WELCOME

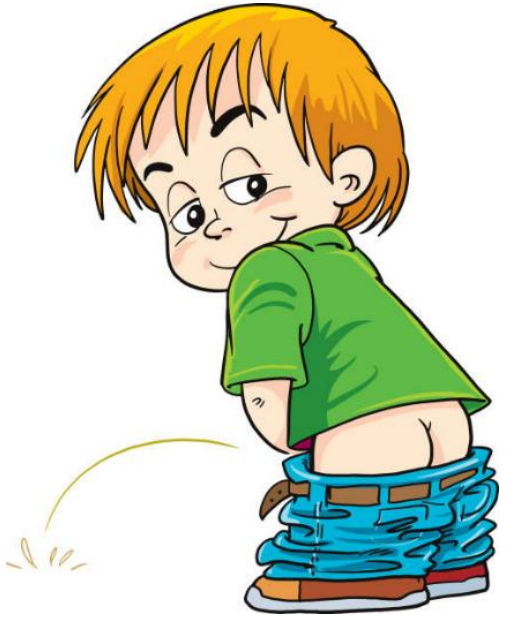
RESERVE COMMAND
TAGAPAGBUO NG HUKBONG MAMAMAYAN
PHILIPPINE ARMY

CADETS

SAFETY AWARENESS

EMERGENCY
PHONE NUMBER

CLASSROOM RULES



Finds your way towards the toilet silently when you feel the urge

If there is any question, just write it down on the comment box for those who are online, for the F2F keep your question to yourself and wait to be acknowledged

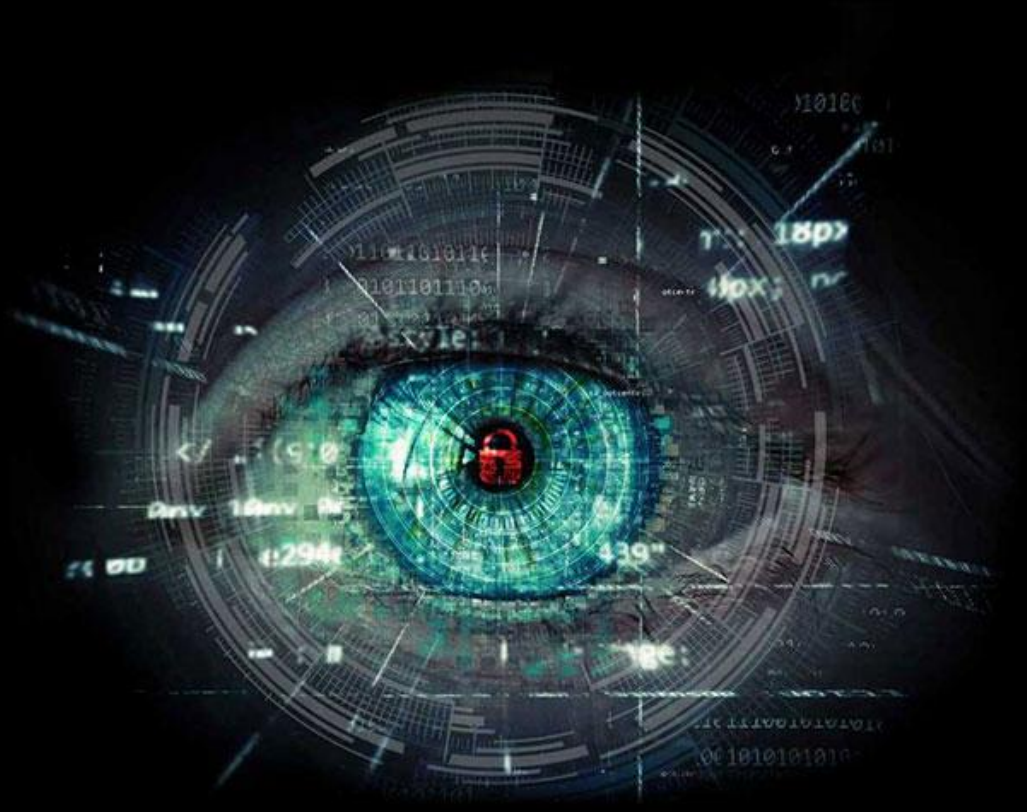
Be responsible to keep yourself awake

References

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
https://www.itgovernance.co.uk/blog/what-are-the-10-steps-to-cyber-security

Cyber Security

TERMINAL LEARNING OBJECTIVE



01

ACTION:
Discuss cyber security, cyber safety tips, RA 10175 and identify the types of cyber threats.

