C10 Ethics & Security

Part 2: Cyber-crime

Security

What exactly are we securing/protecting?

Security

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.

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?

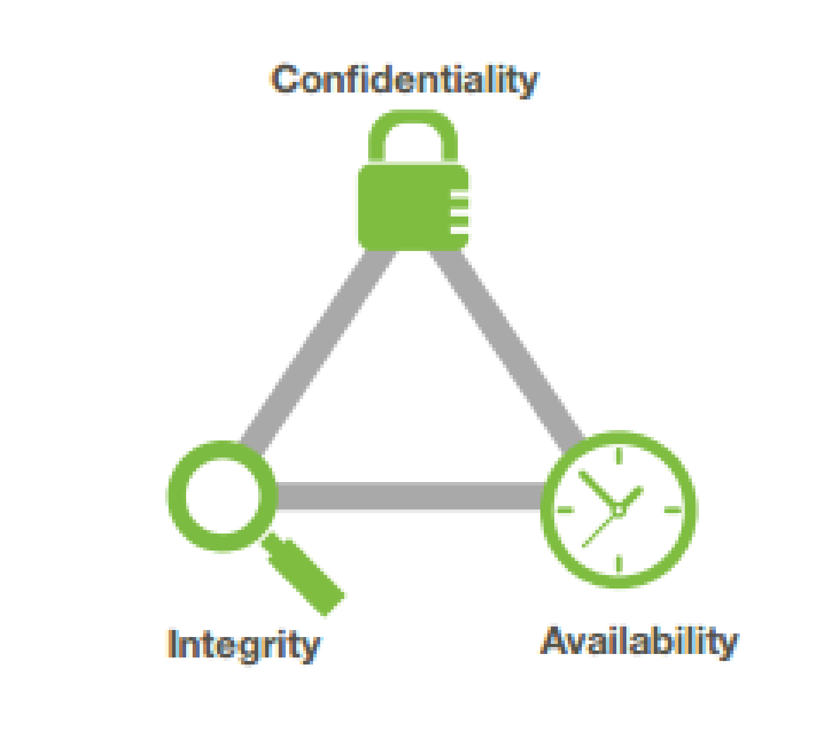
Availability

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

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.



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

vulnerabilities

Assets

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

Exploit vulnerabilities

Threat agents

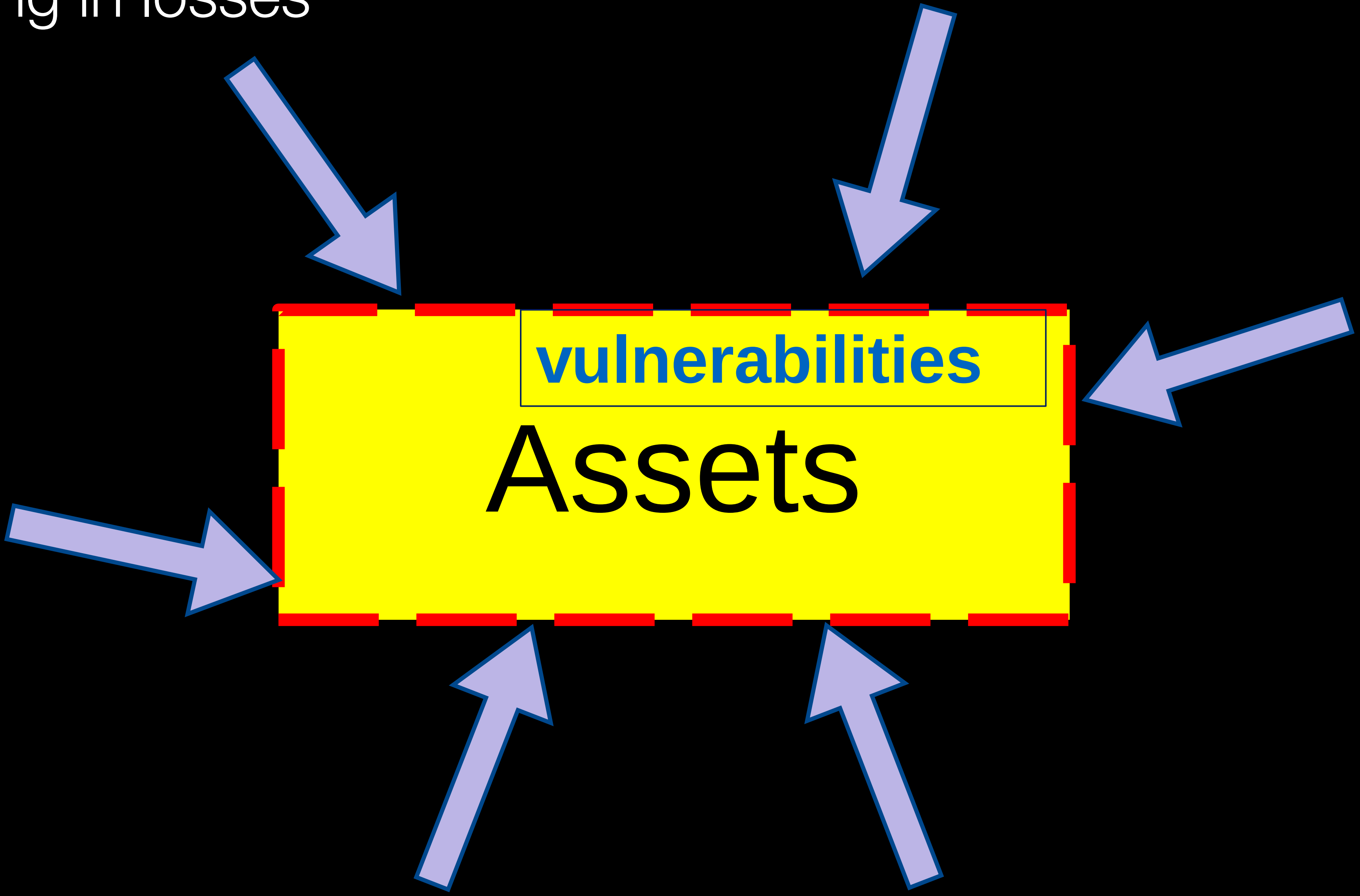
Revenge on a IRS Phone Scamming Company...

