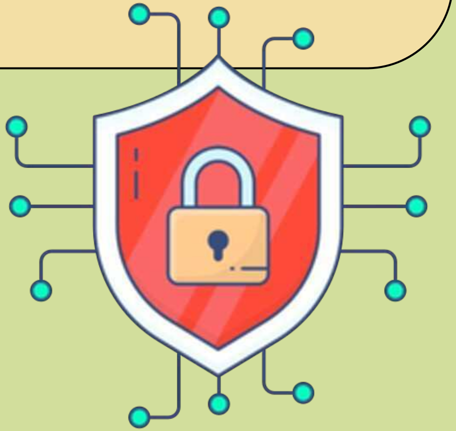
Welcome to Cybersecurity!

Team ***Nebula***

Kerina Drummond | Didi Caceres | Micaiah Cogshell | Diane Gilzow



In one word. What is Cybersecurity?

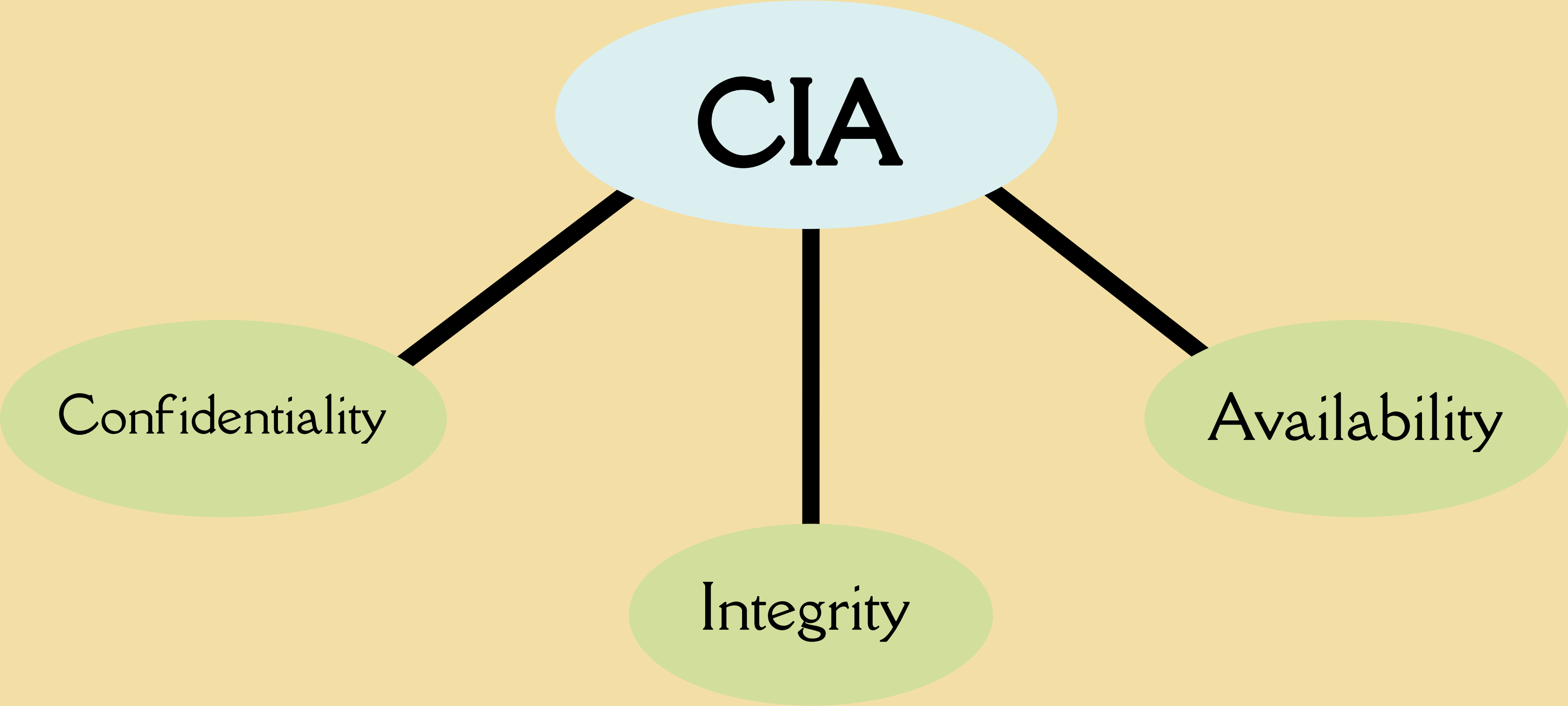
Cybersecurity is …

The practice of protecting systems, networks, and data from unauthorized access and damage from internal and external threats.

