

C11: Social, Ethical, Legal and Economic Issues (Part 2)

Understand the importance of ethics in the conduct of Computing Professionals
Be aware of the impact of Computing in different real-life situations.



Syllabus

3.4.1 Understand the code of ethics (conduct) of a Computing professional.

3.4.2 Describe the impact of computing on lifestyle and workplace for social and economic developments.

3.4.3 Discuss the social, ethical, legal and economic issues of computing and technology.



Impact of Computing in many Sectors

- ▶ Communication (Facebook, Instagram, Google, SpaceX Starlink)
- ▶ Education (Google Classroom/Docs, Student Learning Space)
- ▶ Finance (Cryptocurrency, Kickstarter)
- ▶ Transport (Grab/Uber/Tesla)
- ▶ Data Storage (Cloud/Digital Footprint)
- ▶ Utility (GPS/3D Printing)
- ▶ Devices (Internet-of-things/Monitoring/Surveillance/Drones)

What are the other examples of businesses, that used computing to impact/change the existing industry?



Contents

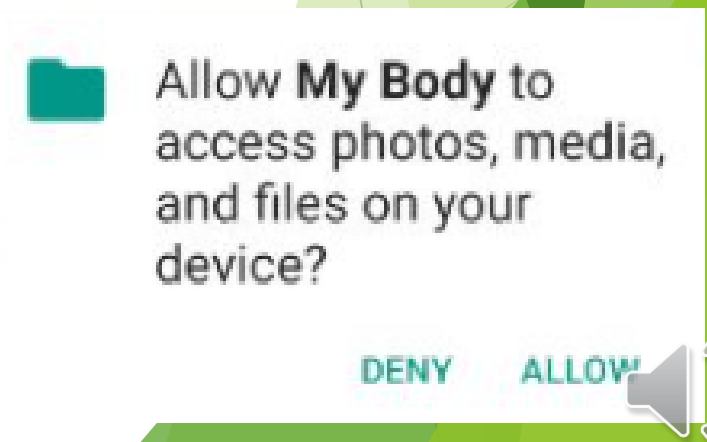
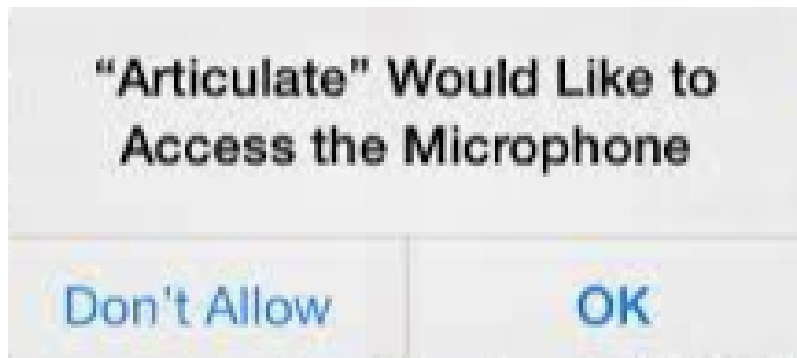
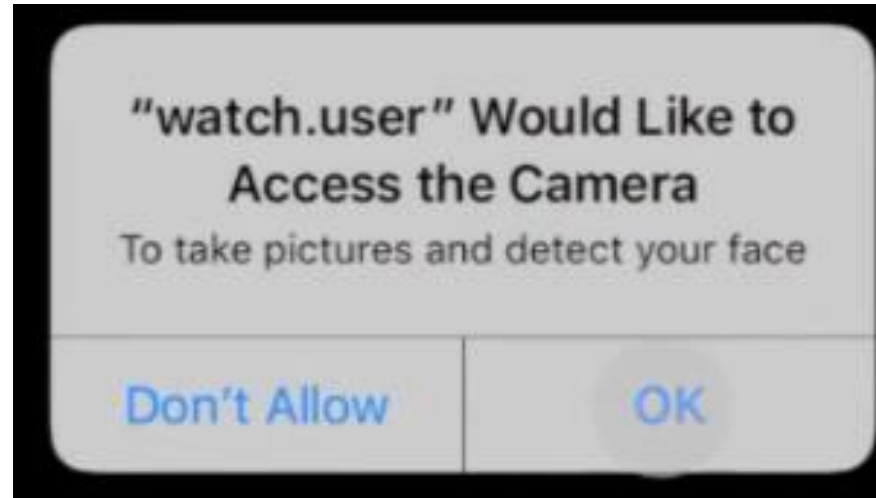
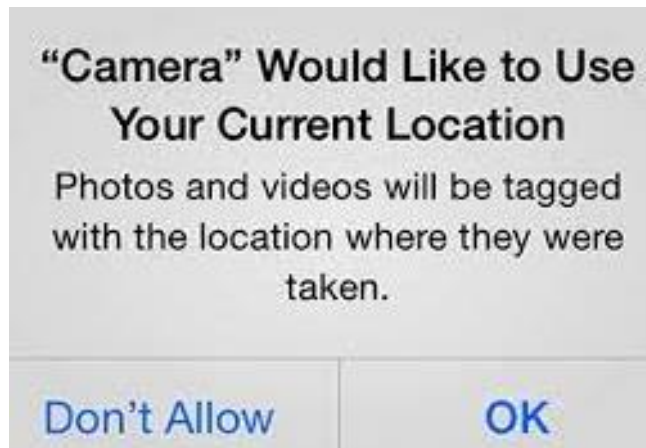
Impact of Computing

1. Communication
2. Cybersecurity
3. Artificial Intelligence (AI)
4. Jobs
5. Data Mining
6. Cryptocurrency



1. Communication: Smartphone Owners

Device asks for your permission



1. Communication: Publishing Information Online

- ▶ “I scratched some random guy’s car”
- ▶ “I sell my homework, pm me”
- ▶ “XYZ celebrity’s phone number is 91234567”
- ▶ “... is a jerk. He can go jump down the building!”
- ▶ “Look at how I wear my school uniform”
- ▶ “XYZ is a lying cheating scumbag!”
- ▶ “Look at my pictures: At Starbarks, Outside my house, Outside my school”

Opinion? Fact? Fake News? Exposing personal information? Bad behaviour? Threats?



