# Secure Your Information, Protect Yourself!

**Assoc. Prof. Ts. Dr. Nur Izura Binti Udzir**
Faculty of Computer Science and Information Technology|
Director, Co-curriculum and Student Development Centre, UPM

# Assoc. Prof. Ts. Dr. Nur Izura Udzir

- Lecturer at Faculty of Computer Science and Information Technology, UPM (since 1998)
- Professional expertise: Information/Computer Security
- Director, Co-curriculum and Student Development Centre, UI

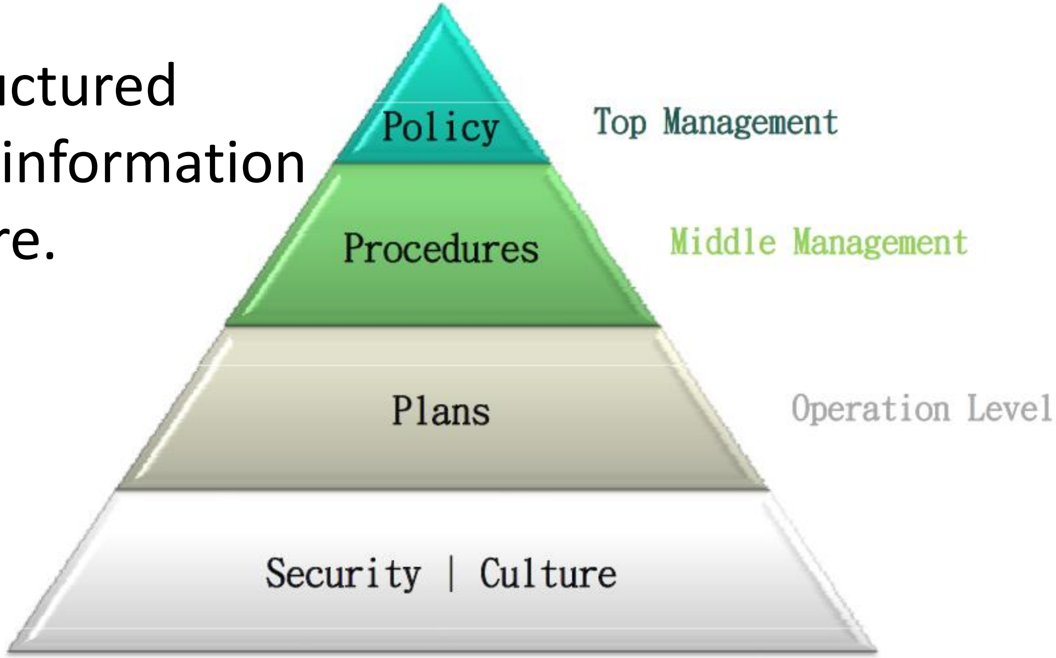
- Education:
  - Bac. Computer Sc. – UPM (1991-1995)
  - M.Sc (Computer Sc.) – UPM (1996-1998)
  - Ph.D (Computer Sc.) – York, UK (2003-2006)
- International Committee Member/Expert **International Organizatior Standardization (ISO)** for ISO/IEC JTC 1/WG11 Smart Cities.
- High Advisory Board, **International Family Institute** (di Turki)
- Committee Member/Expert, DSM/NMC/ISC-G/WG5-2 **Security Technologies** (Jabatan Standard Malaysia).
- Protem Committee, **Information Security Professional Association of Malaysia (ISPA.my)**, 2010.

# Cybersecurity

- Cybersecurity
  - not limited to computer science or ICT related areas only.
- It is now the concern of
  - every individual,
  - every organization,
  - every nation,
  - across all disciplines.
- The rapid growth of digital technology and the Internet, the interconnected devices, online applications
  - have somehow exposed users to threats.

# Information Security Management System (ISMS)

- … is a set of policies concerned with information security management or IT related risks.
- … a systematic and structured approach to managing information so that it remains secure.



