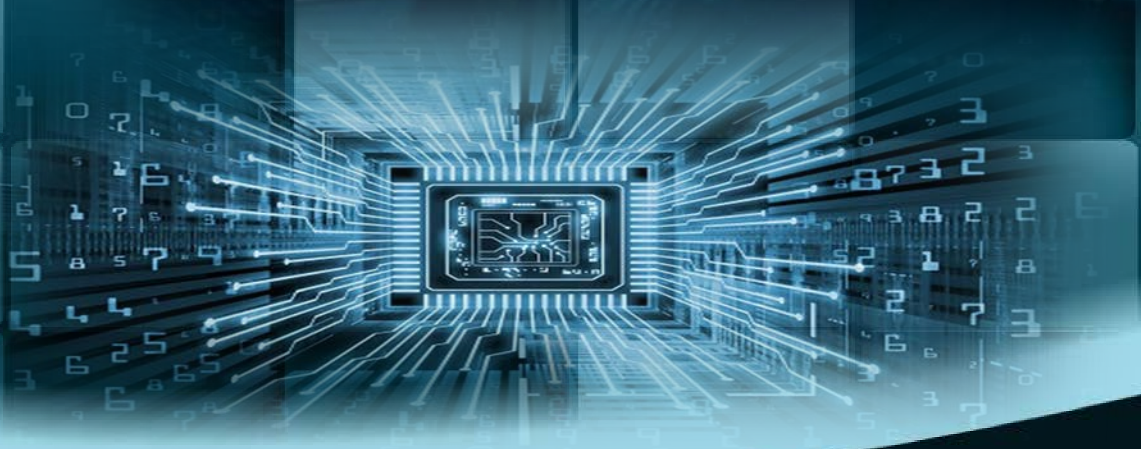
CYBER CRIME AND CYBER SECURITY



Caribbean Community (CARICOM)
Implementation Agency for Crime and Security (IMPACS)
Keate Street, Port of Spain
Tel#1-(868)-235-5511
Fax# 1(868)-627-3064

CARICOM IMPACS

Overview

Cyber Crime & Cyber Security

Being Cyber Smart.

Social Networking.

Phishing and Malware.

Emails.

Wireless Access Points.