1. Communication: Publishing Information

With great power, comes great responsibility

Education in Cyberwellness:

- ▶ Exploring online, safely and confidently
- ▶ Responsible use, respect others
- ▶ Avoid gaming addiction

Law:

Protection from Harassment Act

Protection from Online Falsehoods and Manipulation Act



1. Communication: Publishing Information

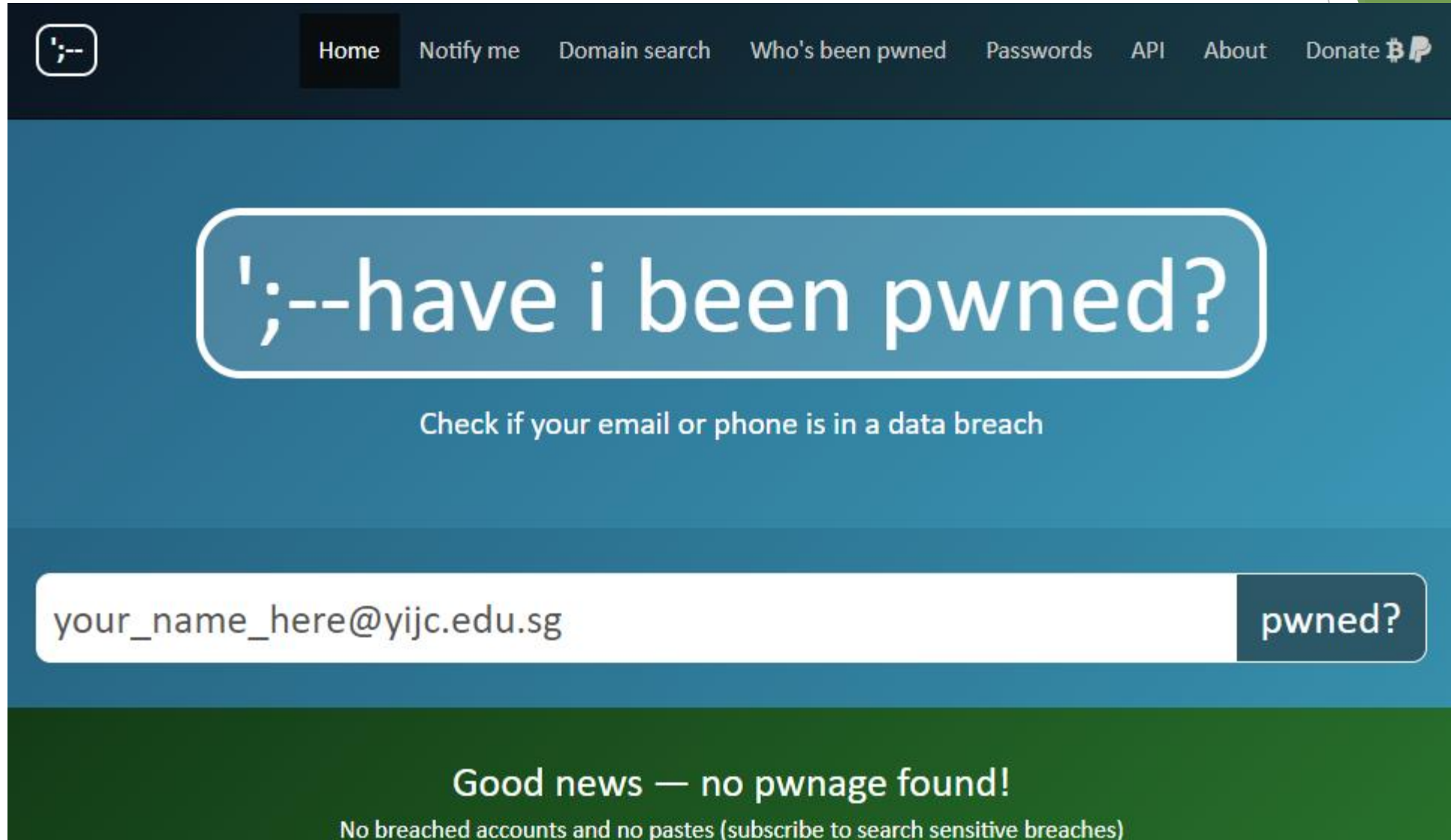
Cancel Culture

- ▶ What is Cancel Culture?
- ▶ How does it affect the targeted individual?
- ▶ How does it affect his/her employment?
- ▶ Is it legal or does it fall under the Harassment Act?



2. Cybersecurity

<https://haveibeenpwned.com/>



The screenshot shows the homepage of the 'Have I Been Pwned' website. The navigation bar at the top includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' with a subtitle 'Check if your email or phone is in a data breach'. A search input field contains the email 'your_name_here@yijc.edu.sg' and a 'pwned?' button. The result section displays 'Good news — no pwnage found!' and 'No breached accounts and no pastes (subscribe to search sensitive breaches)'.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

your_name_here@yijc.edu.sg pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)



2. Cybersecurity

Cybersecurity Breaches: Was it your fault?

What exactly are we securing/protecting?



2. Cybersecurity

What exactly are we securing/protecting?

We spend a lot of effort and expense to protect **information and infrastructure**

Basic principles

#1 Security is a **process**, not a product

#2 Protect **information**, not technology

#3 Security enables business + technology, while **minimizing risk**. It doesn't stop business.

#4 It's **impossible** to anticipate, mitigate and guarantee **against every single threat** out there, and it's not valuable to do so, either.



2. Cybersecurity

CIA Triad: Protecting information

Confidentiality

The ability to protect data from those not **authorised to view it**.

Data 'breaches' are commonly associated with loss of confidentiality

Integrity

The ability to prevent data from being **changed in an unauthorised or undesirable manner**.

What would it take for us to be able to reverse those changes?

Availability

The ability to gain **authorised access to data when we need it**



2. Cybersecurity

Threats and attacks

An asset (e.g. data, servers, support systems) might have one or more **vulnerabilities that can be exploited** by a threat agent in a threat action.

As a result, the confidentiality, integrity or availability of resources may be compromised.



2. Cybersecurity

Vulnerability + Threat Agent → Threat

Vulnerability

A weakness, or finding that is non-compliant to a requirement, specification or a standard

our unprotected area of an otherwise secure system,

which leaves the system open to potential attack or other problem

e.g. buffer overflows, SQL injections, weak passwords



2. Cybersecurity

Vulnerability + Threat Agent → Threat

Threat agent

Has motive, opportunity and means to take advantage of a vulnerability, thereby realizing a threat

e.g. property/ID/Info thieves, vandals, activists, hackers, thrill seekers, botnet operators, competitors, insiders, natural threats



Threat agents

The logo for "Project Mayhem" features a central green hooded figure with a white play button icon on its chest. The figure is set against a black background with green splatters. The words "PROJECT" and "MAYHEM" are written vertically in green on the left and right sides, respectively. Below the figure, the text "Anti - IRS Scam - Call Flood" is written in white.