THE CIA TRIAD

What is the CIA Triad?

And how does it correlate with cyber?



CIA

Confidentiality

Integrity

Availability

The "C" in CIA

Confidentiality

Ensuring data is only accessible by authorized parties

- Data encryption
- Data classification and labeling
- Access controls
- Multi Factor authentication
- Strong Password Policy

The “I” in CIA

Integrity

Ensuring data is accurate and unmodified

Data cannot be **altered** or **destroyed**

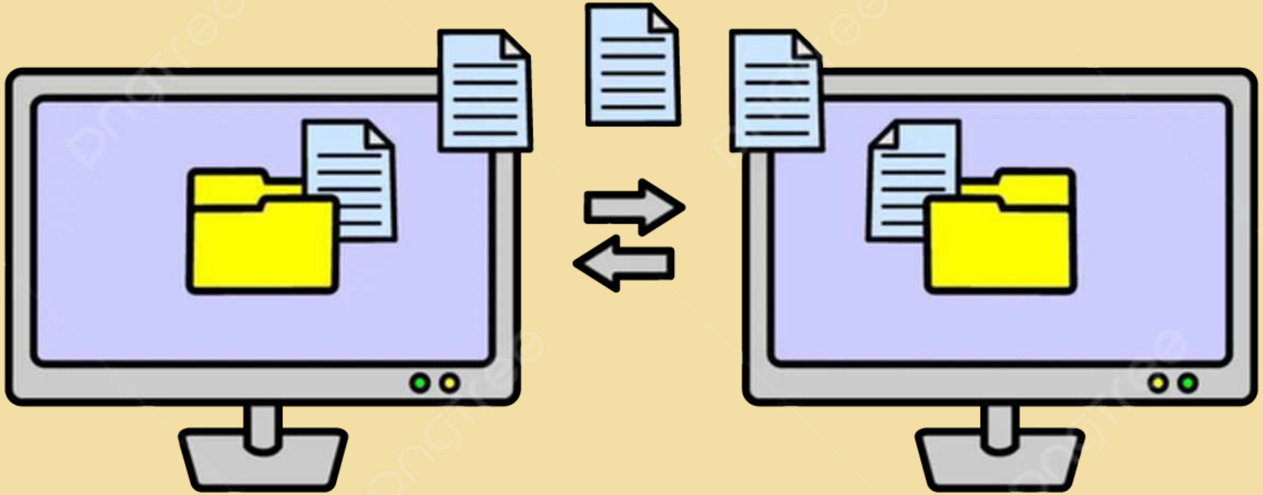
Tools such as hashes are used to check for integrity.

The "A" in CIA

Availability

Keeping systems and data accessible to authorized individuals.

Consistent backups helps to keep information readily available in case of operational downtime or unexpected shutdowns.



Authentication VS Authorization

What is the difference?

Authentication

The verification of Identity

Who are you?

Authorization

Things that can be accessed

What you do?

MALWARE

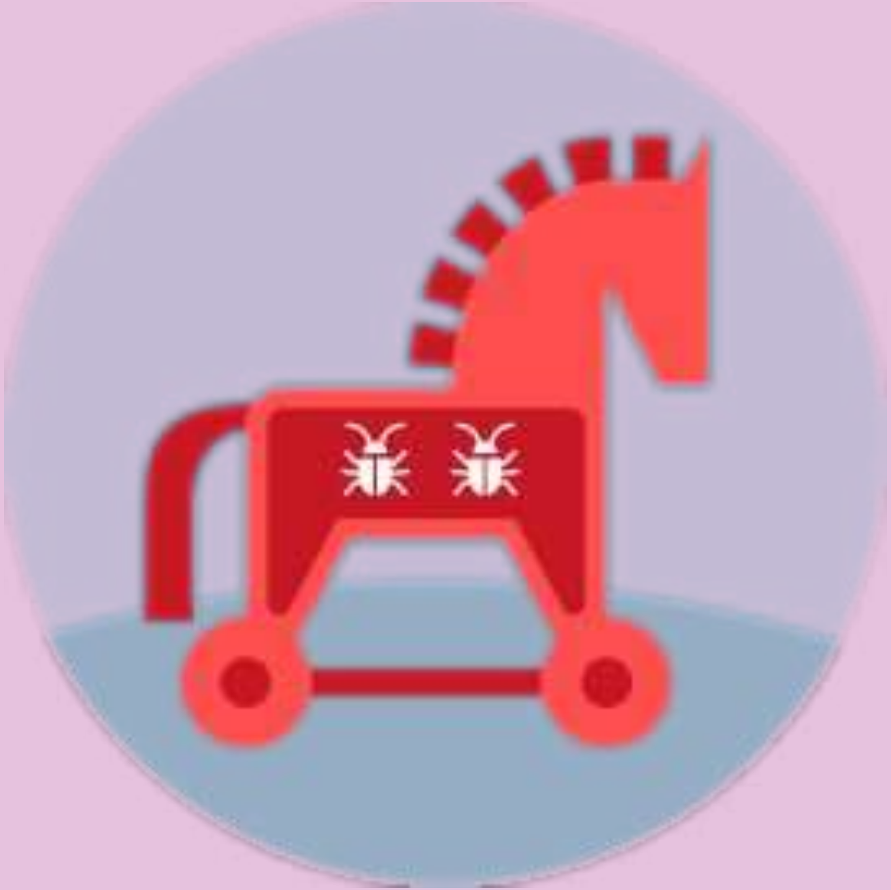
What is Malware?