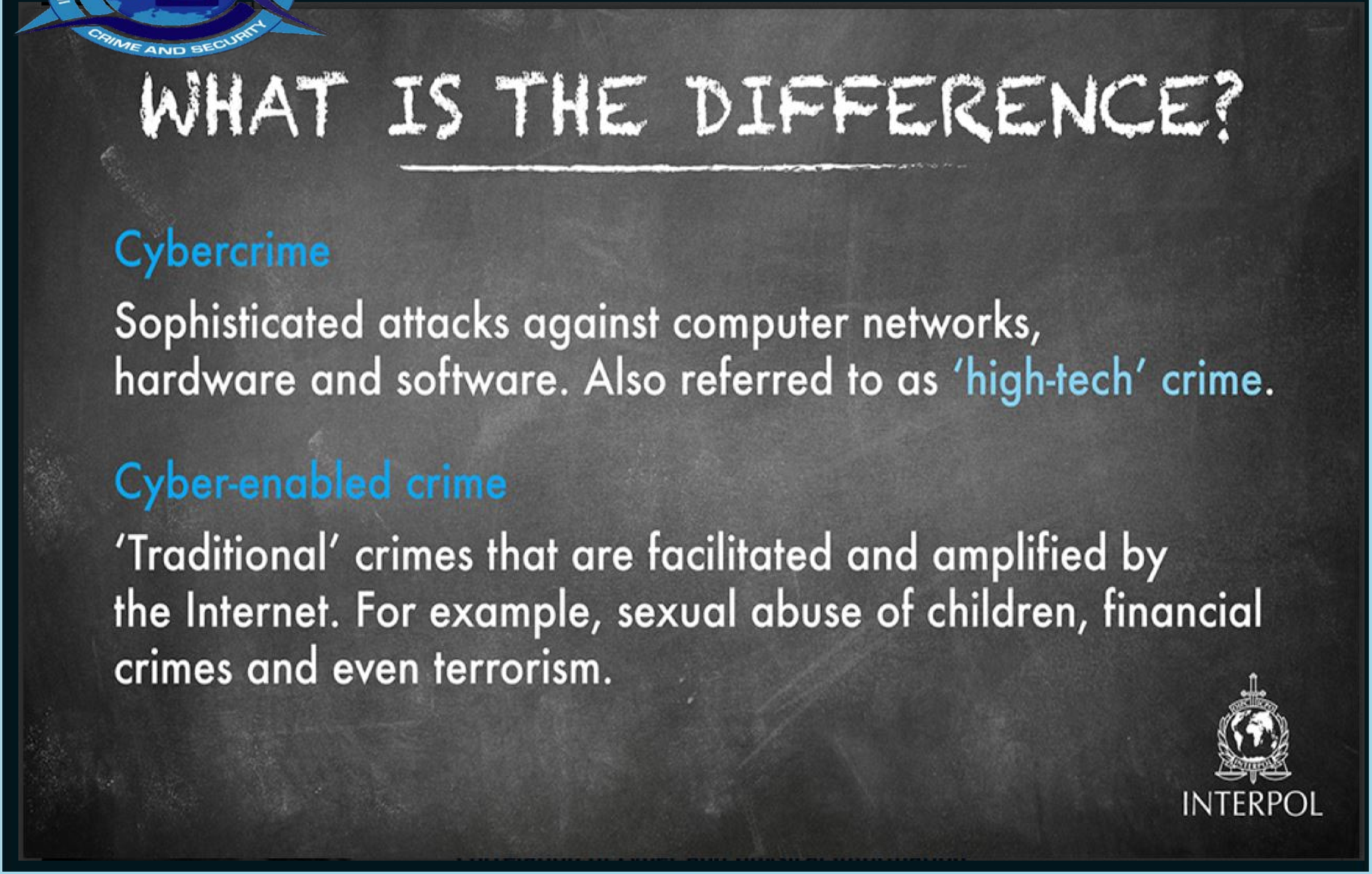
Cyber Security.

Security Considerations.

Smartphone Awareness

Anti Virus Protection.

Cybercrime



WHAT IS THE DIFFERENCE?

Cybercrime

Sophisticated attacks against computer networks, hardware and software. Also referred to as ‘high-tech’ crime.

Cyber-enabled crime

‘Traditional’ crimes that are facilitated and amplified by the Internet. For example, sexual abuse of children, financial crimes and even terrorism.

INTERPOL

Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

- Source: Cisco. (2019). *What Is Cybersecurity?* [online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

What is being cyber smart?

- ✓ Be mindful about the type of data being exchanged online.
- ✓ Being mindful about what links you click on or websites you visit
- ✓ Understanding the purpose of work computing devices
- ✓ Being mindful about what you do or post online.
- ✓ Keeping in mind that what you do or post online can affect your family, friends and your professional existence and the safety and security of others.
- ✓ Understanding the purpose of and adhering to BYOD policies and guidelines

Social Networking

- Social Networking sites and applications are an increasingly entwined part of our everyday lives.

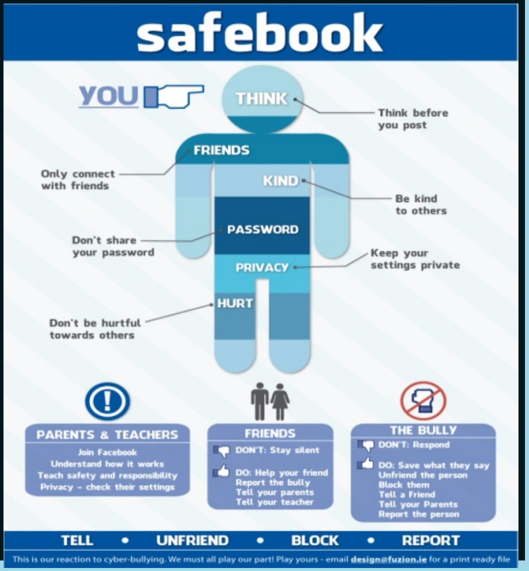
- However, much like any other part of the internet, social networks can be fraught with serious security risks.