Revenge on a IRS Phone Scamming Company...

I am a security developer who tries to prevent victims from being scammed by different types of scams. These can be Tech Scams, Phone scams, and more. If you would like to help my personal development costs, then this is where to do it! Thanks!

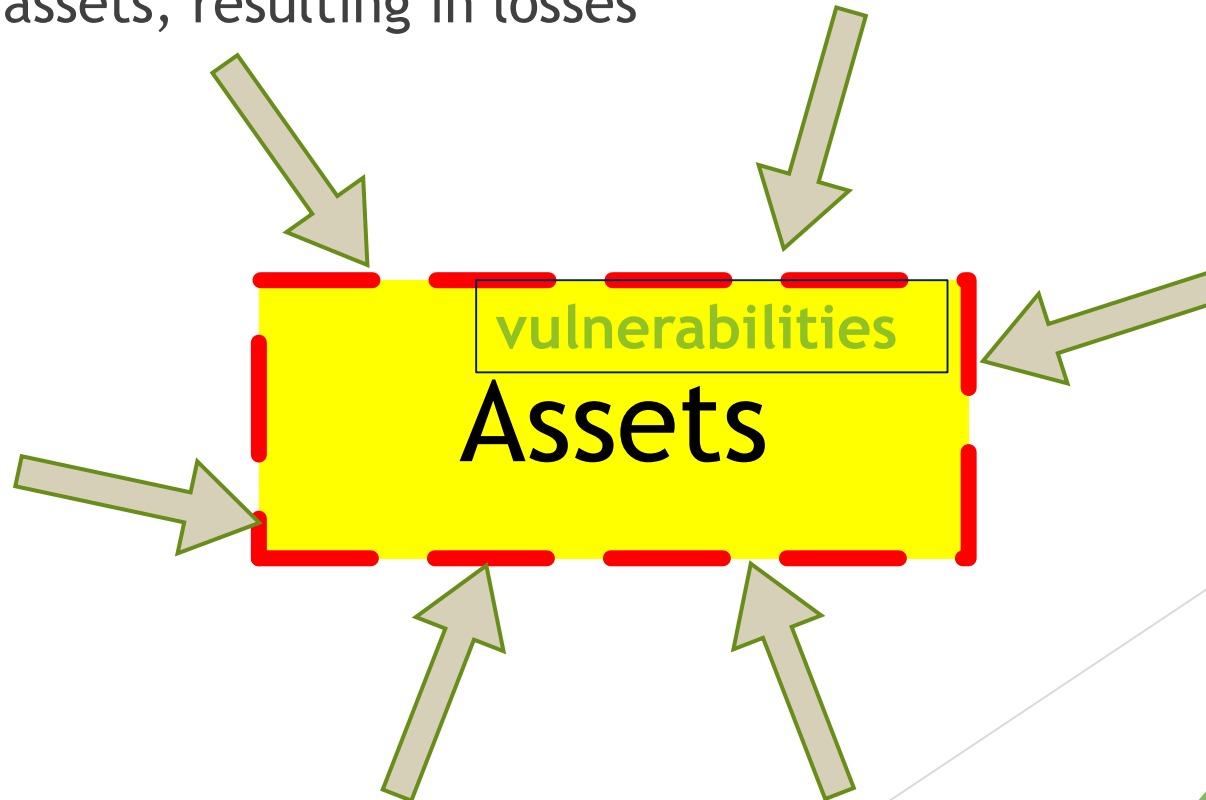


2. Cybersecurity

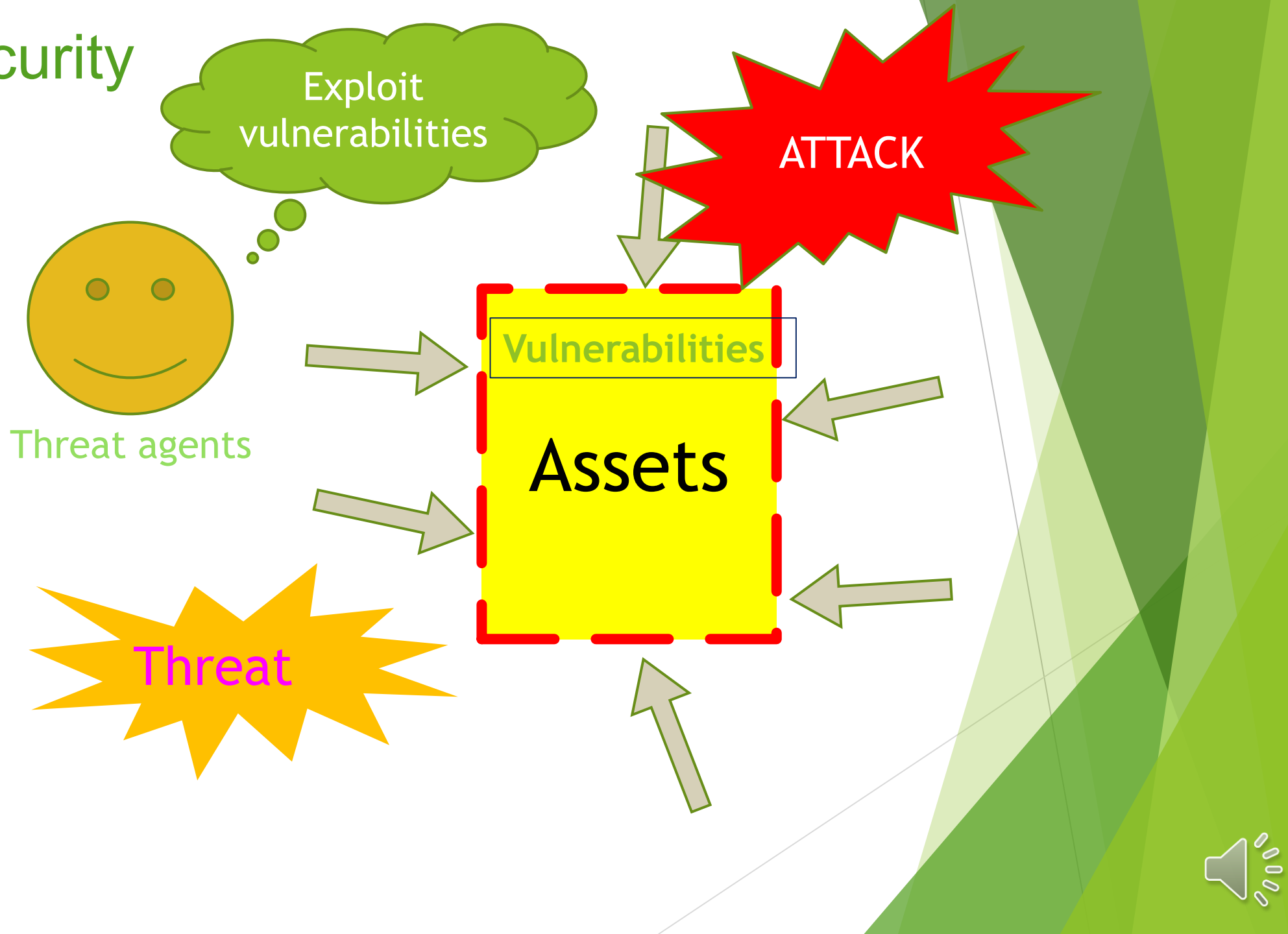
Vulnerability + Threat Agent → Threat

Threat

An event, process, activity, perpetuated by one or more threat agents, which when realized, has an adverse effect on organization assets, resulting in losses



2. Cybersecurity



2. Cybersecurity

Types of attack

Interception: unauthorised access to data, applications or environments

Fabrication: generating data, processes and communications in a system

Modification: tampering with an information asset

Interruption: causes assets to become un-usable on a temporary or permanent basis

Examples

malware, password cracks / brute force / dictionary, DoS / DDoS, man in the middle, TCP hijack, spam, social engineering, phishing, ransomware, ...

Common techniques used by cyber-attackers



2. Cybersecurity

Types of cyber-attack (Further readings)

Common examples