Malware is any software that is designed to disrupt, damage, or gain access to a computer system without the user’s consent.

Trojans

Trojans are named after the Trojan Horse; this malware disguises itself as desirable files to trick users into downloading.

Ex: Trying to download a pirated movie but getting a virus instead.



Worms

Worms are named after their ability to "worm" through networks of computers; spreading through replicating themselves within a network, and they usually need a patient 0 to interact with the original worm.

Ex: your computer suddenly glitching and freezing because John Doe, your coworker, implemented a program on his computer that had a software bug. Now all the computers are glitching.

Adware

This is one of the most common forms of malware, named after its main feature: ads. It works by serving you unwanted ads as pop-ups, new browser windows, new tabs and messages. Its main focus is to collect information from the user's computer.

Ex: Clicking on a $50 Nintendo Switch ad, and now you won't stop getting popups every time you open your browser.

What did we learn?

The Common Denominator

As you may have noticed, each example had a common denominator: you.

Whether it's you or someone you know, this malware only works if someone allows it into their computer.

PROACTIVITY IN CYBER!

What does Proactivity Mean?

1 *'Prepared for the worst, but hoping for the best!'*

2 Thinking Ahead!

3 Using tactics such as Preventative Controls and Safe Online Practices.

Preventative Controls

What even *are* controls?

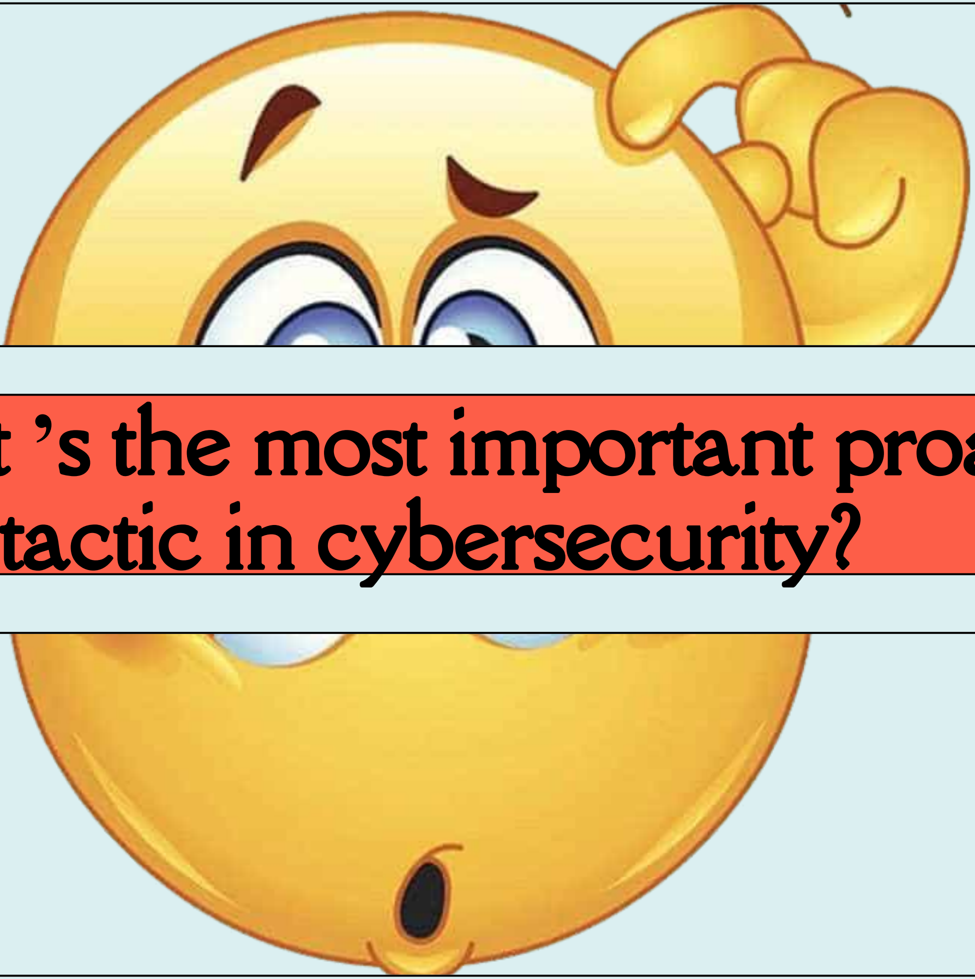
Definition : Cyber controls are technical, physical, or managerial features that are meant to prevent, detect, or reduce the damage that is left from a cyberattack (CISA, 2023).