02

CONDITION:
Given in an online and face to face classroom environment, power point presentation

03

STANDARD:
The student must:
Protect and defend computer systems and networks from cybersecurity attacks.

SCOPE OF LEARNING

Cyber Security

Types of Cyber Threats

Different Types of Malware

Cyber Safety Tips

10 Steps to Cyber Security

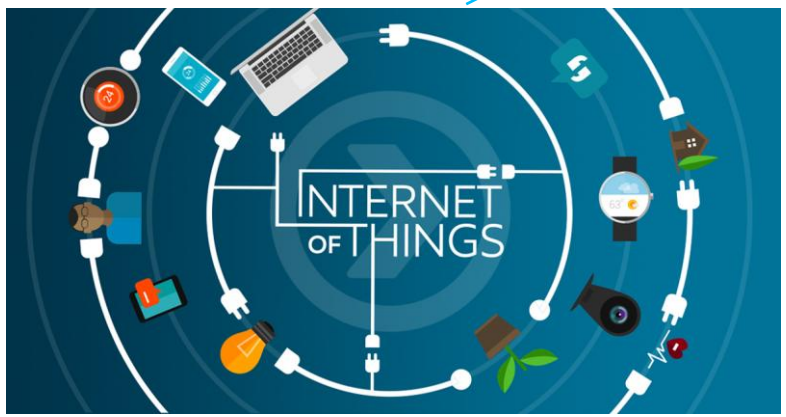
REPUBLIC ACT NO. 10175

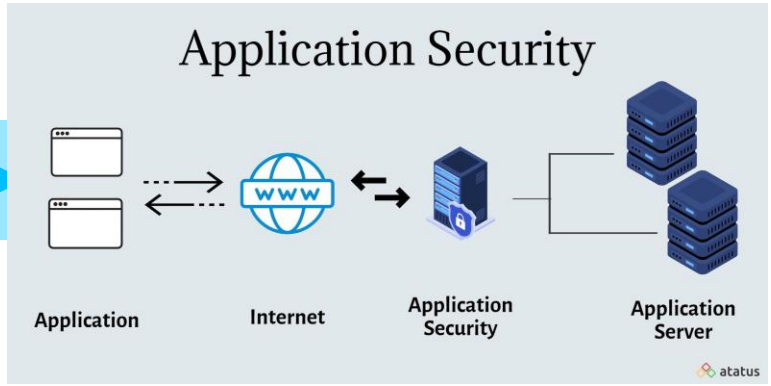
Cybercrime Prevention Act of 2012

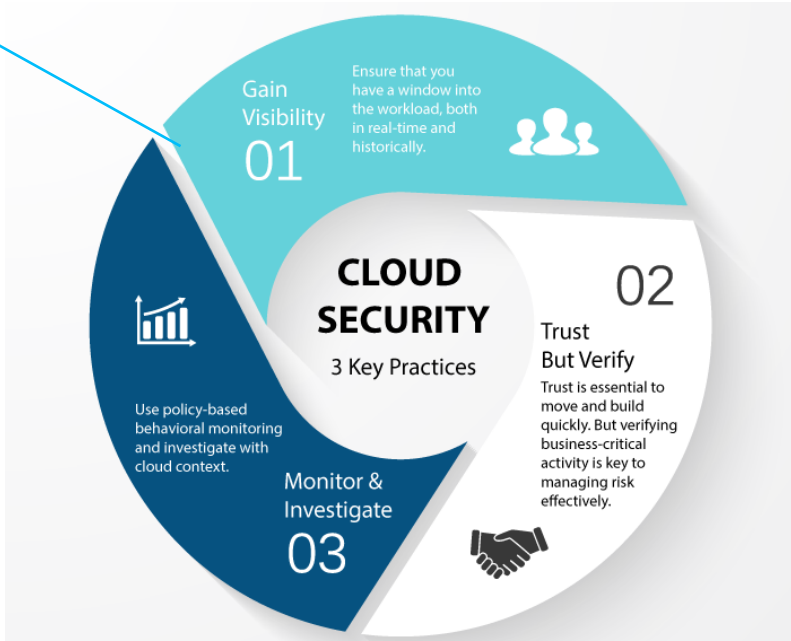
Cyber Security

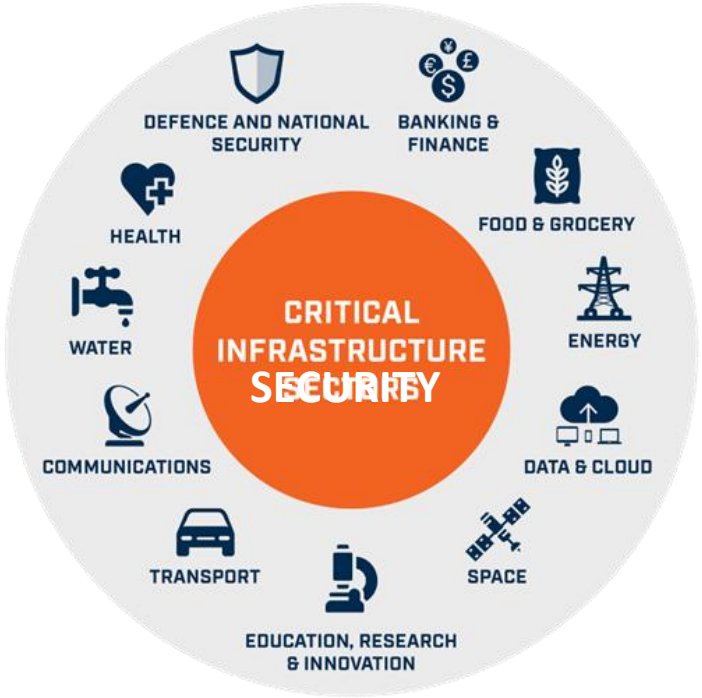
Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Cybersecurity can be categorized into five distinct types:









Critical Infrastructure security is of paramount importance in protecting systems and services that are essential to society and the economy: power and water distribution networks, transport and communications grids. The real-world, high profile consequences of a cyber-attack could include service disruption, environmental damage, financial loss and personal injury on a large scale.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Cloud security, also known as **cloud computing security**, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection


Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Internet of Things security can be understood as a cybersecurity strategy and protection mechanism that safeguards against the possibility of cyberattacks which specifically target physical IoT devices that are connected to the network.

The threats countered by cyber-security are three-fold:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.
2. Cyber-attack often involves politically motivated information gathering.
3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

Malware (malicious software)

One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

Virus

A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans

A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware

A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

There are a number of different types of malware, including:

Ransomware

Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware

Advertising software which can be used to spread malware.