Interception:

Social Engineering

Phishing

Man-in-the-middle (MITM)

TCP hijacking

Password cracking

Fabrication:

Malware

Trojan horses

Virus

Worm

Modification:

SQL injection

Interruption:

Ransomware

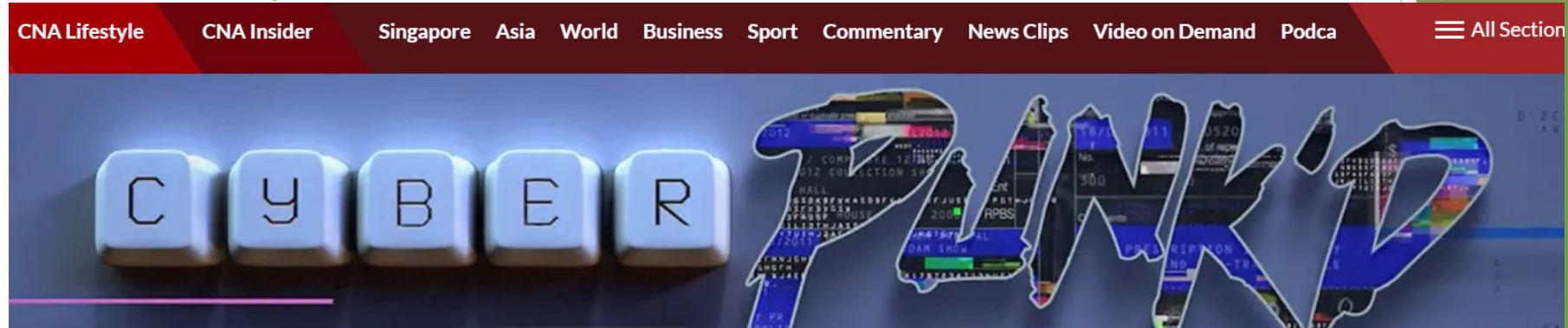
wannacry

Distributed Denial of Service (DDoS)

E.g. Starhub DDoS attacks



2. Cybersecurity 40 minute Video

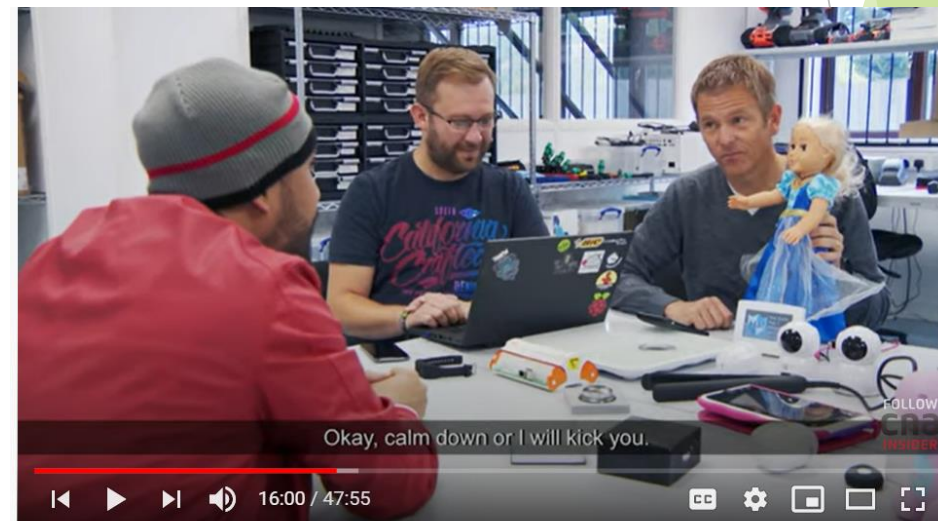


<https://www.channelnewsasia.com/news/video-on-demand/cyber-punkd>



#CNAInsider #CNAInsiderExplains #Cybersecurity

How to stay safe on the Internet: practice good cyber hygiene | CyberPunk'D | Part 1/2



#CNAInsider #CNAInsiderExplains #Cybersecurity

How to stay safe when using smart devices | CyberPunk'D | Part 2/2



2. Cybersecurity

Nationwide Education/Outreach on Cybersecurity

The Singapore Government is committed to building a strong cybersecurity culture ([Link](#))

Private Sector: (Cyber Security Agency of Singapore (CSA) enhances cybersecurity awareness: Talks, Conferences, Online Portal, Online resources)

Public Service: (IT security awareness programme)

General Public: (CSA's "Cyber Tips 4 You" programme, Total Defense: Digital Defense)



2. Cybersecurity

Cybersecurity Education for...