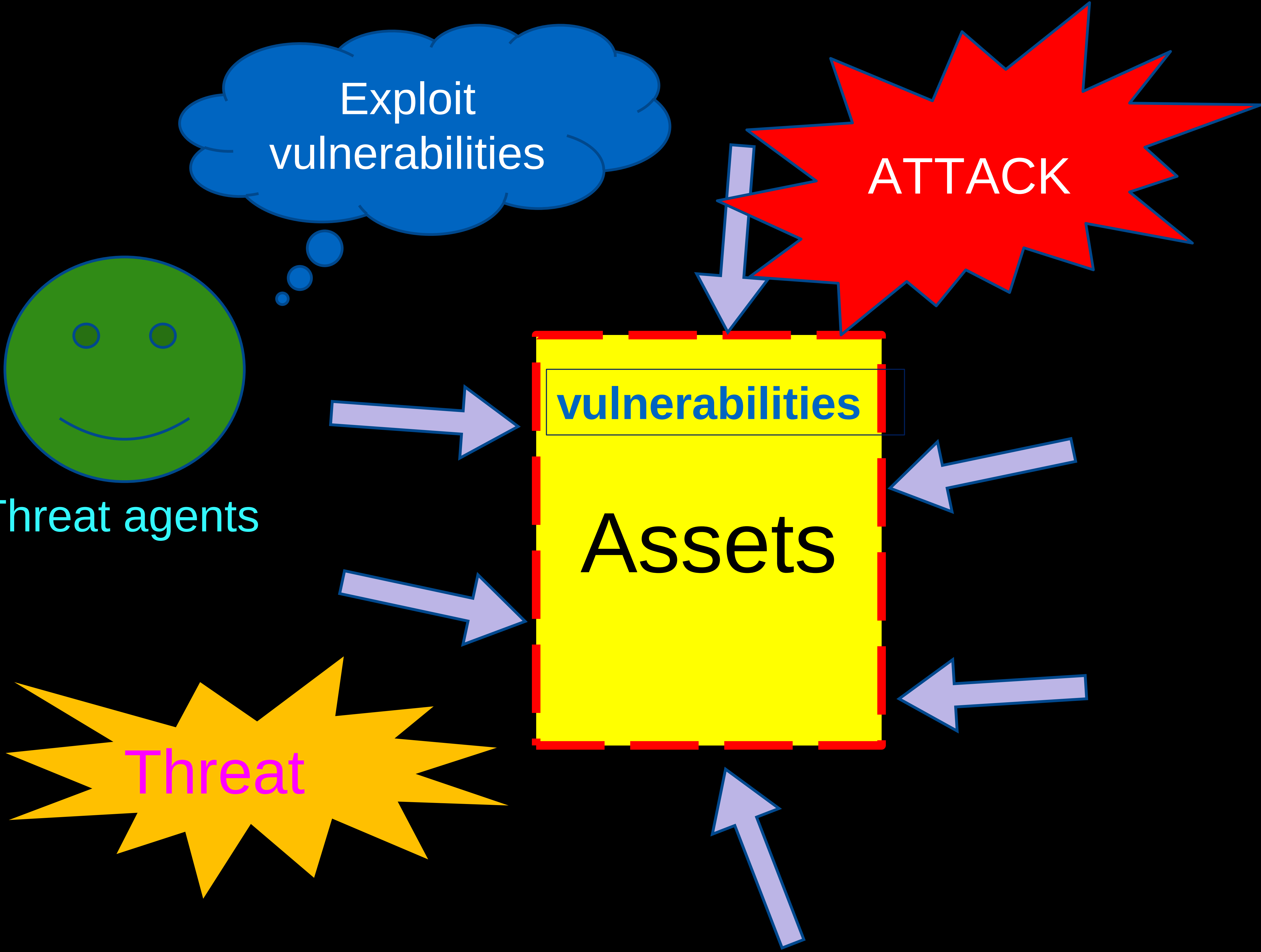
I am a security developer who tries to prevent victims from being scammed by different types of scams. These can be Tech Scams, Phone scams, and more. If you would like to help my personal development costs, then this is where to do it! Thanks!

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




Exploit vulnerabilities
ATTACK
vulnerabilities
Assets
Threat agents
Threat

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, …

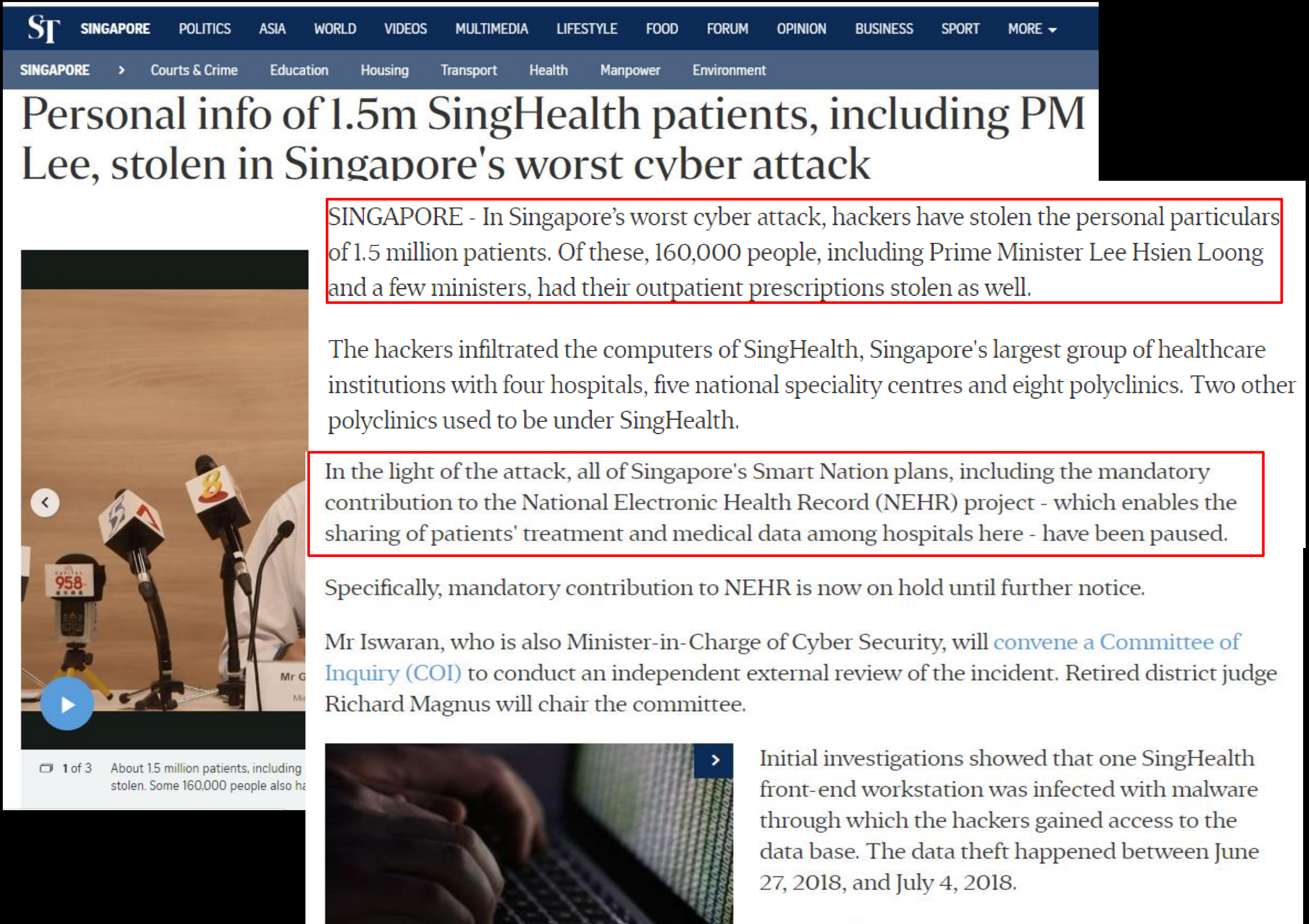
Common techniques used by cyber-attackers

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

Examples of cyber-attack incidents:
Equifax
Singhealth fined
Starhub broadband

Singhealth Data Breach



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

SINGAPORE - In Singapore's worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.

The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

In the light of the attack, all of Singapore's Smart Nation plans, including the mandatory contribution to the National Electronic Health Record (NEHR) project - which enables the sharing of patients' treatment and medical data among hospitals here - have been paused.

Specifically, mandatory contribution to NEHR is now on hold until further notice.

Mr Iswaran, who is also Minister-in-Charge of Cyber Security, will convene a Committee of Inquiry (COI) to conduct an independent external review of the incident. Retired district judge Richard Magnus will chair the committee.

1 of 3 About 1.5 million patients, including
stolen. Some 160,000 people also ha

Initial investigations showed that one SingHealth front-end workstation was infected with malware through which the hackers gained access to the data base. The data theft happened between June 27, 2018, and July 4, 2018.

How SingHealth's database was hacked

Personal data of 1.5 million SingHealth patients was stolen in Singapore's largest data breach to date, where hackers infiltrated the healthcare group's database through a deliberate, well-planned cyber attack. Here is how it happened.

THE INITIAL BREACH

- A SingHealth front-end workstation is breached, likely through malware that was downloaded through a compromised website or a phishing e-mail.
- The malware allows hackers to obtain account credentials, such as the username and password. This gives them privileged access to the SingHealth database.