Preventative controls have the goal of stopping a breach from occurring **before** it happens.

Ex: Firewalls

<u>Proactively prevents breaches</u>

But what ’s the most important proactive tactic in cybersecurity?



Safe Online Practice, of course!

Safe Online Practices

IBM reports that '83% of organizations reported insider attacks in 2024', so major businesses need to prioritize teaching and encouraging their team to understand how to navigate the internet safely (Nadeau, 2024).

Human 's are the most important cybersecurity layer!

Employee Trainings, Posters, Policies, etc

Safe Online Practices should be **prioritized** , not **neglected** !

CYBERSECURITY POLICY

Why have policy, especially in cybersecurity?

Answer:

Fix the issue of human error

What is cybersecurity policy?

Why even have it?

Establishes security guidelines for all employees that must be complied with

How to set a strong, secure password

Enable multi-factor authentication (MFA or 2FA)

When should a password be reset

Roles and responsibilities (access control)

Regularly assess employees on security knowledge (how to spot a phishing email)

Philosophical Topic

Are we adequately thinking through the long-term impact of technologies being developed today (the short arm of predictive knowledge)?

Yes? No? Maybe so ...?

We say NO!

And here ’s why …

The Shortarm of Predictive Knowledge

1

It's impossible to predict the impacts of technology! Oh no!

2

New technology oftentimes has undiscovered vulnerabilities or can bring more negative consequences.

EX:

Breaking into home WiFis through a tea kettle?!?

TED Talk Clip

This is an example of the unexpected consequences of modern technology, which can not be completely predicted or avoided.

How do we combat this?

It's impossible to avoid **all** consequences of new technology. Instead, we can **reduce** the impacts of new technology.

Through understanding

The CIA Triad

Malware

Proactivity within cybersecurity

& Cyber Policy

Individuals can protect their information as best as they can in this evolving climate.

Final thoughts

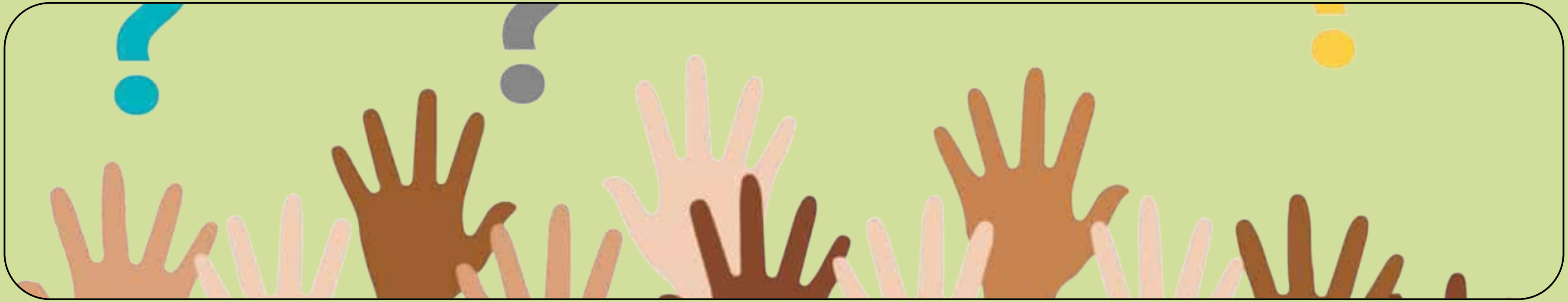
Cybersecurity is the prioritization of internet safety! It's used to protect the confidentiality, integrity, and availability of information.

Cybersecurity has the job of protecting against malware, such as adware, worms, etc.

Cybersecurity is best done proactivity

Cybersecurity policies gives companies a blueprint of how to defend systems.

While we can't predict technological consequences, we can protect against significant damage.



Any Questions?

THANK YOU

Kerina Drummond
Didi Caceres
Micaiah Cogshell
Diane Gilzow