- ▶ Individuals: Social Engineering, Phishing, Doxxing, Ransomware, Identity Theft, Spyware: Invasion of Privacy, Cryptojacking, Brute Force Attacks
- ▶ Experts: CIA, Defense-in-depth
- ▶ Businesses: Data breach, IoT Product Vulnerabilities
- ▶ Nation: Total Defense 6th Pillar
- ▶ Updating Laws: Increased Regulation and Legislation



2. Cybersecurity



2. Cybersecurity



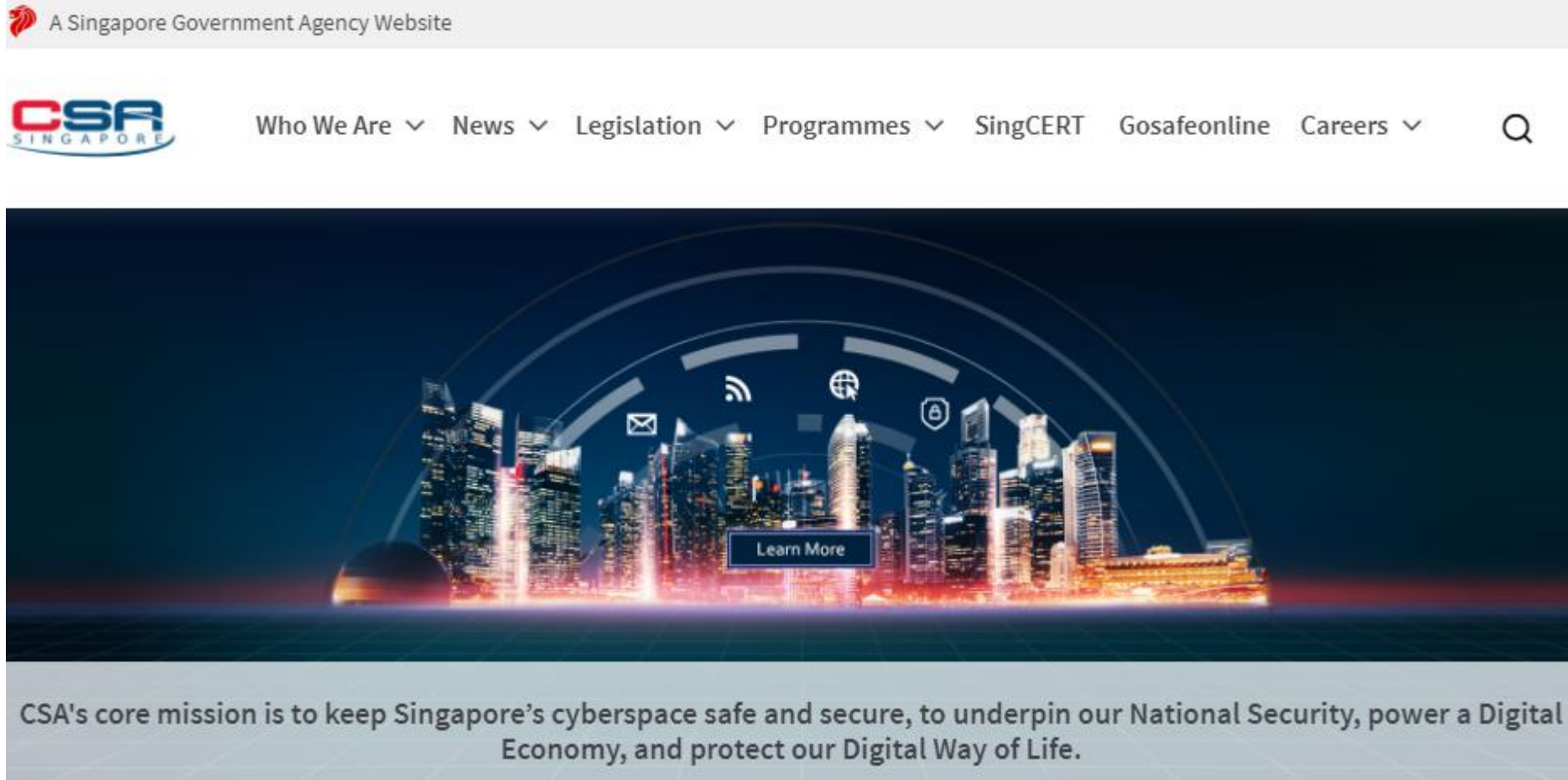
Online security is becoming more important than ever. While there's no bulletproof way to prevent a cyber attack, here are some easy tips to help you keep your personal information safe and secure.

Back up your data  <p>Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.</p>	Keep your operating system up to date  <p>Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.</p>	Install antivirus software  <p>Free online antivirus software can be fakes. Purchase antivirus software from a reputable company and run it regularly.</p>	Choose unique passwords  <p>Create unique passwords for each account - that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.</p>	Set up two-factor authentication (2FA)  <p>Choose to get a code sent to another device like your phone when logging in online - it helps stop hackers getting into your accounts.</p>	Use creative recovery answers  <p>Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.</p>
Be cautious of free WiFi networks  <p>Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.</p>	Be smart with social media  <p>What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.</p>	Don't give out personal info  <p>Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.</p>	Check bank statements regularly  <p>Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.</p>	Get a regular credit check  <p>An annual credit check will alert you if someone else is using your details to get loans or credit.</p>	<p>To report a cyber security problem, visit www.cert.govt.nz</p>



2. Cybersecurity

Cyber Security Agency of Singapore



<https://www.csa.gov.sg/gosafeonline>



2. Cybersecurity

Digital Defence

DIGITAL DEFENCE
BE SECURE, ALERT & RESPONSIBLE ONLINE

What is Digital Defence?

TOTAL DEFENCE

A new pillar of Total Defence to guard against threats from the digital domain.

Cyberattacks on critical infrastructure.

Hackers stealing personal data.

Spread of deliberate online falsehoods that could cause social unrest.

Most of us use digital devices in work and play. Good cyber hygiene, and vigilance against fake news is our defence.

As the first line of defence, Singaporeans can:

Adopt good cybersecurity practices to safeguard our personal data, devices and systems.

Be aware of phishing attacks and internet scams.

Use social media discerningly and responsibly.

Be vigilant against fake news and the spread of deliberate online falsehoods.

The new pillar will help strengthen Total Defence against the new threats of today.

