

WELCOME TO CYBERSECURITY: HOW WE STAY SAFE ONLINE



THE DIGITAL WORLD IS YOUR WORLD

We play, learn, and talk online every single day. It is an extension of our physical lives.

WHAT IS AT STAKE?

Just like we lock our front doors at night to protect our homes, we need to learn how to lock our digital doors.

YOUR MISSION

Today, you will learn the secrets of how hackers operate, the laws that protect us, and the specific steps you can take to become a Digital Defender for your friends and family.

What is Cybersecurity?



The Definition

Cybersecurity is the collection of tools, policies, training, and best practices used to protect our computers and digital data [2].

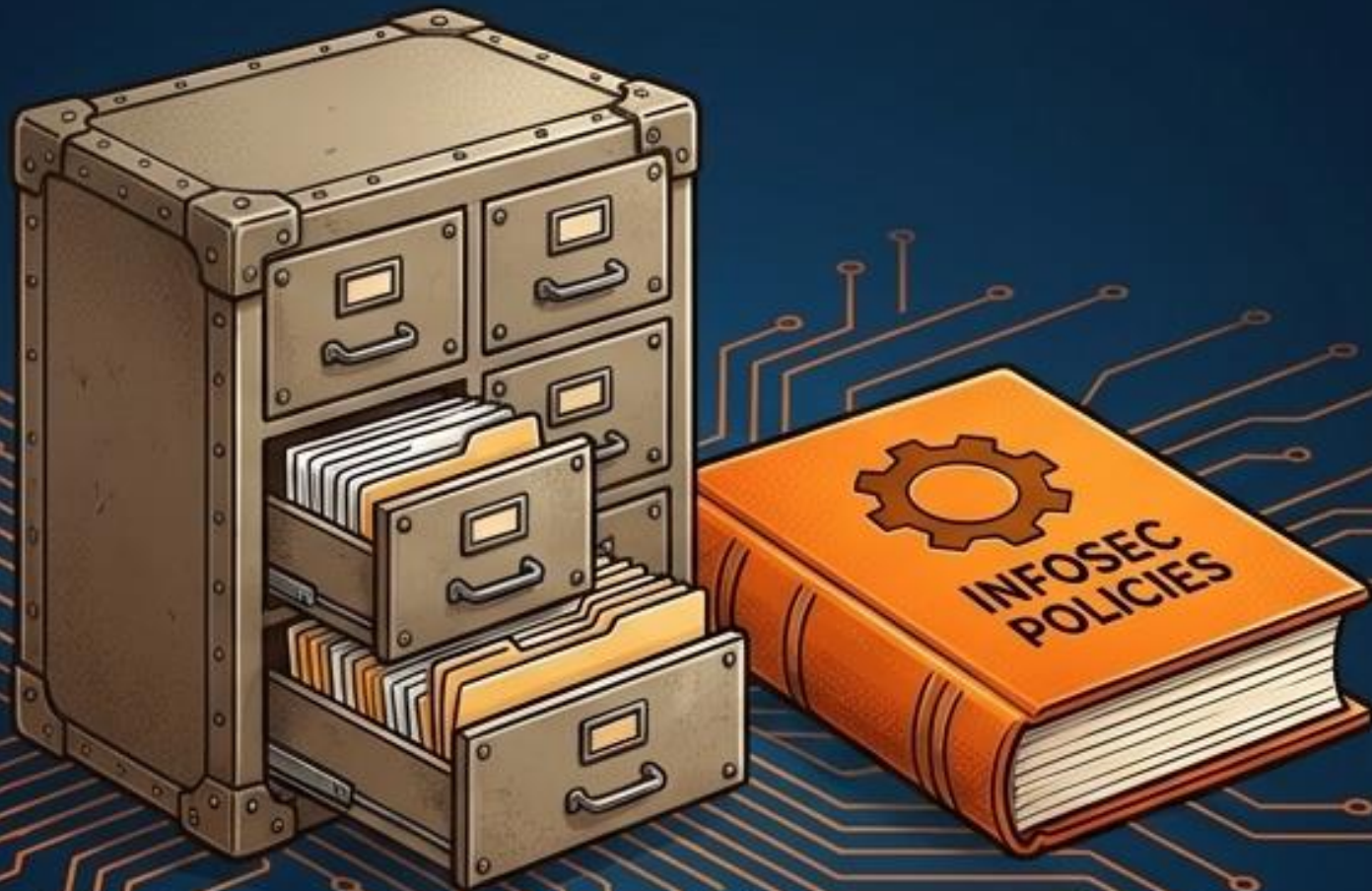
Who is Involved?