HACKERS COLLECT PATIENTS' DATA

June 27 to July 4

- Using the stolen login credentials, hackers use malicious software to access patient data, steal them, probe for more entry points and cover their tracks.
- The hackers specifically target Prime Minister Lee Hsien Loong's personal particulars and prescription information.
- At the same time, hackers steal the demographic data of 1.5 million patients. This includes name, IC number, address, gender, race and date of birth.
- Outpatient prescription details of 160,000 patients are also stolen.
- The affected patients had visited SingHealth outpatient clinics and polyclinics between May 1, 2015, and July 4 this year.

AUTHORITIES DISCOVER AND CONTAIN THE BREACH

July 4

- Administrators of the Integrated Health Information Systems (IHiS) detect unusual activity on one of SingHealth's IT databases. They investigate the incident and additional cyber-security measures are put in place to stop the unauthorised activity.
- Hackers continue to mount repeated attacks on different fronts to gain access to the database, but are detected due to increased monitoring.
- No further data is leaked.

ACTION AND PRECAUTIONS TAKEN

July 10

- Internal investigations confirm it is a cyber attack. SingHealth informs the Ministry of Health and the Cyber Security Agency of Singapore.
Given its scale and sophistication, the cyber attack was not the work of casual hackers or criminal gangs, say the authorities. It was deliberate, targeted and well planned.
- SingHealth breaks the communication link used by the malicious software.
It increases monitoring across all public information technology systems.
- Connections and systems logs are monitored and computers with malware are seized.
- SingHealth resets network servers and forces all employees to reset their passwords.

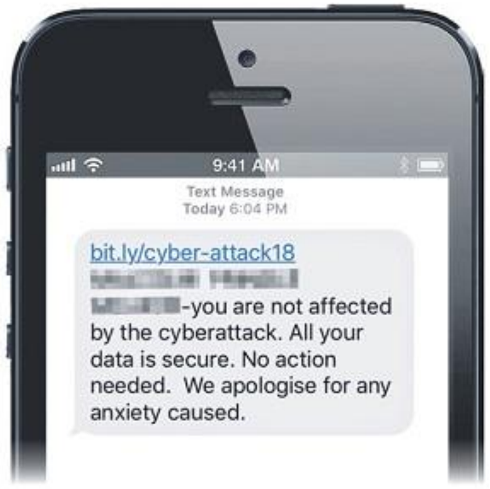
July 12

- SingHealth lodges a police report.

WHAT'S NEXT

July 20

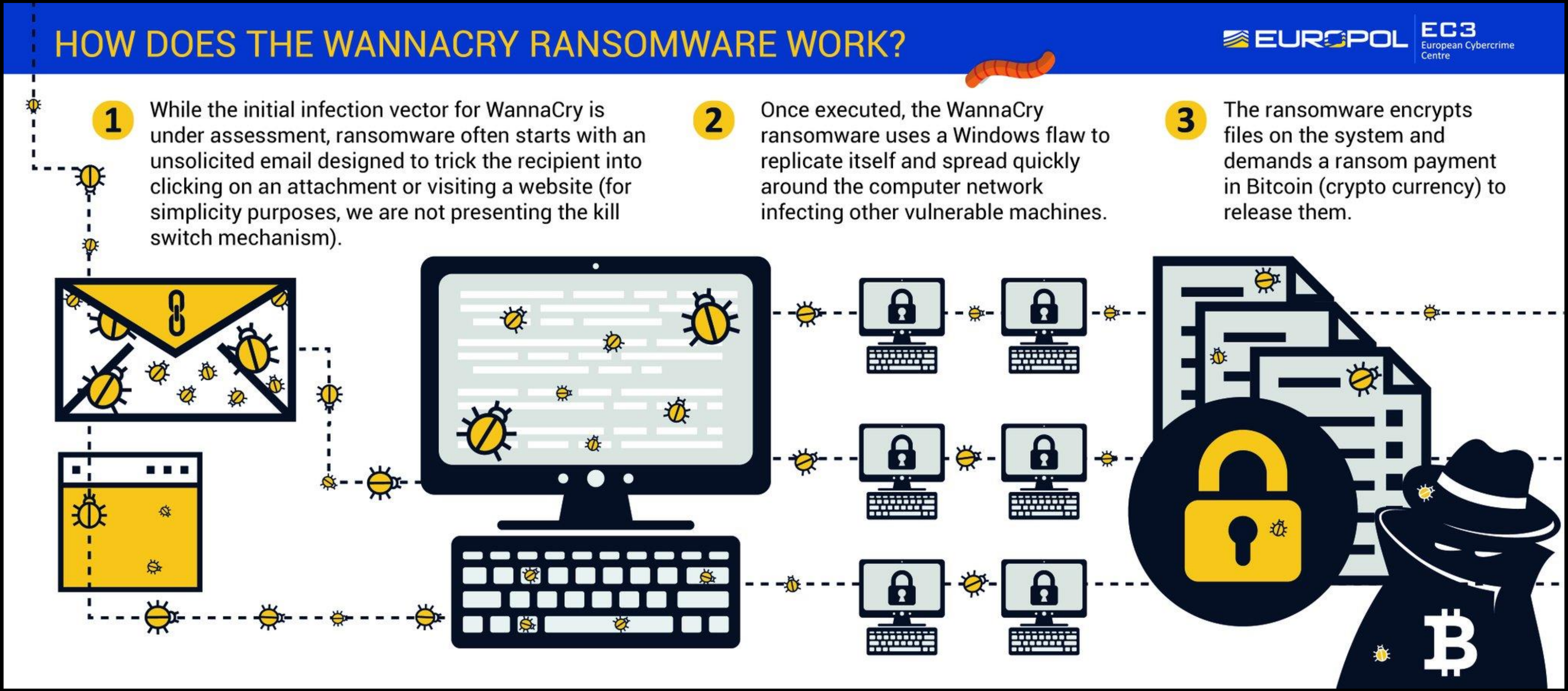
- SingHealth is progressively contacting all patients who visited its specialists and polyclinics between May 1, 2015, and July 4 this year.
- Patients will get one of three SMS notifications, depending on how much of their data has been stolen.



bit.ly/cyber-attack18
[redacted]
[redacted]-you are not affected by the cyberattack. All your data is secure. No action needed. We apologise for any anxiety caused.

- Those without mobile phone numbers registered with SingHealth will be informed via post.
- Patients can also check if their data was stolen by going to the SingHealth website at www.singhealth.com.sg or by using the Health Buddy mobile app.
- Minister-in-charge of Cybersecurity S. Iswaran has also convened a Commitee of Inquiry, led by retired senior district judge Richard Magnus.