# Attacks

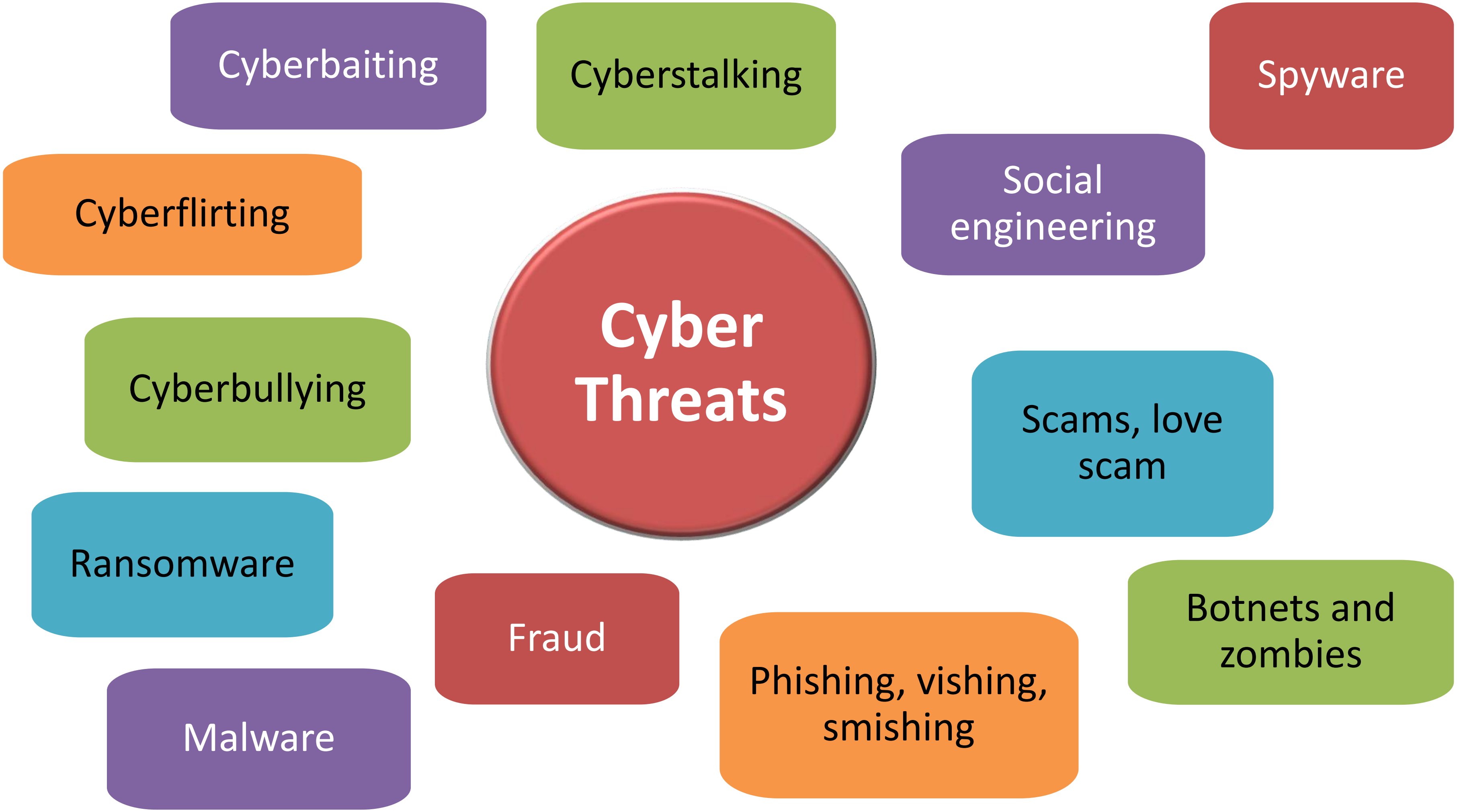
Attacker is motivated by profit.

## Passive attacks

- Learn or make use of information from the system but does not affect system resources
- Eavesdropping, monitoring, or transmissions

## Active attacks

- Involve some modification of the data stream
- or the creation of a false stream



Cyber Threats

Cyberbaiting

Cyberstalking

Spyware

Cyberflirting

Social engineering

Cyberbullying

Scams, love scam

Ransomware

Fraud

Botnets and zombies

Phishing, vishing, smishing

Malware

# Most Security Problems Are

# People-Related

Most damage NOT due to attacks, but …

“Oops!”