It includes risk management approaches and actions taken by both big organizations and everyday users like us [2, 19].

The Goal

To safeguard the cyber environment and ensure that the digital assets we care about are kept safe from damage, unauthorized access, or theft [2].

Cybersecurity vs. Keeping Information Safe



Keeping Information Safe (InfoSec)

The big picture. It focuses on protecting all forms of information. This includes physical paper files, printed records, and the overall rules an organization uses to manage its data [67, 197].



Cybersecurity

A specialized branch of InfoSec. It focuses specifically on protecting digital systems, networks, and electronic devices from digital threats and malware [76].

The Difference: If you lock a paper diary in a physical safe, that is **Information Security**. If you put a strong password on your digital journal app, that is **Cybersecurity**.

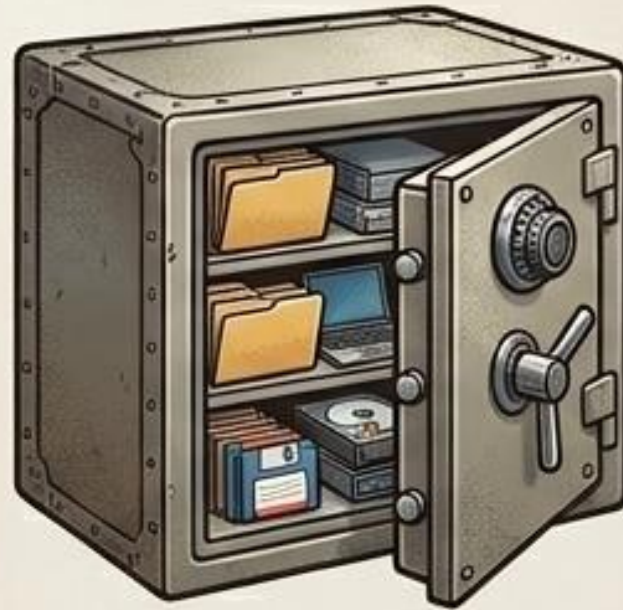
Useful Words to Learn

ACCESS



The ability to make use of an information system or its resources. Think of this as having the “digital keys” to enter a locked room [10].

ASSETS



The valuable things we are trying to protect. This isn't just data; it includes major applications, computer systems, equipment, and even the people using them [13].

MALWARE



Short for “malicious software.” It is a bad program inserted into a system covertly to cause harm or compromise a victim's data [30].

Common Ways Hackers Attack



Phishing (The Trick)

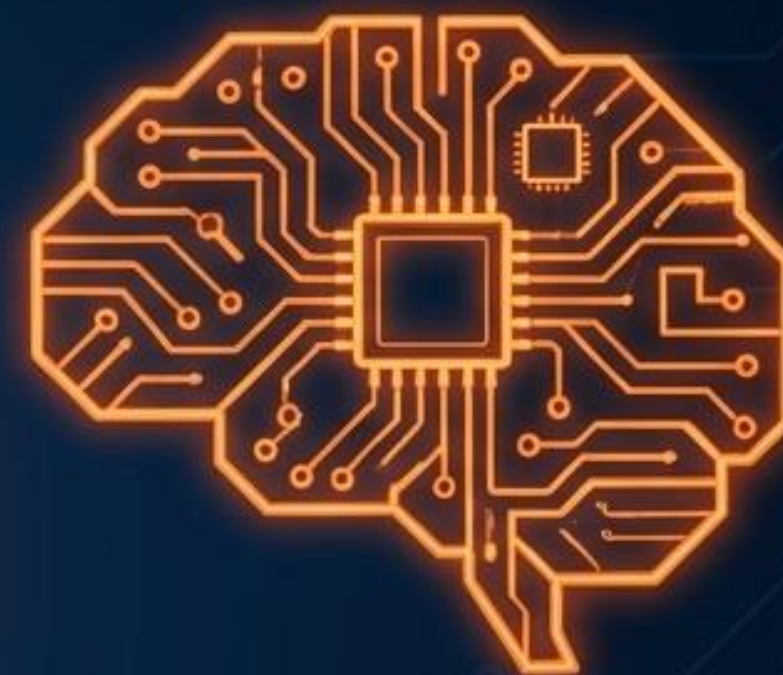
Tricking individuals into handing over sensitive personal information. Hackers use deceptive, fake emails or text messages that look like they are from trusted sources (like your bank or a video game company) [34, 201].