Sources: CYBER SECURITY AGENCY OF SINGAPORE, MINISTRY OF HEALTH, MINISTRY OF INFORMATION AND COMMUNICATIONS, MALWAREBYTES STRAITS TIMES GRAPHICS

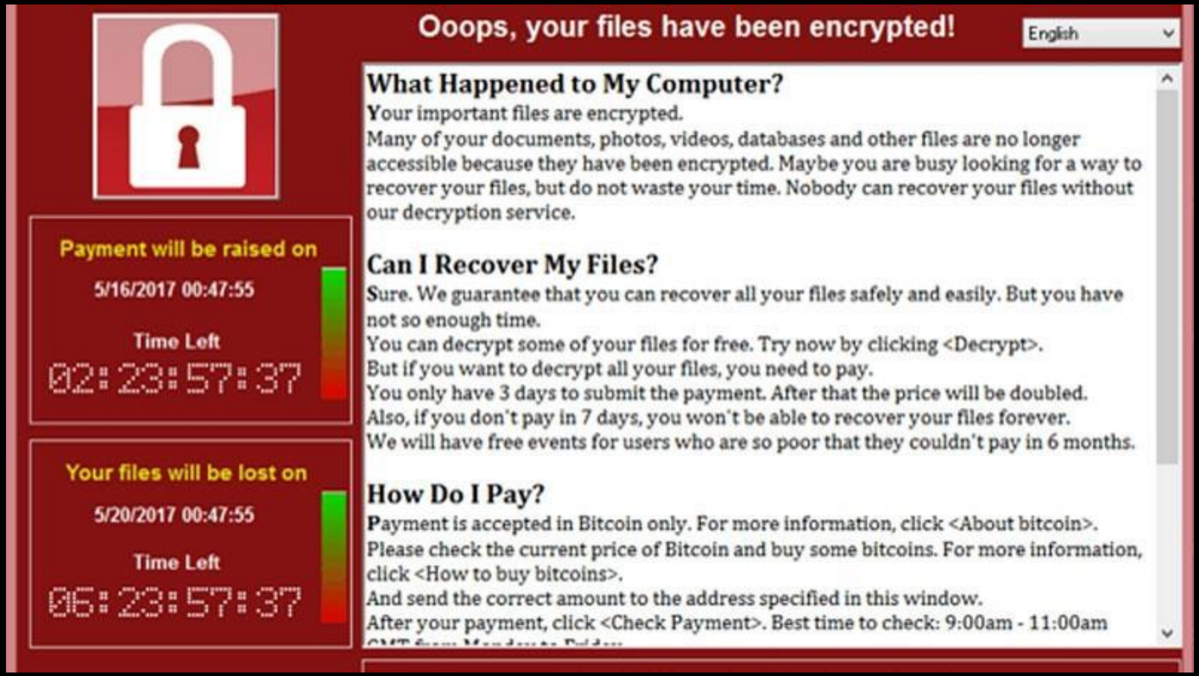


HOW DOES THE WANNACRY RANSOMWARE WORK?

1 While the initial infection vector for WannaCry is under assessment, ransomware often starts with an unsolicited email designed to trick the recipient into clicking on an attachment or visiting a website (for simplicity purposes, we are not presenting the kill switch mechanism).

2 Once executed, the WannaCry ransomware uses a Windows flaw to replicate itself and spread quickly around the computer network infecting other vulnerable machines.

3 The ransomware encrypts files on the system and demands a ransom payment in Bitcoin (crypto currency) to release them.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

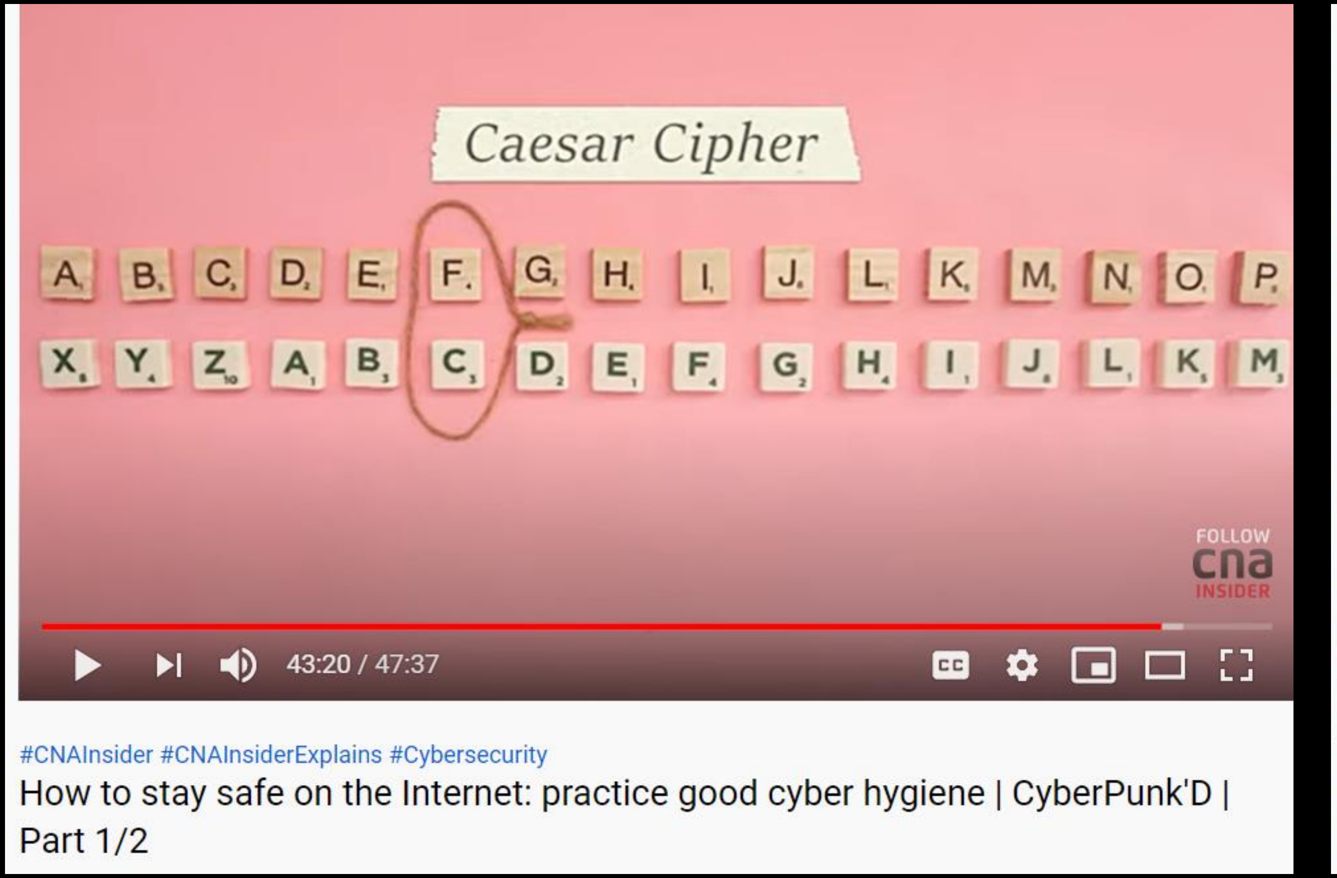
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Social Engineering

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


Caesar Cipher
A B C D E F G H I J L K M N O P
X Y Z A B C D E F G H I J L K M
FOLLOW
cna
INSIDER
43:20 / 47:37

#CNAInsider #CNAInsiderExplains #Cybersecurity

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

Okay, calm down or I will kick you.

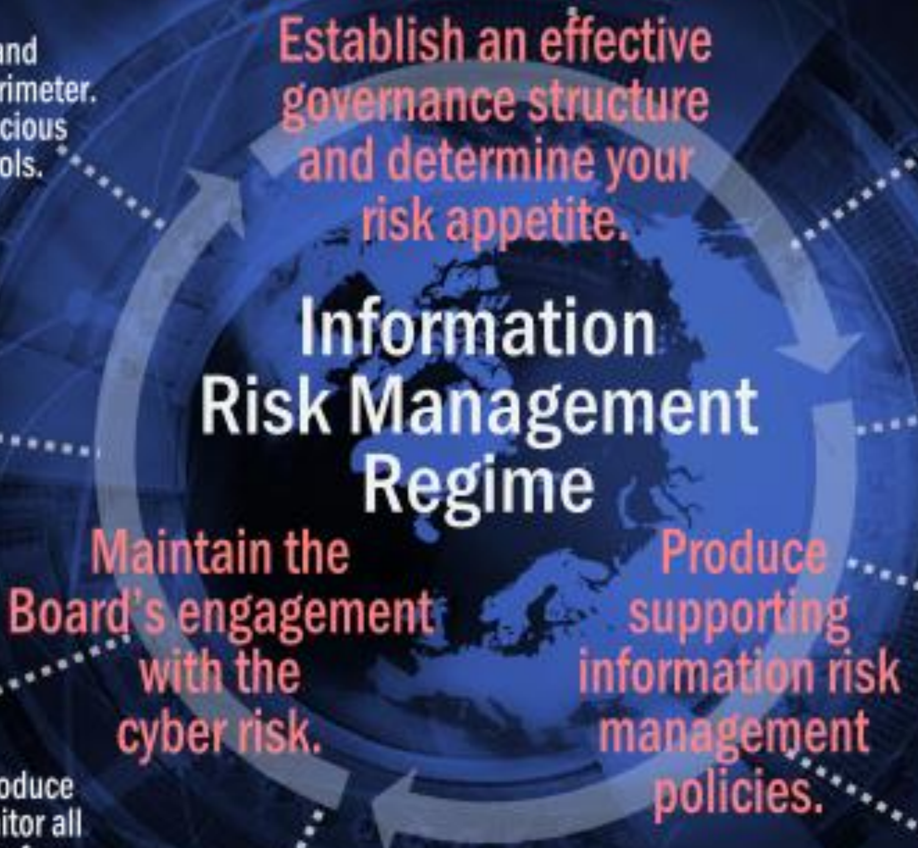
#CNAInsider #CNAInsiderExplains #Cybersecurity