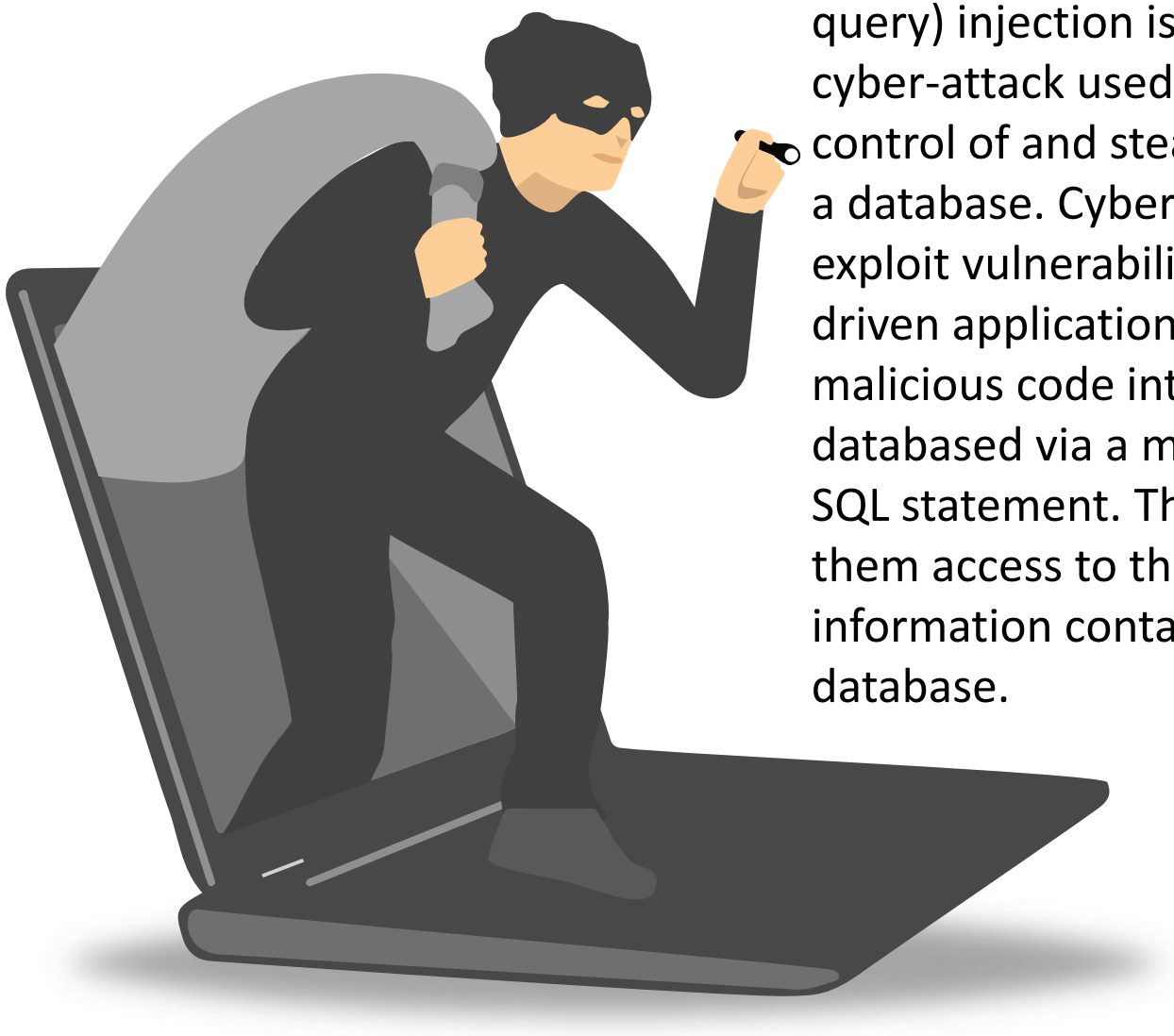
Botnets

Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

There are a number of different types of malware, including:



SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data.

Cyber Safety Tips

protect yourself against cyberattacks

1. Update your software and operating system
2. Use anti-virus software
3. Use strong passwords
4. Do not open email attachments from unknown senders
5. Do not click on links in emails from unknown senders or unfamiliar websites
6. Avoid using unsecure WiFi networks in public places

REPUBLIC ACT NO. 10175

AN ACT **DEFINING CYBERCRIME,** PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES.

This Act shall be known as the "Cybercrime Prevention Act of 2012”.

The Cybercrime Prevention Act of 2012 focuses on the pre-emption, prevention, and prosecution of cybercrimes such as offenses against the privacy, confidentiality, integrity, and availability of computer data and systems, computer-related offenses, and content-related offenses.

PUNISHABLE ACTS

Cybercrime Offenses.

The following acts constitute the offense of cybercrime punishable under this Act:

a. Offenses against the confidentiality, integrity and availability of computer data and systems:

- Illegal Access
- Illegal Interception
- Data Interference
- System Interference
- Misuse of Devices.
- Cyber-squatting

b. Computer-related Offenses:

- Computer-related Forgery
- Computer-related Fraud
- Computer-related Identity Theft

PUNISHABLE ACTS

Cybercrime Offenses.

