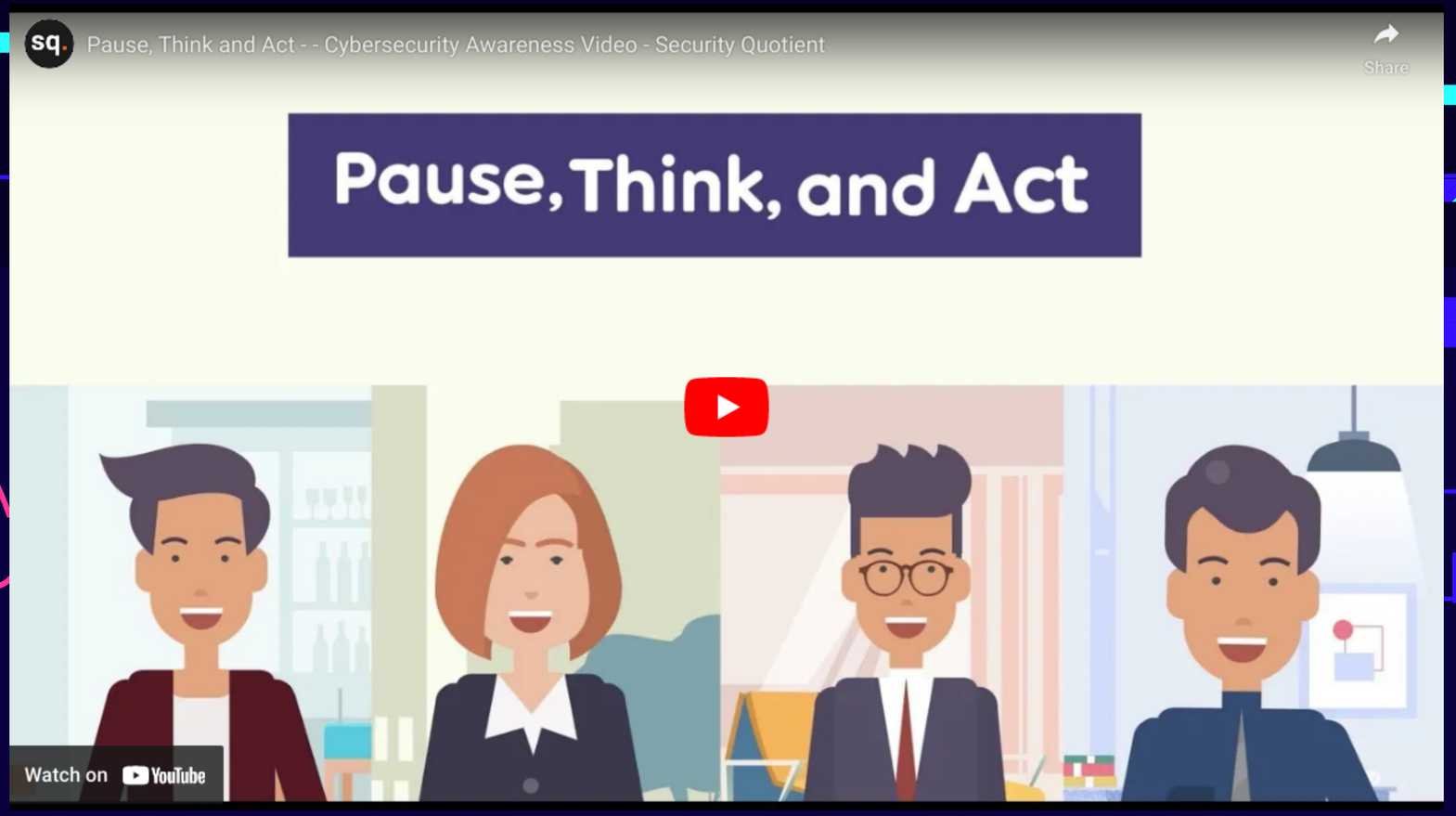
The right of an individual not to have private information about himself disclosed, and to live freely from surveillance and intrusion.

Rule XIII. Penalties

Section 52. Unauthorized Processing of Personal Information and Sensitive Personal Information.

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

CYBERSECURITY AWARENESS



THANK YOU