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

10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.



Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Produce supporting information risk management policies.

Maintain the Board's engagement with the cyber risk.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

Cabinet Office

Top tips for cyber security

certnz

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

Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

Keep your operating system up to date

Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

Install antivirus software

Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

Choose unique passwords

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.

Set up two-factor authentication (2FA)

Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.

Use creative recovery answers

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.

Be cautious of free WiFi networks

Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.

Be smart with social media

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.

Don't give out personal info

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.

Check bank statements regularly

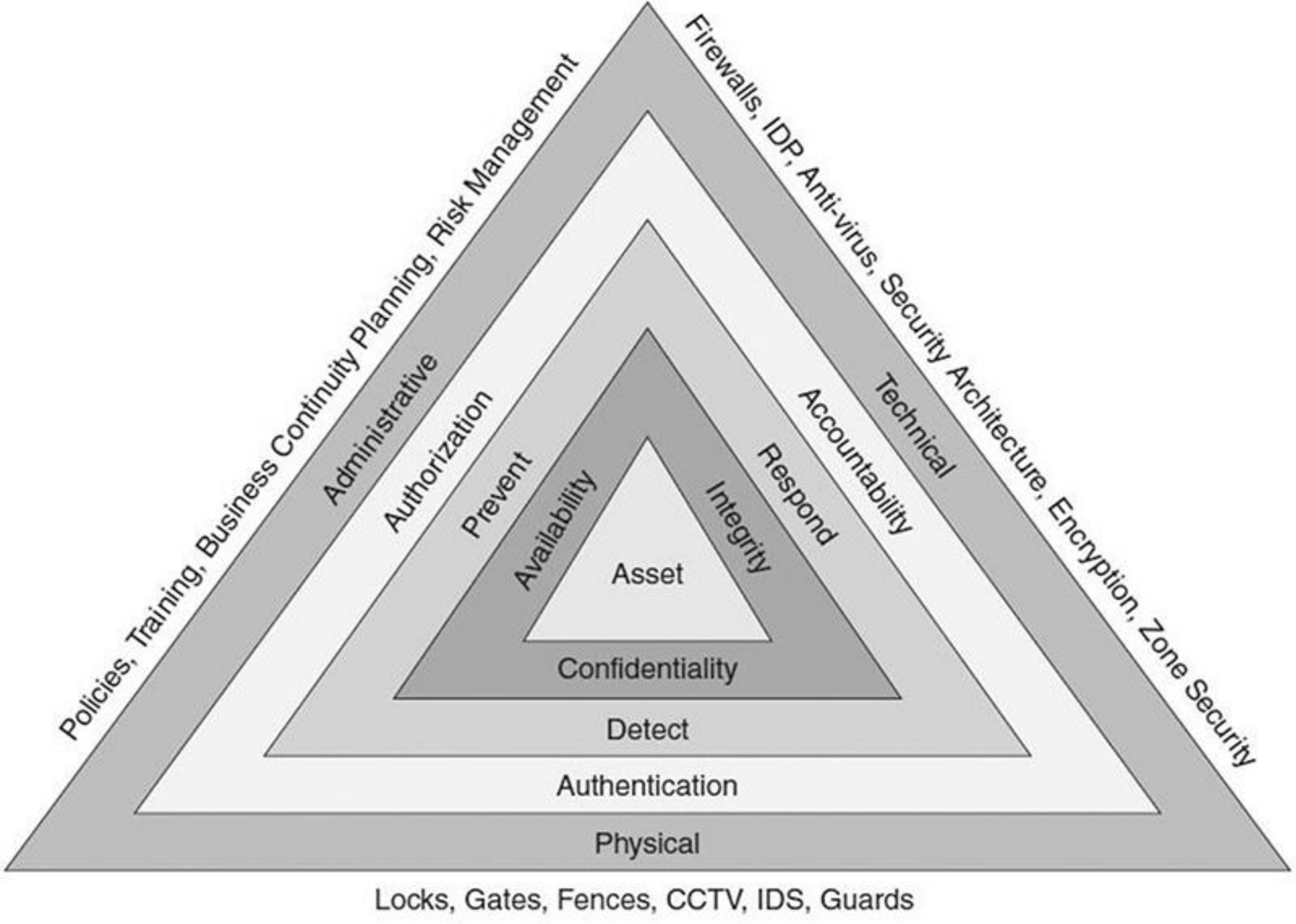
Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