Ransomware (The Trap)

A highly disruptive type of malware that locks or encrypts your files so you cannot use them. The hacker then demands that you pay them money (a ransom) to unlock your own data [259].

How Attacks are Changing



The AI Threat

Hackers are no longer just manually typing code; they are using Artificial Intelligence to make their attacks faster, smarter, and much more common. Because of AI tools, attacks by cybercriminals have skyrocketed by a massive 89% [47].

Blink of an Eye

The speed of attacks is accelerating drastically. In some cases, the fastest recorded time for a hacker to break out and spread through a system is only 27 seconds [49].

The Law in the Philippines

Our Shield

In the Philippines, the main defense against online crime is the Cybercrime Prevention Act of 2012, officially known as Republic Act No. 10175 [1].



Why It Was Created

The State recognizes how vital technology is to our overall social and economic development. The law was created to provide an environment where information is freely exchanged but safely protected [2].

Its Power

It safeguards the integrity, confidentiality, and availability of our computer systems by making digital digital misuse, abuse, and illegal access punishable by law [2].

Crimes the Law Punishes

Illegal Access



Stealing "Access": Getting into the whole or any part of a computer system without the right or permission to do so. It is the exact digital version of breaking and entering into a physical house [3].

Wanted

Computer-related Identity Theft



Stealing an "Asset": The intentional acquisition, use, misuse, transfer, alteration, or deletion of someone else's identifying information (like passwords or private details) without their permission [4].

Wanted

The Three Goals of Security

Confidentiality

Keeping it Private: Ensuring that only authorized users can see sensitive information. It is like putting a padlock on your private diary [198, 305].

Availability

Keeping it Working: Making sure systems work when needed. A perfectly private system is useless if authorized people cannot access it reliably and on time [200, 305].



Integrity

Keeping it Accurate: Ensuring information is trustworthy and has not been tampered with or changed by a hacker. It means the data is exactly what it is supposed to be [199].

Steps to Protect Yourself



1. Use Multi-Factor Authentication (MFA)

Add an extra layer of protection. MFA requires two or more proofs of identity: something you know (like a password) AND something you have (like a temporary code sent to your phone) [204].