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY

IMPACS

Social Networking

- **SKEPTICAL** of any requests for information.
- **CAUTIOUS** of any information you put on there.
- Use a **strong password (Alphanumeric and symbols)**
- Use **privacy settings**. Insist your friends use theirs too.
- Whenever possible, **organize contacts into "categories"**
- **Verify** friend/follower requests.
- **Never** enable Geo-location Feature.



This is our reaction to cyber-bullying. We must all play our part! Play yours - email **design@fuzion.ie** for a print ready file

Web Searches

- Use **RELIABLE** Online resources.
- **VERIFY** data discovered online.
- Be **MINDFUL** of cookies and website trackers
- Use **ONLY** dedicated devices for online research.
- Devices used to access critical systems **MUST NOT** be used to surf the internet, particularly social media websites.
- Downloading of music and executable files **MUST NOT** be done on devices used to access critical systems.

Phishing and Malware

Phishing – it’s when a scammer disguises a trustworthy source (URL/link) to obtain private information such as password and credit card information

Malware – Malicious software disguised as legitimate software design to collect and transmit private information such as passwords, without the user consent or knowledge.

Phishing and Malware Counter Measures

- Use **HTTPS** to connect to your social networking sites whenever possible, especially when connecting from a public hotspot.
- Be wary if your net banking and Social networks use HTTP for login credentials only.
- Ensure that you use a **Multiple Anti Virus service** and ensure that antivirus solutions are **up to date**.

Emails

Email is a wonderful tool for sending and receiving a lot of information quickly and securely. However, it’s important that your personal information remains secure and safe and that you aren’t open to viruses or hackers.

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY

IMPACS

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY
IMPACS

Email Safety Tips

- Change your password regularly and keep it in a safe place. Don’t share your password with anyone.
- Don’t open attachments from anyone you don’t know.
- Log out or sign off from your account when you’ve finished looking at/sending your email.
- Don’t reply to spam or forward chain emails.
- Keep your personal information personal – don’t share bank or credit card information by email.
- Your bank will not discuss your private financial situation by email.

crestock.com © Hoang Hai Ninh

Wireless Access Points.

- Every rose has its thorns, and every useful technology has its vulnerabilities. Cutting the wires to let users work anywhere and connect remotely to information resources from increasingly powerful mobile devices can provide an attractive work environment and increase productivity. But it does not come free.

  “***With every major advance in networking technology comes new ways to exploit it.”***

Amit Sinha

chief technologist

Motorola Enterprise Mobility Solutions.

Wireless Internet Risks.

- Wireless hotspots located at airports, libraries, hotels, cafes and restaurants are havens for hackers.
- Man in the Middle attacks (MITM).
- Wireless packet Sniffers.
- Wireless Router Exploitation for nefarious enterprise.
- BYOD (Bring your own device) wireless security threats and implications.

Wireless Safety Tips

- Don't assume that public "hot spots" are secure. You should assume that other people can access any information you see or send over a public wireless network.
- Use anti-virus and anti-spyware software, and a firewall.
- Turn off the wireless functionality on your devices when you know you won't use it.

IMPACS

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY

Cyber Security

Cyber security is the state or process of protecting and recovering networks, devices, and programs from any type of cyberattack.

Cyberattacks are an evolving danger to organizations, employees, and consumers. They may be designed to access or destroy sensitive data or extort money. They can, in effect, destroy businesses and damage people’s financial and personal lives.