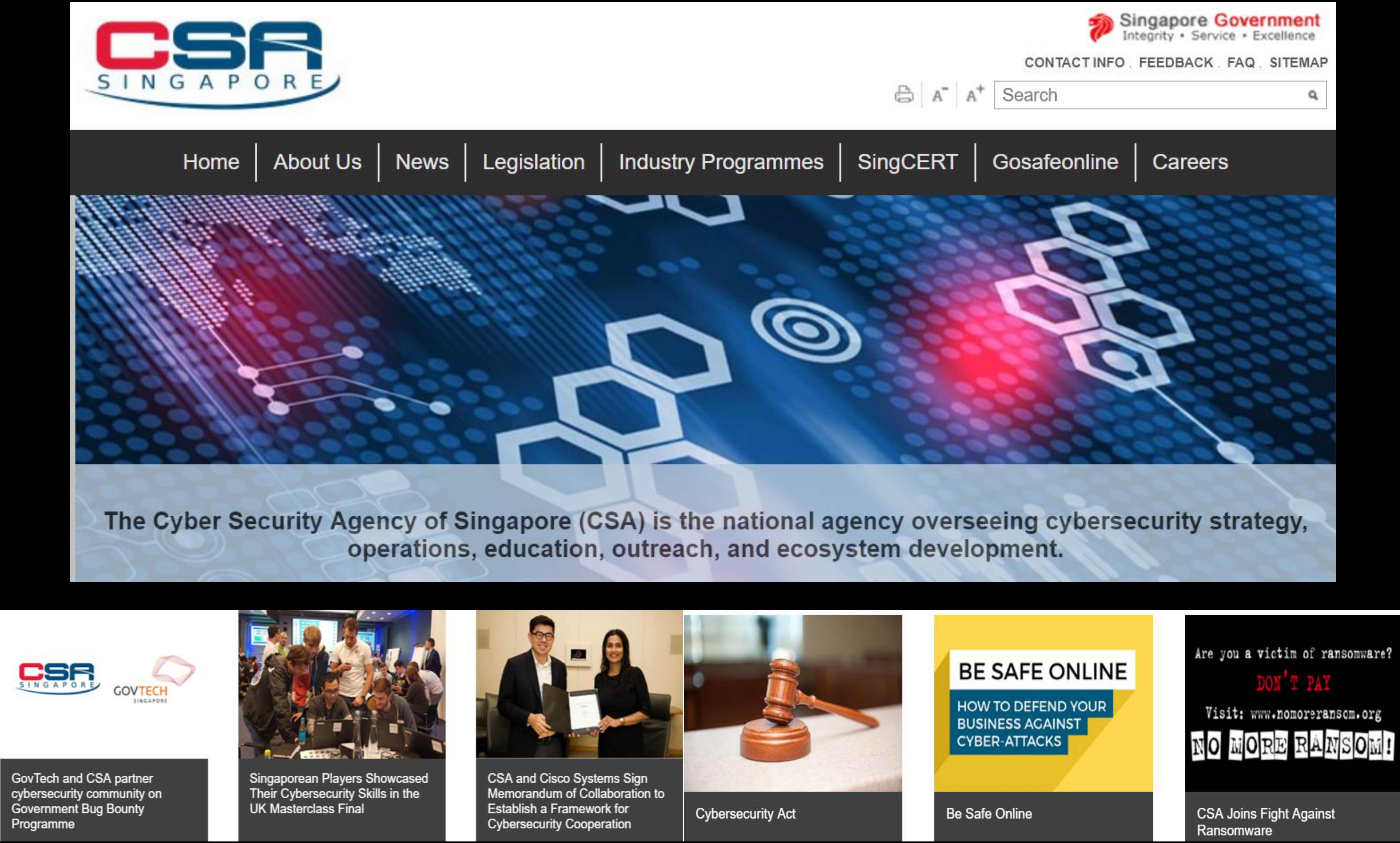
Get a regular credit check

An annual credit check will alert you if someone else is using your details to get loans or credit.

To report a cyber security problem, visit **www.cert.govt.nz**

Defence-in-depth approach


Policies, Training, Business Continuity Planning, Risk Management
Firewalls, IDP, Anti-virus, Security Architecture, Encryption, Zone Security
Administrative
Technical
Authorization
Accountability
Prevent
Respond
Availability
Integrity
Asset
Confidentiality
Detect
Authentication
Physical
Locks, Gates, Fences, CCTV, IDS, Guards



The Cyber Security Agency of Singapore (CSA) is the national agency overseeing cybersecurity strategy, operations, education, outreach, and ecosystem development.

GovTech and CSA partner cybersecurity community on Government Bug Bounty Programme

Singaporean Players Showcased Their Cybersecurity Skills in the UK Masterclass Final

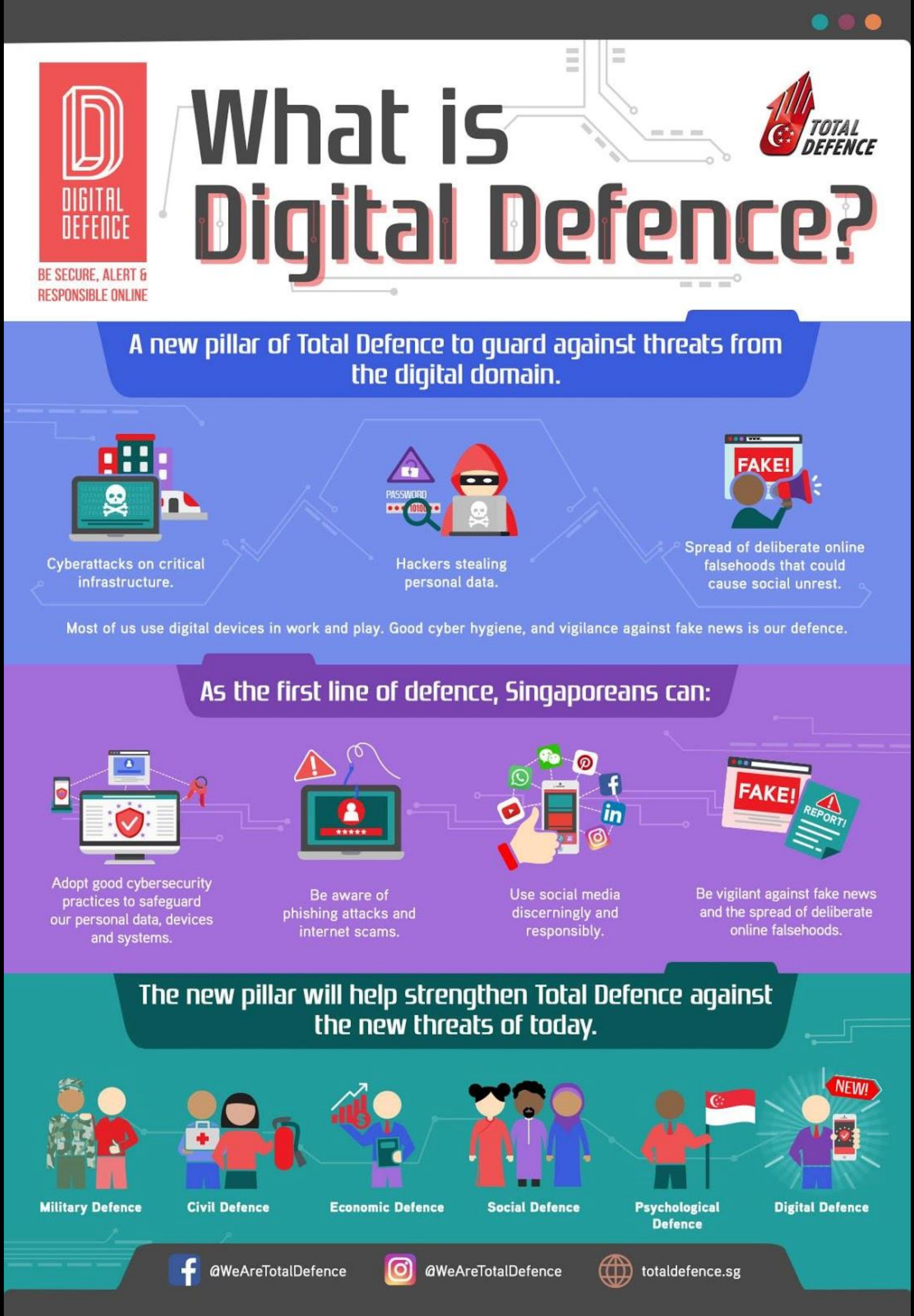
CSA and Cisco Systems Sign Memorandum of Collaboration to Establish a Framework for Cybersecurity Cooperation