2. Make Strong Passwords

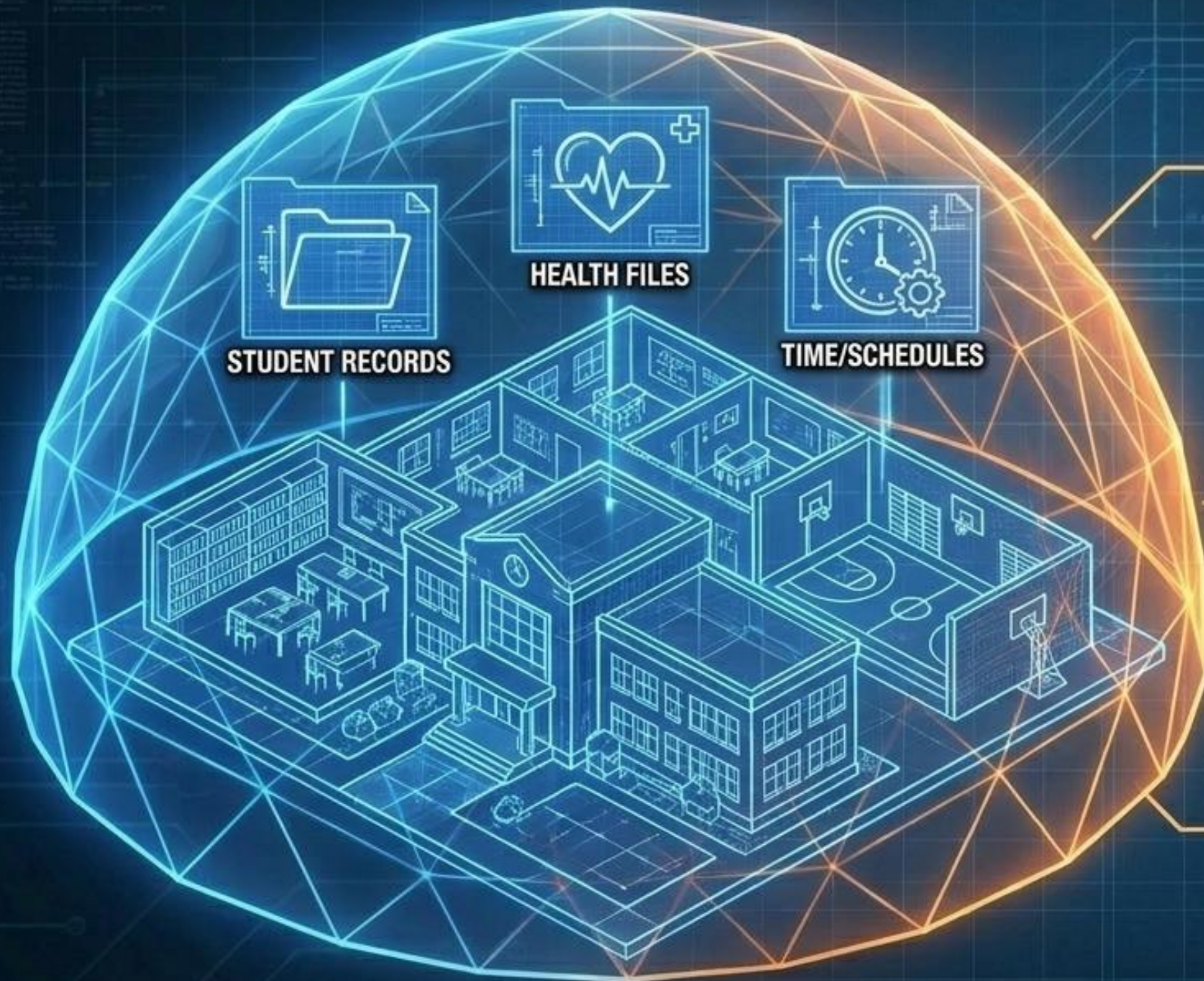
Use complex, unique passwords or long passphrases. Never reuse the same password across different websites or games [205].



3. Update Software Immediately

Do not ignore update reminders! Updates often contain critical patches that fix vulnerabilities and stop known threats from getting in [205].

Why Schools and Businesses Need Security



Protecting Massive Assets

Schools and businesses hold vast amounts of sensitive data that hackers want, including student grades, health records, and private family information [71, 262].

Preventing Disruptions

A successful cyberattack, like a ransomware lockout, can force a school to completely close its doors or a business to halt all operations [263].

Ensuring Availability

Strong cybersecurity ensures that schools don't have to stop classes due to computer failures, keeping learning on track for everyone [263].

Creating Your Own Family Plan



1. Identify Password Areas

Sit down and agree as a family on guidelines for where passwords are used. Remind everyone not to share them or use simple birthdays [179].



2. Set Safety Routines

Make cybersecurity a daily habit. When setting up new devices, review privacy options together. Always avoid using public Wi-Fi when handling sensitive info [179, 182].



3. Use Parental Controls & Open Talk

Use device locks to protect younger siblings. Most importantly, create a safe space where family members feel comfortable asking for help with confusing links or suspicious emails [179].