Source: Norton.com/internetsecurity

Types of Threats

Social Engineering – the term used for a wide range of malicious activities accomplished through human interactions. Psychological manipulation is used to trick users into making security mistakes or giving away sensitive data**.**

Types of Threats

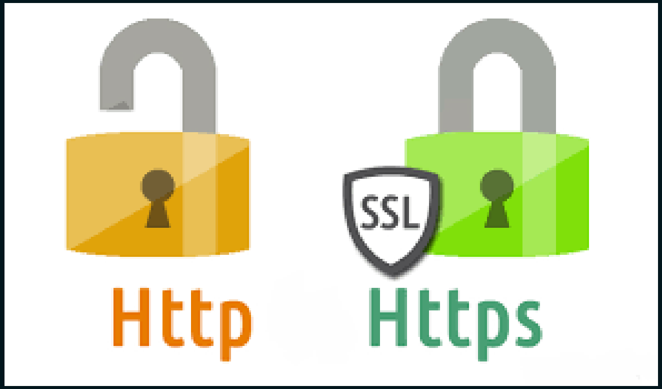
- APTs- Advance Persistent Threats

Attacks in which an unauthorized user infiltrates a network undetected and stays in the network for a long period of time.

Source :Digitalguardiancom. 2015. Digital Guardian. [Online]. [12 September 2019]. Available from: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition

Cyber Security Prevention Tips

How to help protect against Cyber Security attacks



Regularly back up your files

Only trust https:// URLs

Source: Norton.com/internetsecurity

Cyber Safety Tips

- Don’t open attachments or links from unknown senders

- Keep your devices updated with the newest software

Source: Norton.com/internetsecurity

Smartphones

Mobile phones or Smartphones have advance capabilities like those of personal computers (PC’s). Their lax security and popularity have cause them to be more attractive targets for attackers

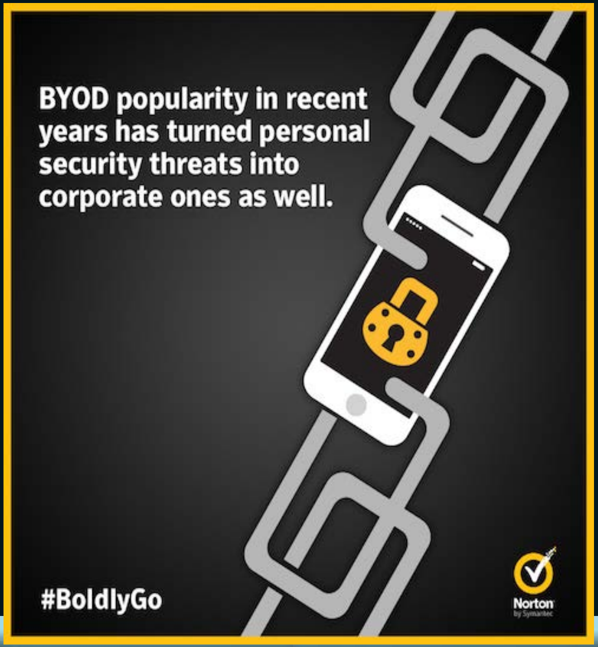
IMPLEMENTATION AGENCY FOR CRIME AND SECURITY
IMPACS

Smartphones Awareness

- Mobile phishing and ransomware through mobile apps
- Cross-platform banking attacks
- Using an infected mobile device to infiltrate nearby devices.
- We are our own enemy