Cybersecurity Act

Be Safe Online

CSA Joins Fight Against Ransomware

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

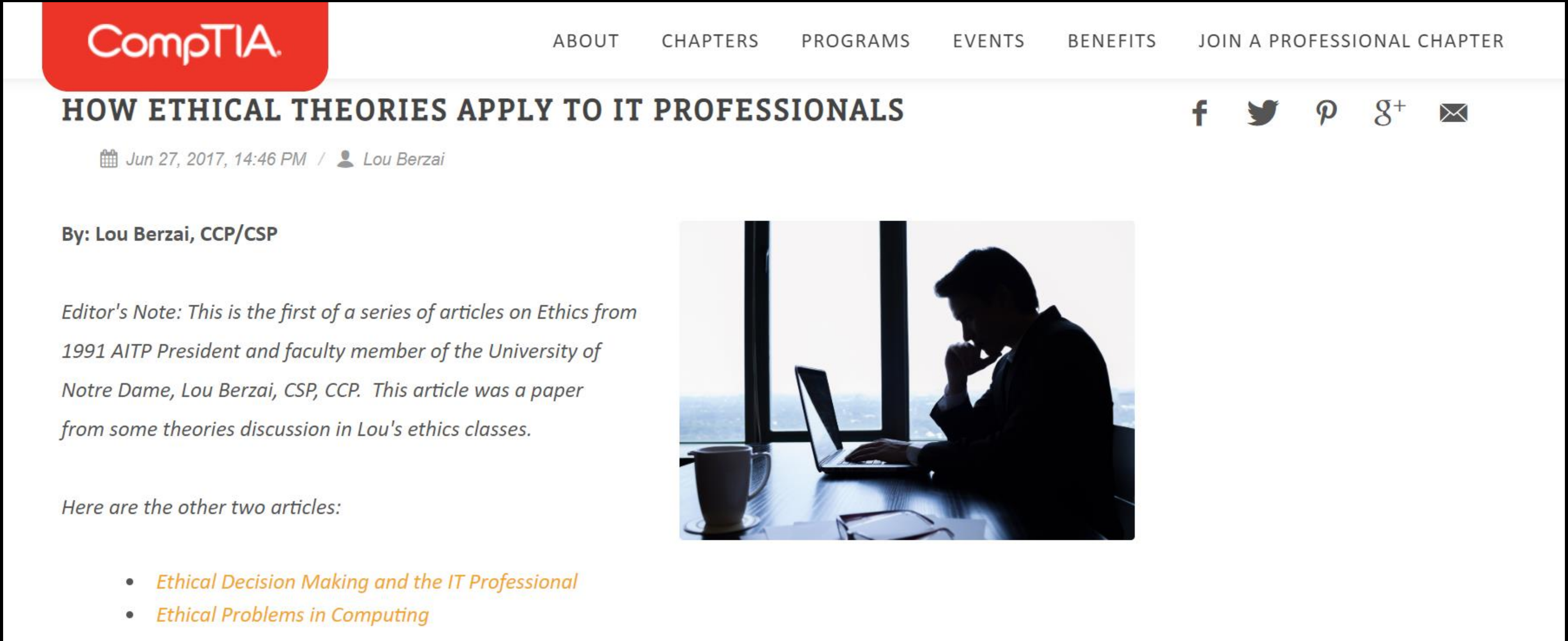
@WeAreTotalDefence

totaldefence.sg

Ten commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

https://sso.agc.gov.sg/Act/CMA1993



HOW ETHICAL THEORIES APPLY TO IT PROFESSIONALS

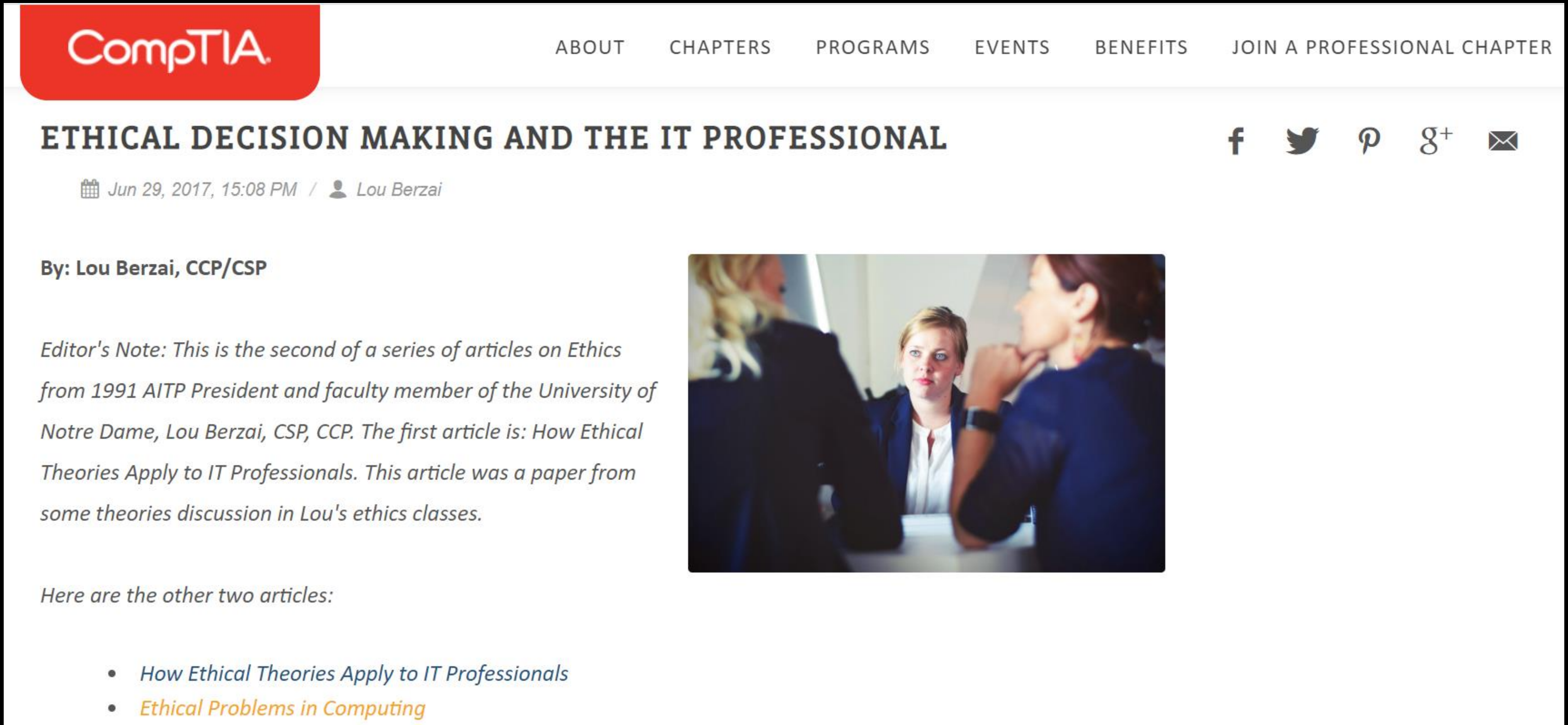
Jun 27, 2017, 14:46 PM / Lou Berzai

By: Lou Berzai, CCP/CSP

Editor's Note: This is the first of a series of articles on Ethics from 1991 AITP President and faculty member of the University of Notre Dame, Lou Berzai, CSP, CCP. This article was a paper from some theories discussion in Lou's ethics classes.

Here are the other two articles:

- *Ethical Decision Making and the IT Professional*
- *Ethical Problems in Computing*