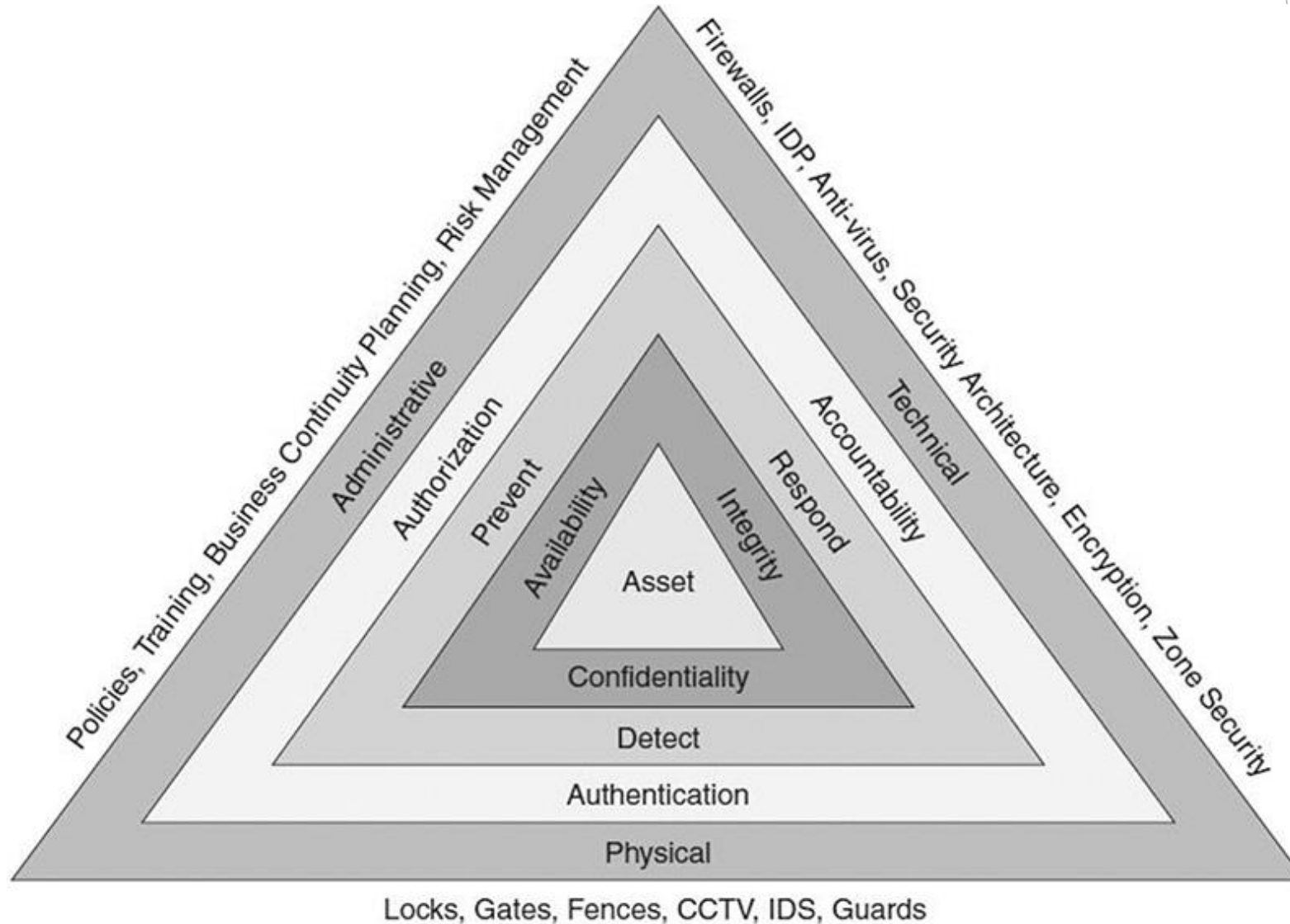
Military Defence Civil Defence Economic Defence Social Defence Psychological Defence Digital Defence

@WeAreTotalDefence @WeAreTotalDefence totaldefence.sg



2. Cybersecurity

Defence-in-depth approach



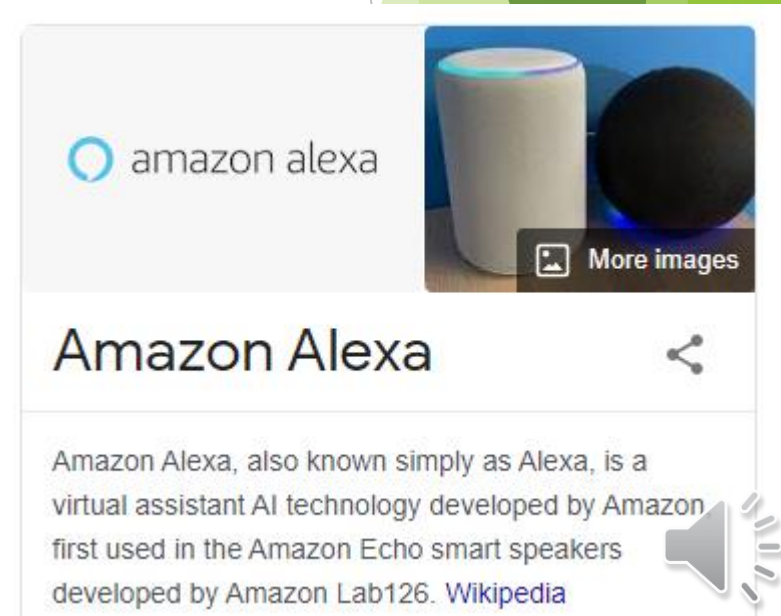
3. AI

Artificial Intelligence

Artificial Intelligence: Simulation of human intelligence processes by computer systems.

These processes include **learning** (the acquisition of information and rules for using the information), **reasoning** (using rules to reach approximate or definite conclusions) and **self-correction**.

Particular applications of AI include expert system speech recognition and machine vision.