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY

IMPACS

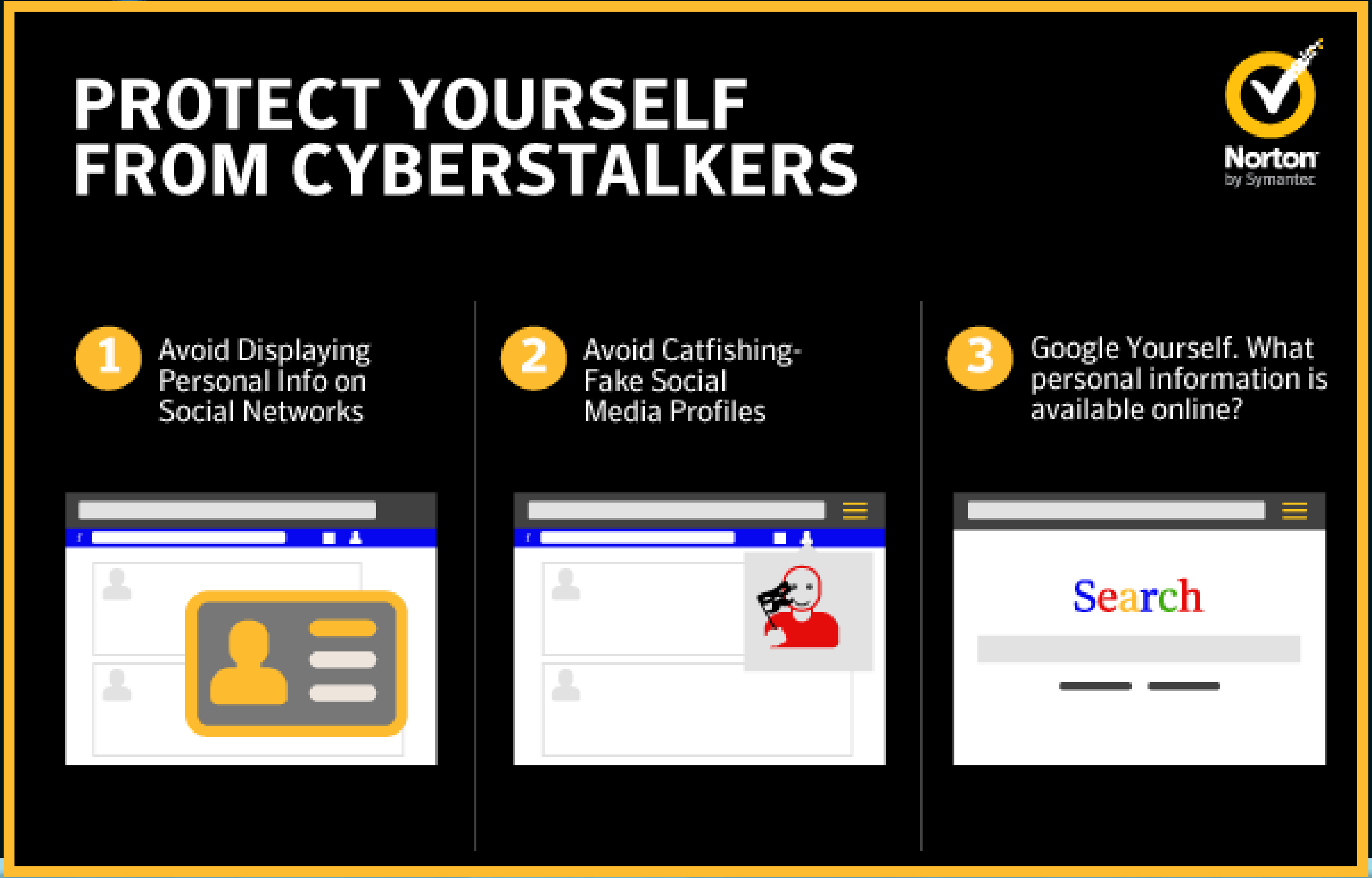


BYOD popularity in recent years has turned personal security threats into corporate ones as well.

Anti Virus Protection

- The general expectation you should have from an antivirus program is that it will do one thing and one thing only, protect your device from harmful software, and that it will do it well.
- Antivirus software keeps a database of what are referred to as "signatures" for known viruses. A signature is a portion of code that identifies a virus. This database is updated regularly over an Internet connection to ensure that you have the most up-to-date signature database.

Protect Yourself



PROTECT YOURSELF FROM CYBERSTALKERS

Norton by Symantec

1 Avoid Displaying Personal Info on Social Networks

2 Avoid Catfishing- Fake Social Media Profiles

3 Google Yourself. What personal information is available online?

Remember

Protection of your sensitive digital data requires constant awareness and adherence to simple methodologies.

What do you think is the weakest element of any Cyber Security Strategy?

Be Cyber Smart!!!

IMPLEMENTATION AGENCY FOR CRIME AND SECURITY

IMPACS

Questions?