“What was that?”

# What do we want to protect?

# Assets

*Asset - Anything that has value to the organisation, its business operations and its continuity (ISO 27001)*

Three main types:

(1) pure information (in whatever format),

(2) physical assets such as buildings and computer systems

(3) software used to process or otherwise manage information

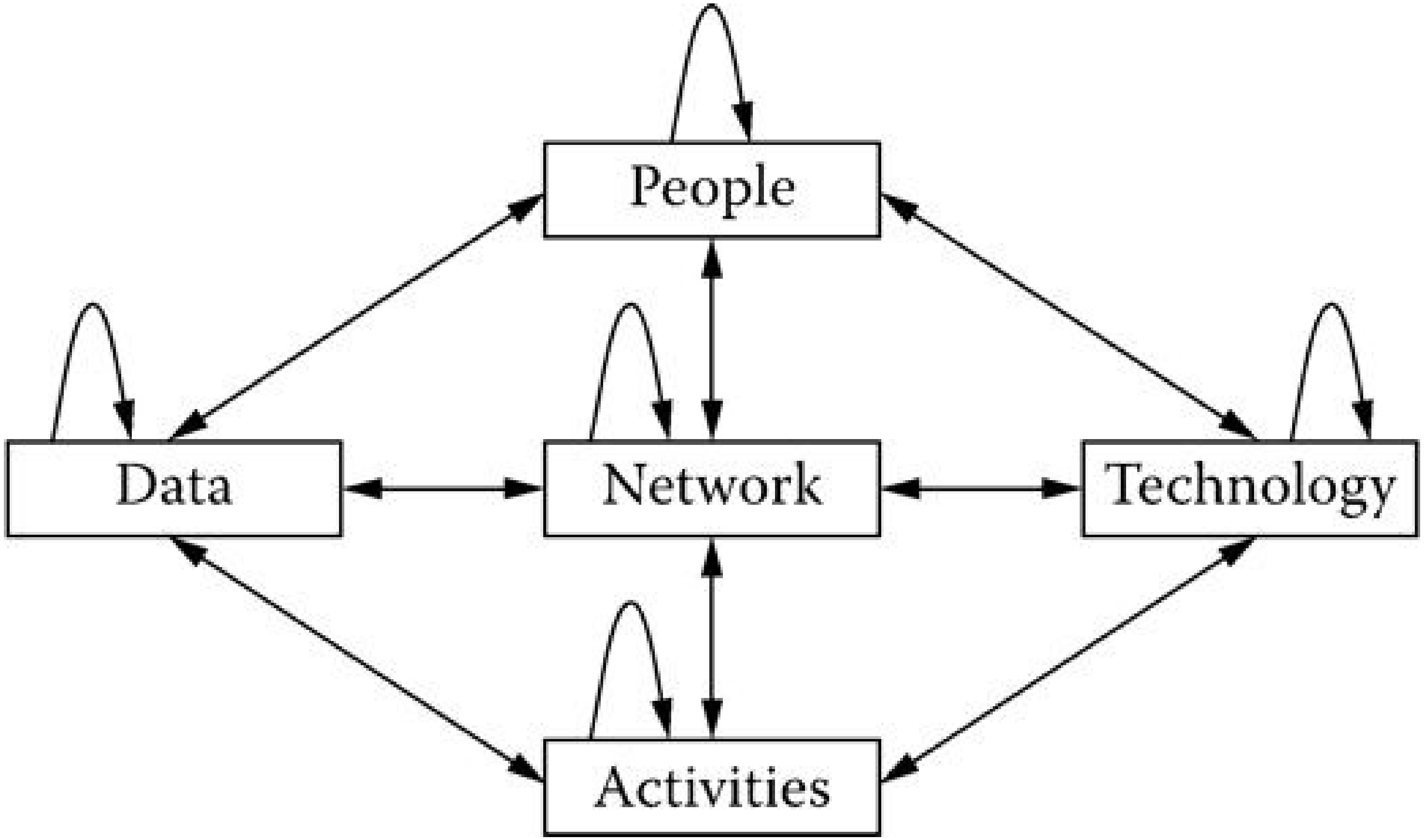
Taylor, 2013

# Assets

- Hardware:
  - laptops, servers, routers, PDAs, mobile phones, smart cards, …
- Software:
  - applications, operating systems, database systems, source code, object code, …
- Data & information:
  - essential data for running and planning your business, design plans, digital content, data about customers, …
- Services & revenue
- Reputation of organization, trust, brand name
- Employees' time