3. AI

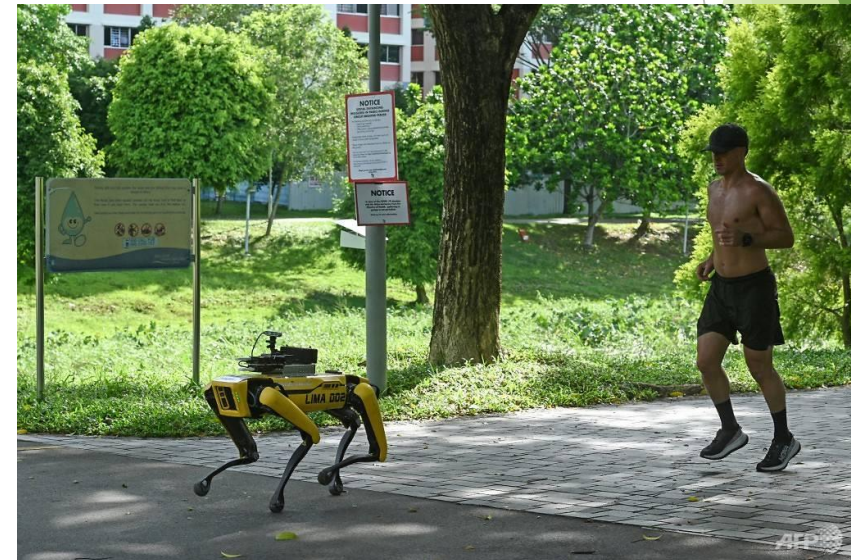
Luddite Horses

3. AI

AI can do Dangerous Jobs

Smart machines can come in handy in cases where there are manpower crunch

It may also be beneficial when it takes on tasks that humans shun or deem too dangerous



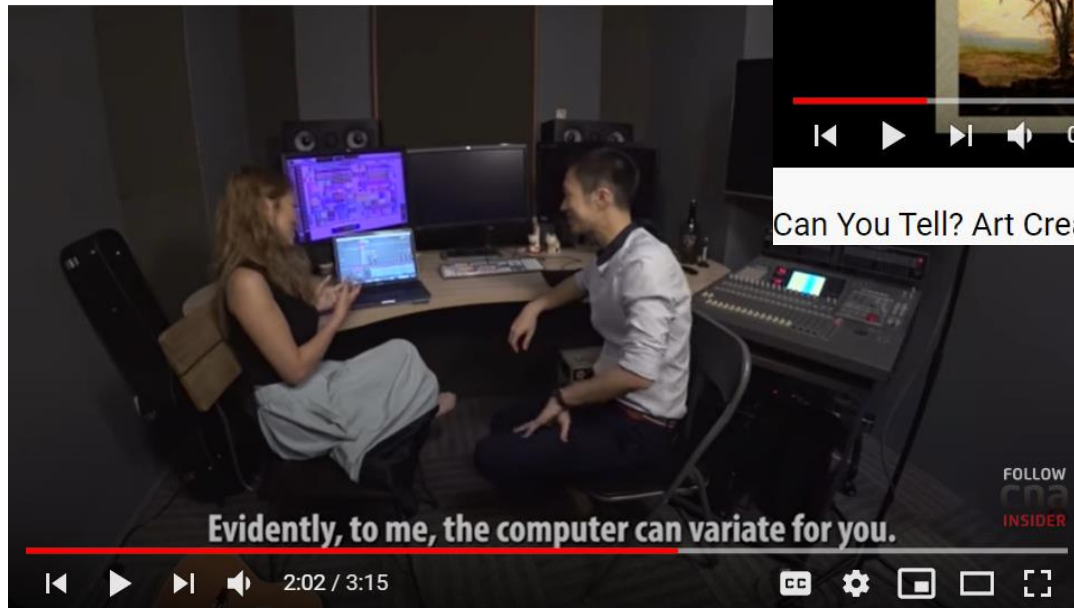
3. AI

Automation: AI replacing human



3. AI

Creativity no longer unique to humans?



#nowplaying #robotmusic #newmusic

How Inch Chua Uses Artificial Intelligence To Write Her Latest Hits



3. AI

IBM's AI takes on world-class debater in argument about preschool

KHARI JOHNSON @KHARIJOHNSON FEBRUARY 11, 2019 6:06 PM



Above: Project Debater

Image Credit: Khari Johnson / VentureBeat

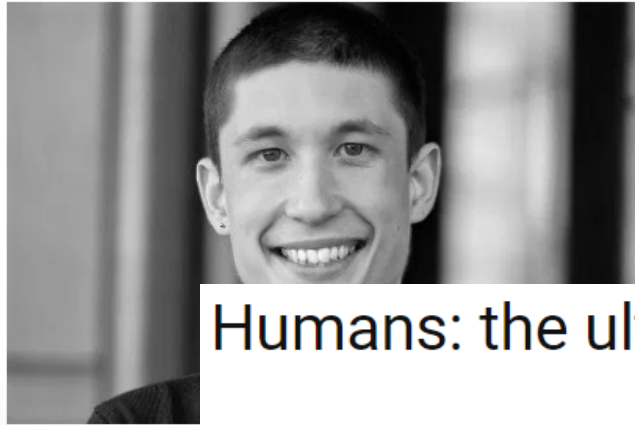
IBM's Project Debater, an AI system that can engage in live debate with humans, today faced off with 2016 World Debating Championship grand finalist and 2012 European Debate champion Harish Natarajan. The debate was about preschool subsidies, with Project Debater arguing in favor and Natarajan arguing against.



3. AI

Biasness in Machine Learning

Three notable examples of AI bias



by **Michael McKenna, Toptal** 14 October 2019

In 2016, the World Economic Forum claimed we are experiencing the fourth wave of the Industrial Revolution: automation using cyber-

