

Basic Cybersecurity Principles

An abstract graphic featuring a network of white lines and dots on a blue background. The lines connect various points, creating a complex, web-like structure that resembles a digital network or a molecular model. The background is a gradient of blue, with a lighter greenish-blue area in the bottom right corner.

What is cybersecurity?

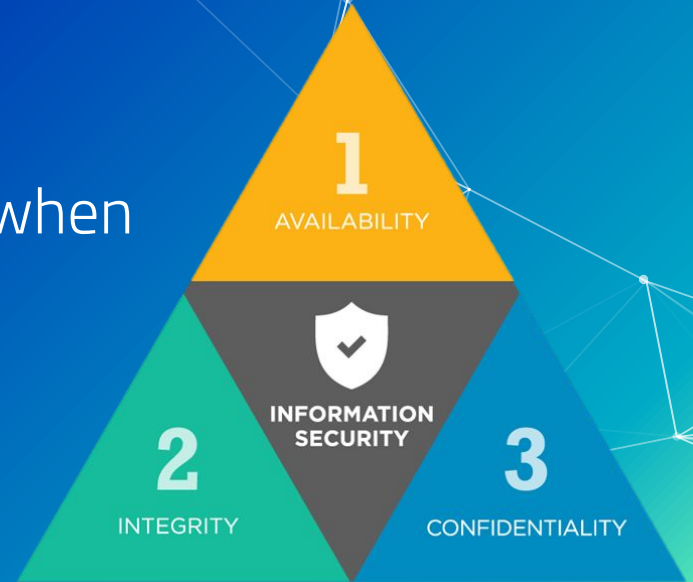
cybersecurity or information security is the protection of computer systems and networks from theft or damage to hardware, software, or electronic data and the disruption or misdirection of the services they provide

CIA Triad

Confidentiality: ensure that only authorized people have access to data

Integrity: ensure that data can be trusted

Availability: ensure that data is available when needed



Let's Make some Analogies

- Confidentiality: Imposter(s) going into the vents
- Integrity: Name every task
- Availability: Players making alibis for each other



Flexibility

Since hackers are often coming up with new ways to attack systems, so must those who are securing the systems.

- Zero-day vulnerabilities

Risk Management

It is impossible for us to solve all problems, so instead in cyber we target the problems that are the riskiest first.

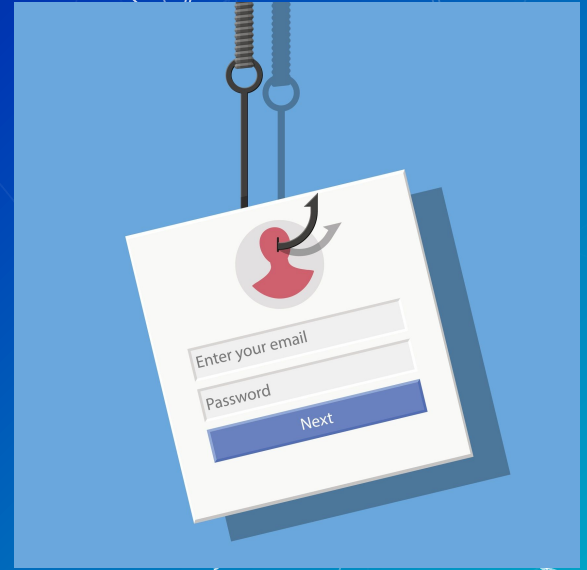
- 1) Identify
- 2) Assess
- 3) Strategize
- 4) Implement
- 5) Monitor



Human Error

Humans are largely what lead to system exploitation, not flaws in the system itself.

- e.g. phishing, visiting unsecure websites, accidentally installing viruses



User Education



Because the weakest link is the person, it is important that people are aware of basic cybersecurity concepts.

- use a secure password that is not the same across all sites
- visit safe/not shady sites
- verify the identity of callers/email senders
- do not click on unknown links

Detection vs. Prevention

Detection:

- Finding suspicious connections on a network
- Looking for unauthorized users
- IS ACTIVE

Prevention:

- Setting password requirements
- Configuring firewall rules
- IS NOT ACTIVE
- Mainly what CyberPatriot focuses on

NYES! More Among Us Analogies!

As a crewmate, how can you **detect** the imposter?

How can you **prevent** the imposters from killing you?



Which is more important?

Detection, not necessarily because it is more effective, but because nowadays preventative measures are not enough to stop cyber threats.

- Prevention can only stop so much
 - e.g. Zero-day vulnerabilities can appear
- Thorough detection ensures that the damage to a system/data is minimized

Now let's try to apply what we learned last week to cyber security.

- How can permissions be insecure?
- Which letter in CIA pertains to this security aspect?
- Which method does this fall under?
- What permissions would you say are the most secure?

```
# ls -l file
-rw-r--r-- 1 root root 0 Nov 19 23:49 file
```

Diagram illustrating the permissions `-rw-r--r--`:

- File type**: Indicated by the first character `-` (regular file).
- Owner (rw-)**: The first three characters `rw-` represent the permissions for the owner.
- Group (r- -)**: The next three characters `r- -` represent the permissions for the group.
- Other (r- -)**: The last three characters `r- -` represent the permissions for others.

Legend:

- `r` = Readable
- `w` = Writeable
- `x` = Executable
- `-` = Denied