Gollmann, 2011

# Computing environment with interacting components



[Raggad, 2010]

# The CIA:
# Information Security Principles

## Confidentiality

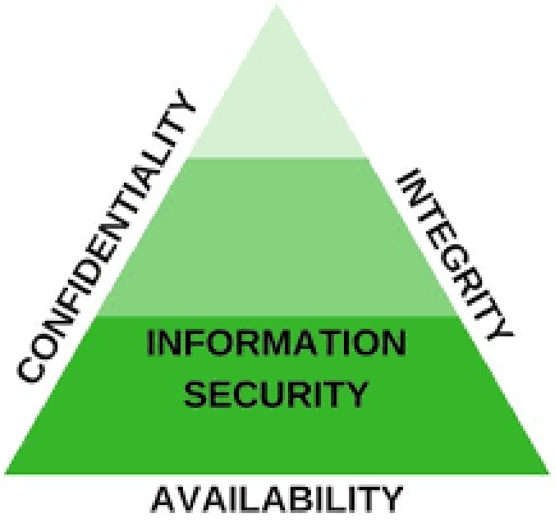
- Information only available to authorized users
- Preventing unauthorized subjects from accessing information

## Integrity

- Information retains intended content and semantics
- Preventing unauthorized subjects from modifying information

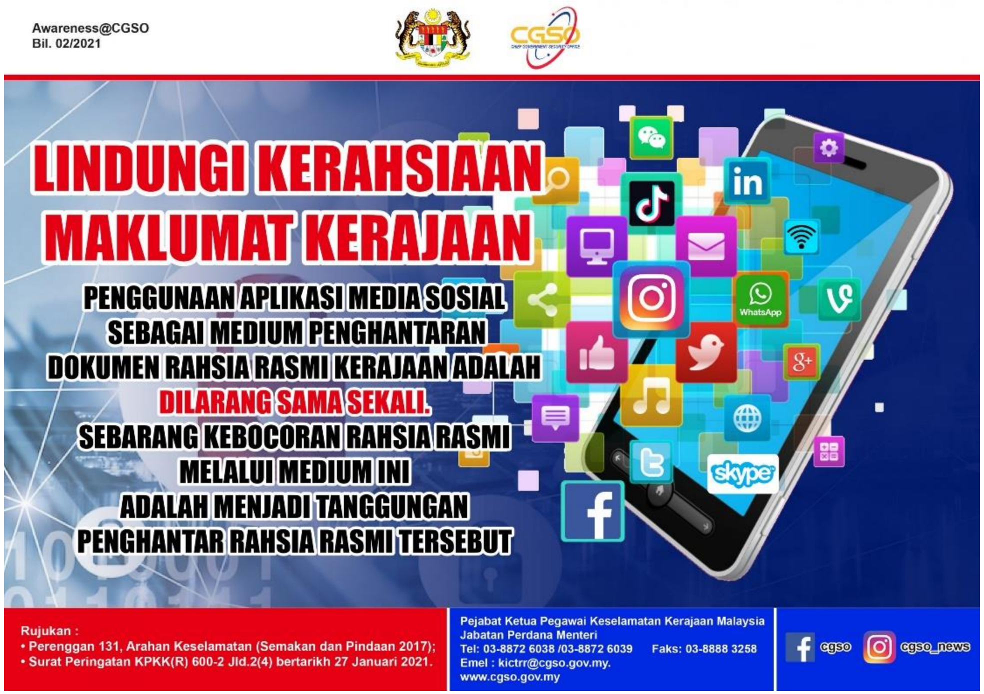
## Availability

- Information retains access and presence
- Preventing information and resources from being inaccessible when needed



# Data Security

- Personal data
  - Employees/staff
  - Students
  - Stakeholders
- Organisation’s info
  - example?
- Customer info
- Whay is our reference?