Humans: the ultimate source of bias in machine learning

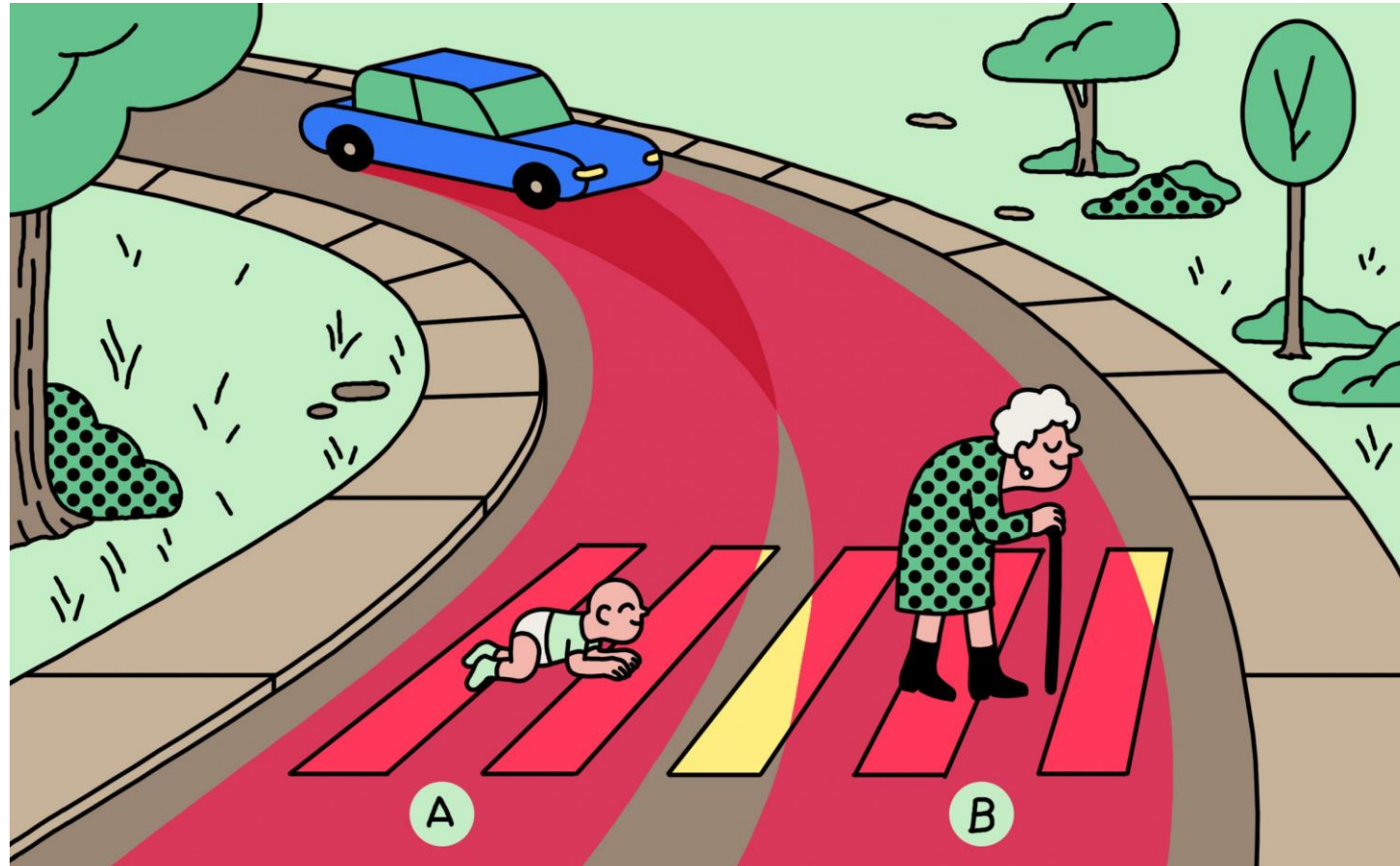
All models are made by humans and reflect human biases. Machine learning models can reflect the biases of organizational teams, of the designers in those teams, the data scientists who implement the models, and the data engineers that gather data. Naturally, they also reflect the bias inherent in the data itself. Just as we expect a level of trustworthiness from human decision-makers, we should expect and deliver a level of trustworthiness from our models.



3. AI

The Moral Machine

Who should die for the other to survive?



3. AI

Issues with AI:

Over-reliance on AI in decision making

- AI as machines that make moral decisions dealing with life and death
- How do we make a moral decision?

Code biases

- Inherent biases in algorithm
- AI can be as bias as humans
- Fighting biases in algorithm

4. Jobs

Which job are at risk?

- AI replaces tasks, not jobs



4. Jobs

Reliability of software

Dependence on computing is increasing.

Machines are moving from taking over tasks to assisting humans to make decisions.

It's important to understand how we can improve the reliability of our software, avoid failures, be aware of biases we build into in, and make machines morally capable.

How can we ensure that we will not be replaced by AI?

Social Media Influencer, Cybersecurity Specialist (White Hat Hacker), AI Engineer, Data Mining Engineer, Data Scientist, Data Protection Officer



5. Data Mining

What is Data Mining?

CS 300: The Computing Professional: Ethics Research Project Topics

A LibGuide to assist students in CS 300 with their history and ethics research projects.

[Home](#)[History Research Project Topics](#)[Ethics Research Project Topics](#)[Finding Articles](#)[Presenting](#)

ETHICS TOPIC SUGGESTIONS

[Adblock](#)
[Anonymity](#)
[Anonymous](#)
[Automated Driving](#)
[Blogging](#)
[Catfishing - No books](#)
[Censored Search Engines](#)
[Content Filters](#)
[Cryptography & Law](#)
[Cyberstalking](#)
[Data Mining](#)
[Database Copyrights](#)
[Database Integrity](#)
[Digital Rights Management](#)
[Digital Sampling](#)
[Digital Self-Help](#)
[Digital Wiretaps](#)
[Disability/Access](#)
[DMCA / Fair Use](#)
[Domain Names](#)
[Edward Snowden](#)
[Electronic Voting](#)
[Email Privacy](#)
[Export Restrictions](#)
[Facebook & Identity](#)
[Facebook & Privacy](#)
[Copyrights](#)

INSPIRATION

From the [New Jersey's Science & Technology University \(NJIT\) Channel](#): Uploaded on May 25, 2010 - NJIT School of Management professor Stephan P Kudyba describes what data mining is and how it is being used in the business world.



COMPUTING ETHICS WEBSITES

- [ACM Code of Ethics and Professional Conduct](#)
Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).
- [BBC Bitesize Ethics and Law](#)
There are laws that govern how we use computers. There are also ethical concerns about issues such as piracy, hacking and the environment.
- [Computer and information Ethics](#)
The Stanford Encyclopedia of Philosophy's essay on Computer and Information Ethics.
- [Computer Ethics Institute](#)
The Computer Ethics Institute has provided an advanced forum and resource for identifying, assessing and responding to ethical issues associated with the advancement of information technologies in society.



5. Data Mining

Applications:

- Behavioural analytics
 - Smart advertising
 - Profiling
- Optimization
 - Early detection of manufacturing issues
 - Yield Optimisation
 - Prediction models
- Machine Learning

Big Data, the new oil



The use of Big Data also has its own Principles on Ethics.



6. Cryptocurrency

What is cryptocurrency?

Bit Coin is the first of more than 5,000 cryptocurrencies in existence today. A new form of decentralized currency that can be used in society, used without an intermediary, with a public ledger accessible to everyone.

Legality varies in different countries.

The seller uses his public key is used to receive funds, and the buyer uses a private key to sign transactions to spend the funds.

When adding transactions to the public ledger, the unique codes used to recognize users' wallets and transactions must conform to the right encryption pattern, to be verified by the majority of all Bitcoin holders.

What are the other ways it impacts society and economy?