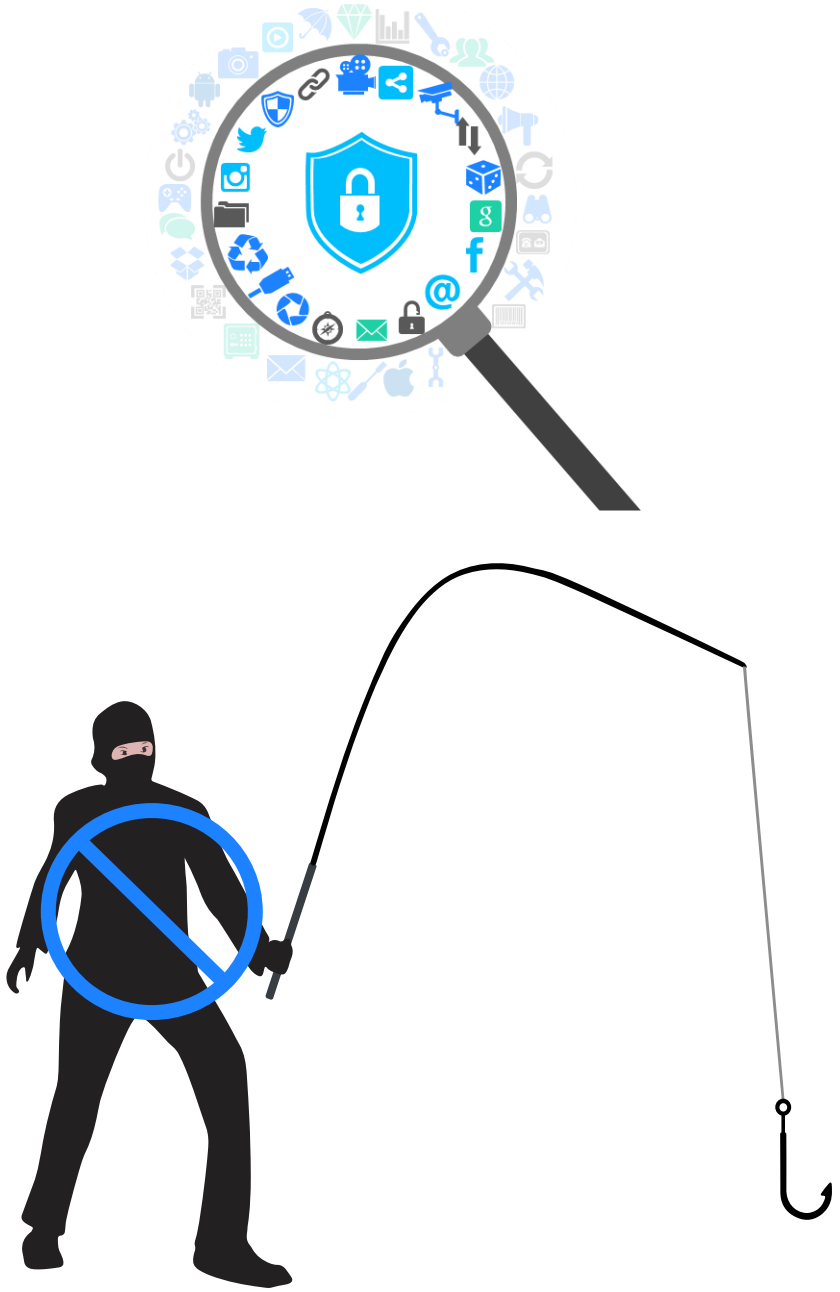
The following acts constitute the offense of cybercrime punishable under this Act:

c. Content-related Offenses:

- Cybersex
- Child Pornography
- Unsolicited Commercial Communications
- Libel

Other Offenses

- Aiding or abetting in the Commission of Cybercrime
- Attempt in the Commission of Cybercrime



The Cybercrime Prevention Act of 2012 penalizes offenses against the privacy, confidentiality, integrity, and availability of computer data and systems, such as illegal access, unauthorized interference, system interference, data interference, misuse of devices, and cybersquatting. In this context, cybersquatting is defined as the acquisition of domain names on the internet in bad faith or with the intent to gain profit, mislead, destroy one's reputation or deprive others of registering or creating an account to the domain name involved. Also, the Cybercrime Prevention Act of 2012 covers any digital fraud, computer-related forgery, and identity theft.