Awareness@CGSO
Bil. 02/2021

LINDUNGI KERAHSIAAN MAKLUMAT KERAJAAN

PENGGUNAAN APLIKASI MEDIA SOSIAL SEBAGAI MEDIUM PENGHANTARAN DOKUMEN RAHSIA RASMI KERAJAAN ADALAH DILARANG SAMA SEKALI.

SEBARANG KEBOCORAN RAHSIA RASMI MELALUI MEDIUM INI ADALAH MENJADI TANGGUNGAN PENGHANTAR RAHSIA RASMI TERSEBUT

Rujukan :
- Perenggan 131, Arahan Keselamatan (Semakan dan Pindaan 2017);
- Surat Peringatan KPKK(R) 600-2 Jld.2(4) bertarikh 27 Januari 2021.

Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Jabatan Perdana Menteri
Tel: 03-8872 6038 /03-8872 6039 Faks: 03-8888 3258
Emel : kictrr@cgso.gov.my.
www.cgso.gov.my

cgso cgso_news

# Malaysian Cyberlaws

1. Digital Signature Act 1997

2. Optical Discs Act 2000 (ODA)

3. Telemedicine Act 1997

4. Electronic Commerce Act 2006

5. Computer Crimes Act 1997

6. Personal Data Protection Act 2010

7. Copyright (Amendment) Act 1997

8. Communication and Multimedia Act 1998

9. Electronic Government Activities Act 2007

# Information Classification

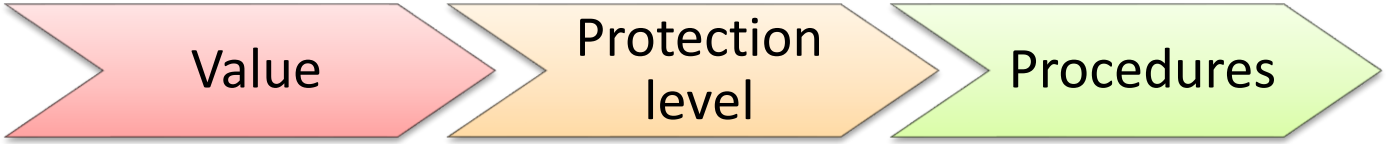
Not all information has the same value

Need to evaluate value based on CIA

Value determines protection level

Protection levels determine procedures

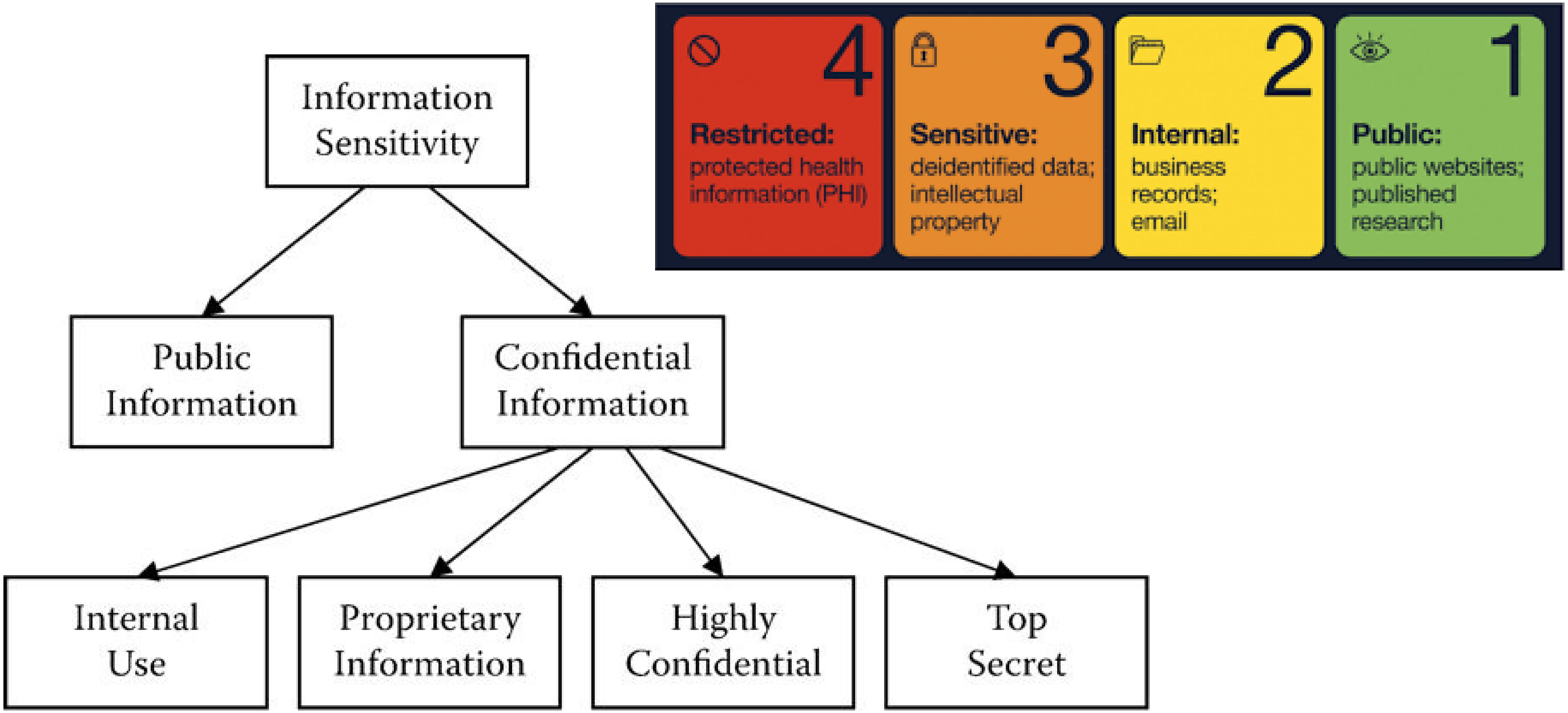
Labeling informs users on handling



Value → Protection level → Procedures

Watson, Purdue

# Information Classification



Information Sensitivity

Public Information

Confidential Information

Internal Use

Proprietary Information

Highly Confidential

Top Secret

4 **Restricted:** protected health information (PHI)

3 **Sensitive:** deidentified data; intellectual property

2 **Internal:** business records; email

1 **Public:** public websites; published research

Raggad, 2010

# Common Security Mistakes

Poor password

- Using the same password without the two-factor authentication
- Using weak passwords
- Too lazy to remember their passwords – post-it-notes
- Reusing passwords

Using unknown flash drives

No security solutions – e.g. No anti-virus

Downloading unsolicited antivirus software

Downloading apps from third-parties

Ignoring on software updates/security patches.

Disabling User Account Control Features

Ignoring SSL certificate warnings

# Common Security Mistakes

Too trustworthy

- Opening e-mail attachments
- Clicking questionable links
- Answering phishing emails

Using public WiFi

Browsing on unsecured connections

Leaving devices unattended

Leaving your webcam open to attack

Oversharing on social media

‘It won’t happen to me’