ETHICAL DECISION MAKING AND THE IT PROFESSIONAL

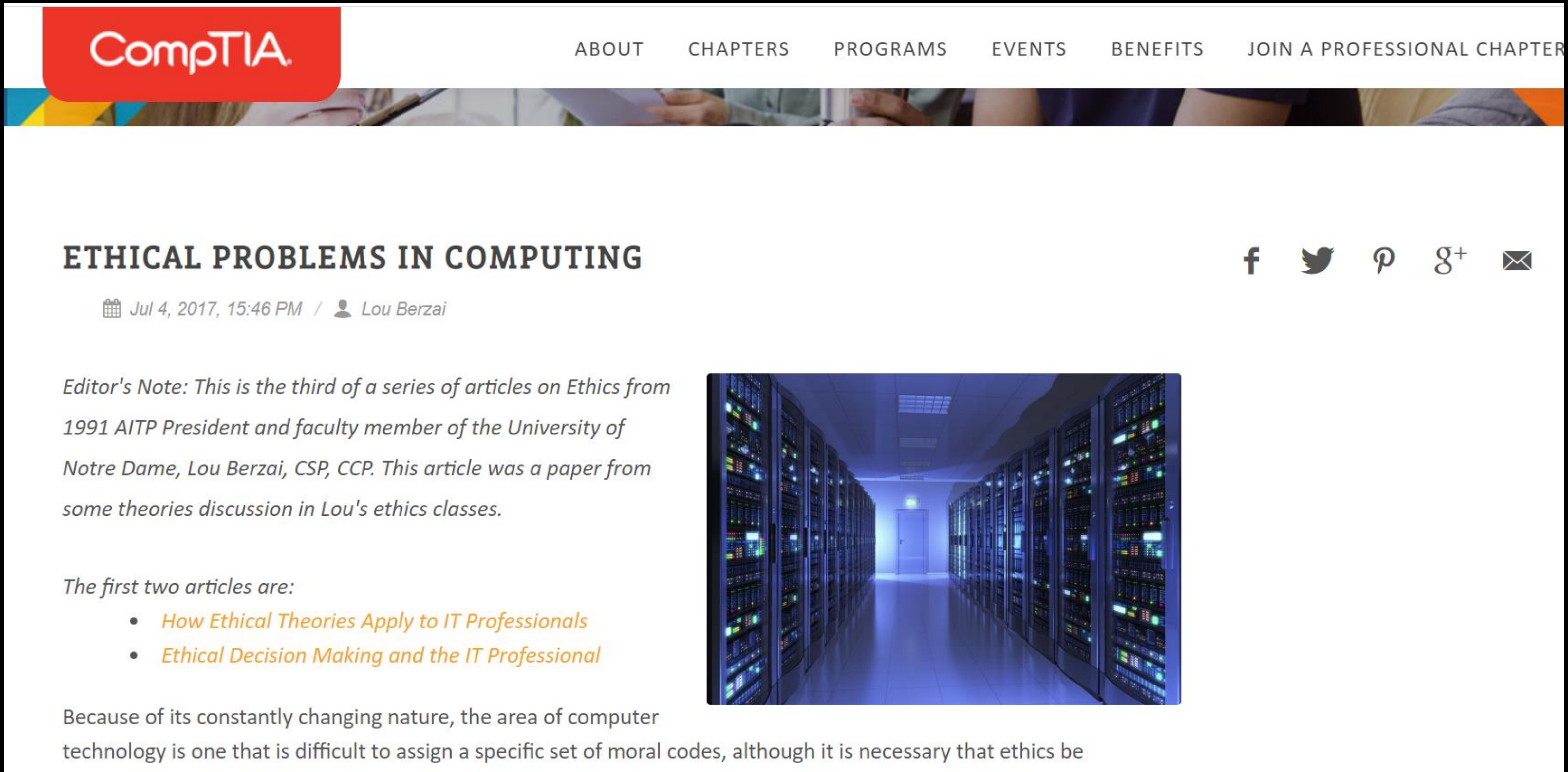
Jun 29, 2017, 15:08 PM / Lou Berzai

By: Lou Berzai, CCP/CSP

Editor's Note: This is the second of a series of articles on Ethics from 1991 AITP President and faculty member of the University of Notre Dame, Lou Berzai, CSP, CCP. The first article is: How Ethical Theories Apply to IT Professionals. This article was a paper from some theories discussion in Lou's ethics classes.

Here are the other two articles:

- *How Ethical Theories Apply to IT Professionals*
- *Ethical Problems in Computing*



ETHICAL PROBLEMS IN COMPUTING

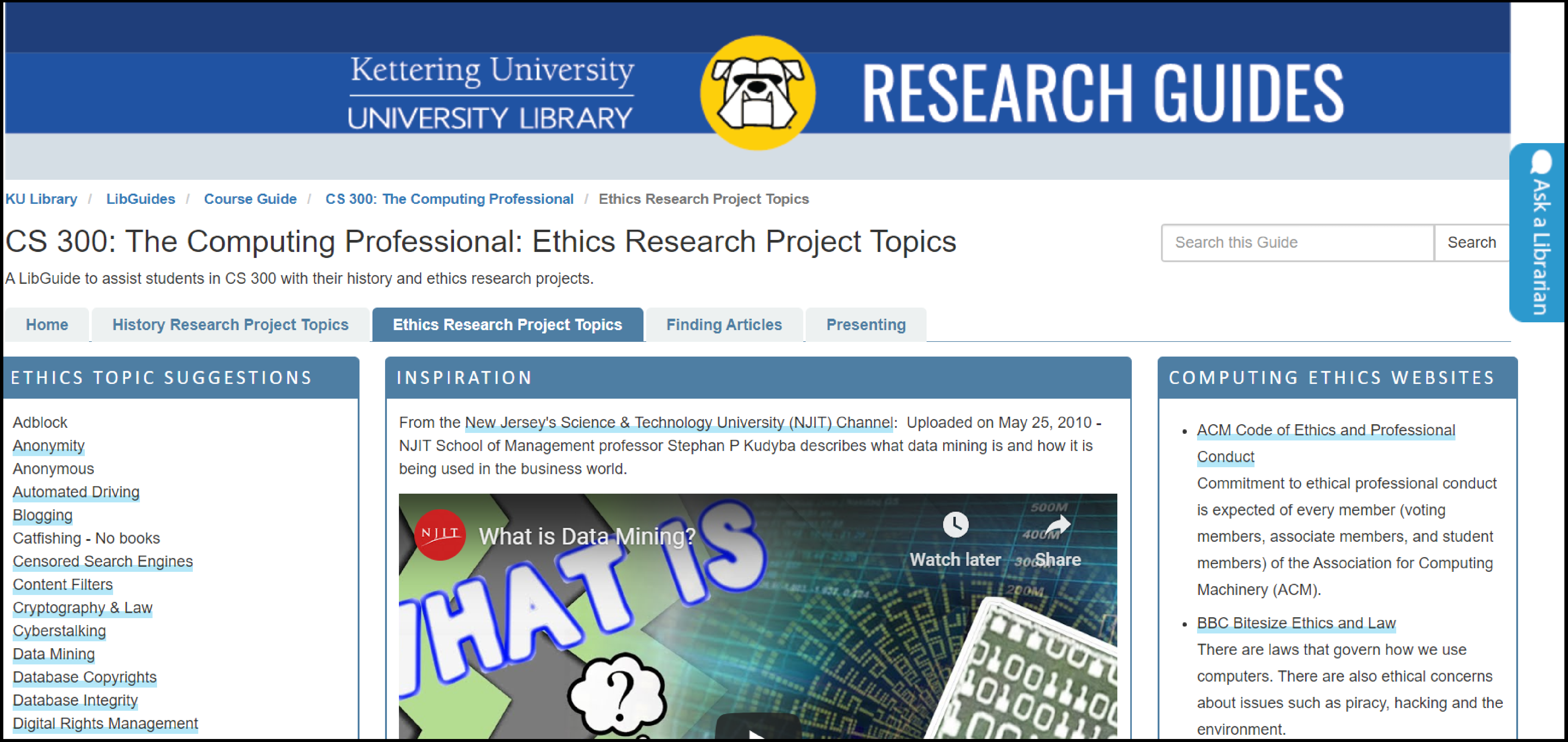
Jul 4, 2017, 15:46 PM / Lou Berzai

Editor's Note: This is the third of a series of articles on Ethics from 1991 AITP President and faculty member of the University of Notre Dame, Lou Berzai, CSP, CCP. This article was a paper from some theories discussion in Lou's ethics classes.

The first two articles are:

- *How Ethical Theories Apply to IT Professionals*
- *Ethical Decision Making and the IT Professional*

Because of its constantly changing nature, the area of computer technology is one that is difficult to assign a specific set of moral codes, although it is necessary that ethics be



Kettering University
UNIVERSITY LIBRARY

RESEARCH GUIDES

KU Library / LibGuides / Course Guide / CS 300: The Computing Professional / Ethics Research Project Topics

CS 300: The Computing Professional: Ethics Research Project Topics

Search this Guide | Search

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

Ask a Librarian

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

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.

Good reads

- Cyber threats, 2018 and beyond
- Singapore, one of the top destinations for cyberattackers
- Decoding cyber threats
- Digital defence as sixth pillar of total defence
- Basic security principles

Ethical Hacking

- The black, white and grey of hacking

The dark web

- What is the dark web?