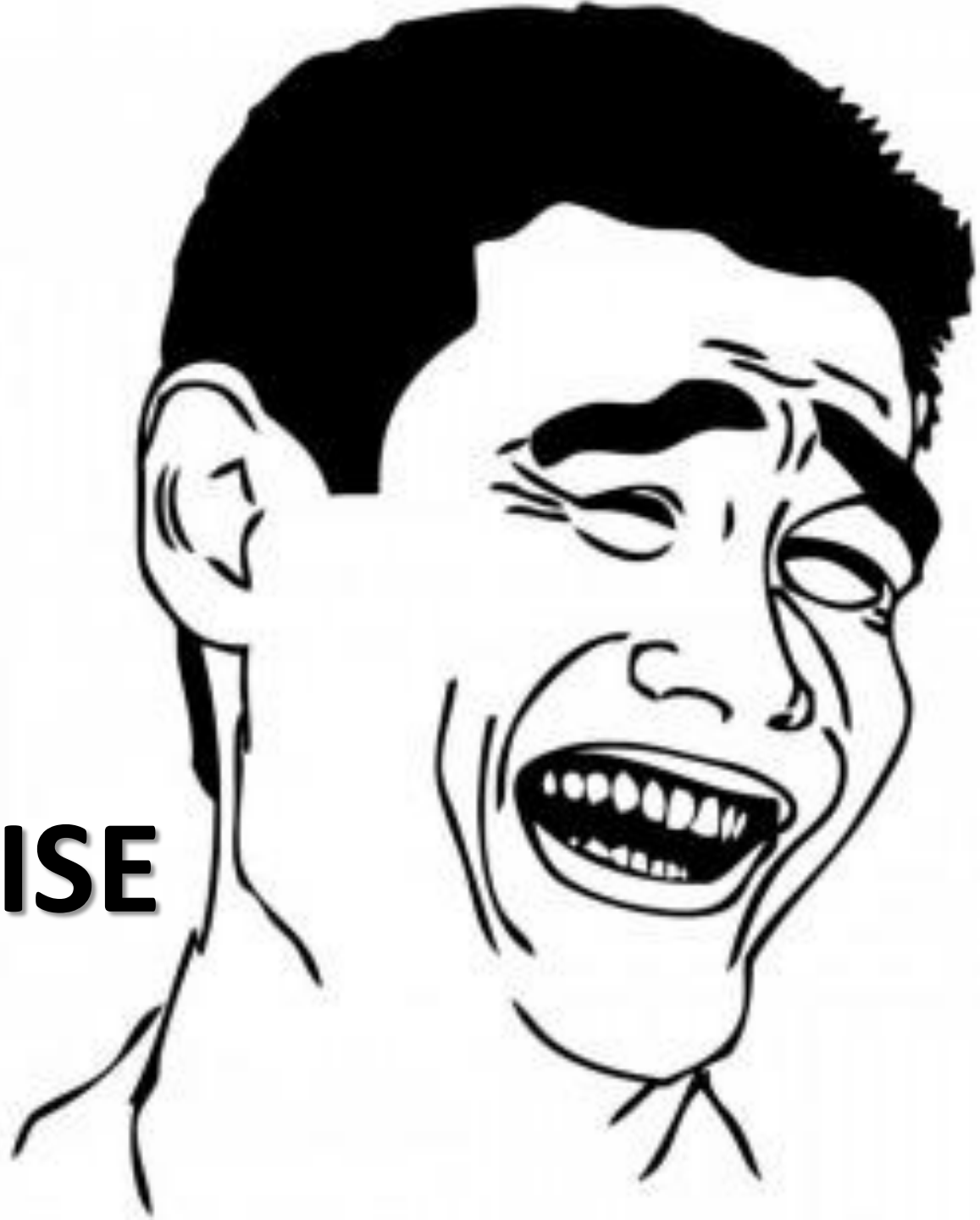
Any QUESTION???


THANK YOU
And
Good Day!
Enter
Shift

UWIAN NA!

MAY QUIZ PA!

CADETS GET ½ CROSSWISE



1-5.) Categorized cybersecurity into five distinct types.
6. What is Malware?
7-10.) Give at least 4 different types of malware.
11-16.) What are the offenses against the confidentiality, integrity and availability of computer data and systems?
17-20.) What are the 4 Content-related Offenses?

Essay

How can you protect and defend computer systems and networks from cybersecurity attacks?

THANK YOU