# Common Security Mistakes

## Poor password

Using the same password without the two-factor authentication

Using weak passwords

Too lazy to remember their passwords – post-it-notes

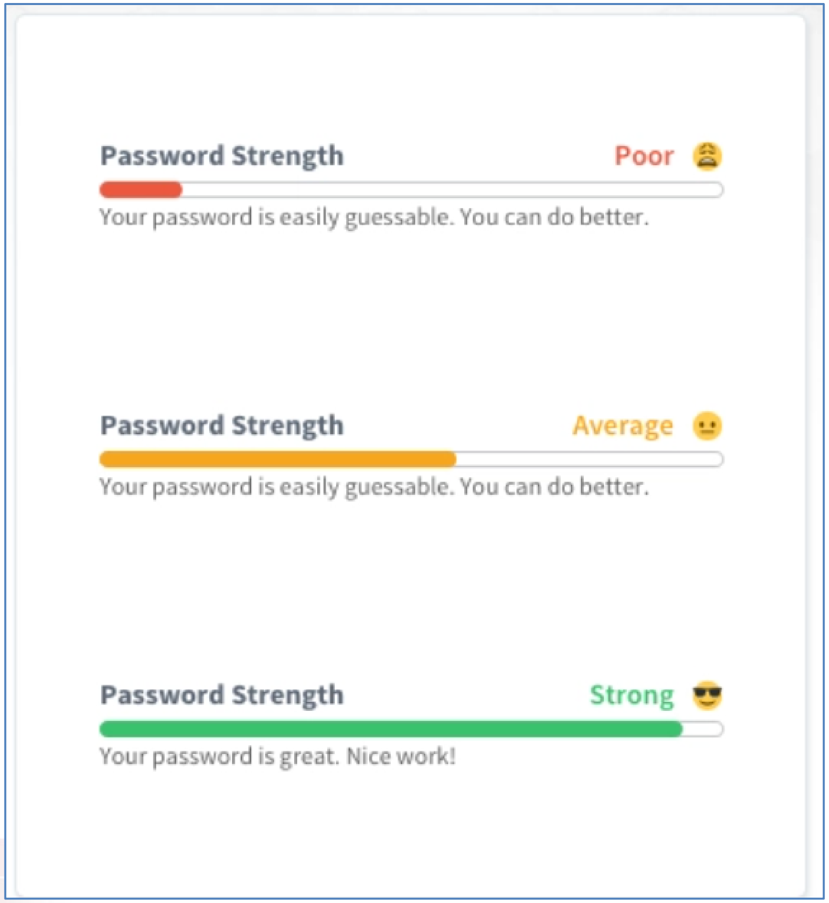
Reusing passwords

# Some security tips…

## Passwords

Always strengthen your password.

- Mix letters, numbers, symbols
- Change periodically (from time to time)


Password Strength Poor 😩

Your password is easily guessable. You can do better.

Password Strength Average 😐

Your password is easily guessable. You can do better.

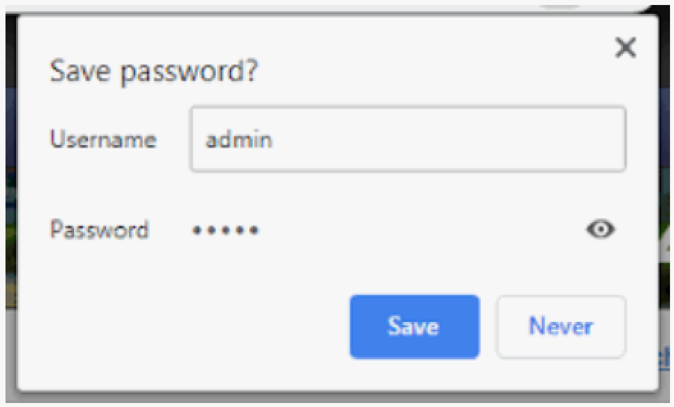
Password Strength Strong 😎

Your password is great. Nice work!

# Some security tips…

## Passwords

- Never allow system/apps to “save password” or “remember password”

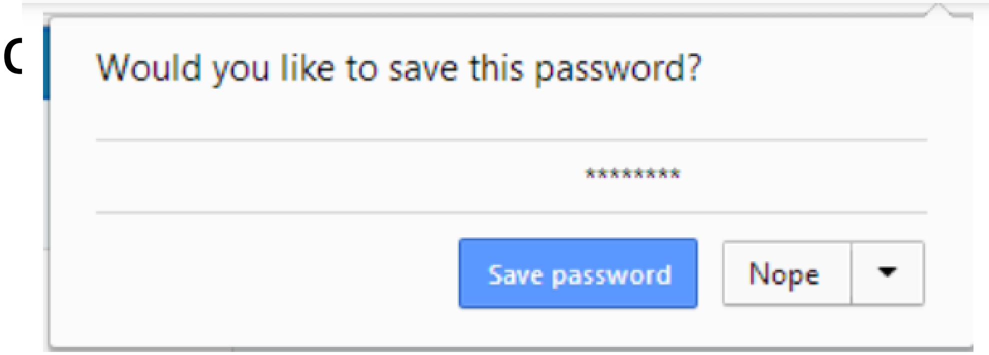


Save password?

Username admin

Password •••••

- Never share your passw



Would you like to save this password?

********

# Some security tips…

## Protect personal & company data

- Use two-factor authentication
  - Password
  - Code / PIN

- (or multi-factor)
  - Something you are / biometric
  - Something you have
  - Something you know
  - Location
  - Time

# Common Security Mistakes

Using unknown flash drives

Security Awareness Episode 5: Removable Media

https://www.youtube.com/watch?v=FRxrHduwPjY (1:22)

# Common Security Mistakes

No security solutions – e.g. No anti-virus

**Install and antivirus and anti-malware.**

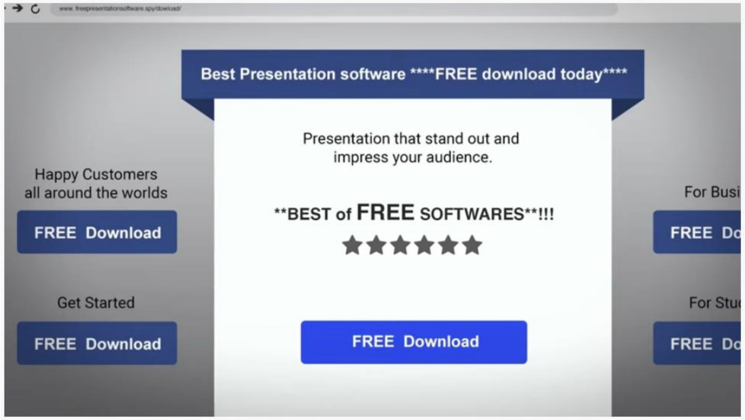
Myth - Antivirus is a complete protection ☒

- ➢ No complete solution – AV + IDA + firewall + user awareness

# Common Security Mistakes

Downloading unsolicited antivirus software

Downloading apps from third-parties



Best Presentation software ****FREE download today****

Presentation that stand out and impress your audience.

**BEST of FREE SOFTWARES**!!!

★★★★★★

Happy Customers all around the worlds

FREE Download

Get Started

FREE Download

FREE Download

For Busi

FREE Do

For Stud

FREE Do

Security Awareness Episode 7: Internet Downloads

[https://www.youtube.com/watch?v=7Apu1EWZPhQ](https://www.youtube.com/watch?v=7Apu1EWZPhQ)
(1:39)

# Common Security Mistakes

Ignoring on software updates/security patches.

Disabling User Account Control Features

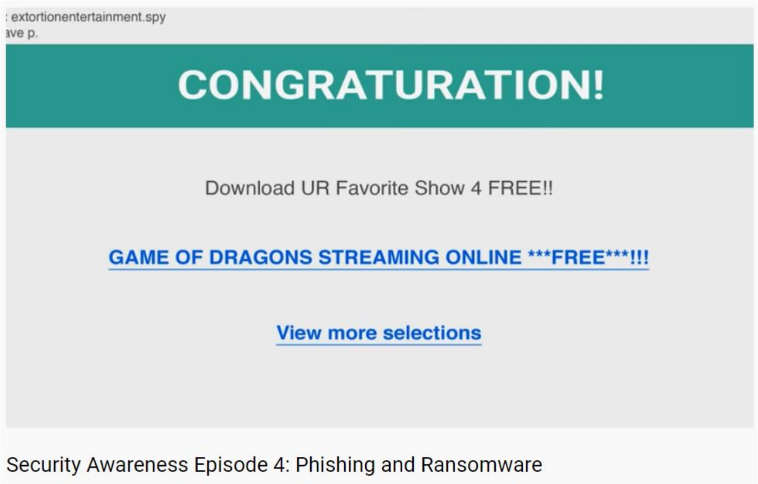
Ignoring SSL certificate warnings

**Update your OS with latest patches.**

# Common Security Mistakes

## Too trustworthy

- Opening e-mail attachments
- Clicking questionable links
- Answering phishing emails



: extortionentertainment.spy
ave p.

CONGRATURATION!

Download UR Favorite Show 4 FREE!!

GAME OF DRAGONS STREAMING ONLINE ***FREE***!!!

View more selections

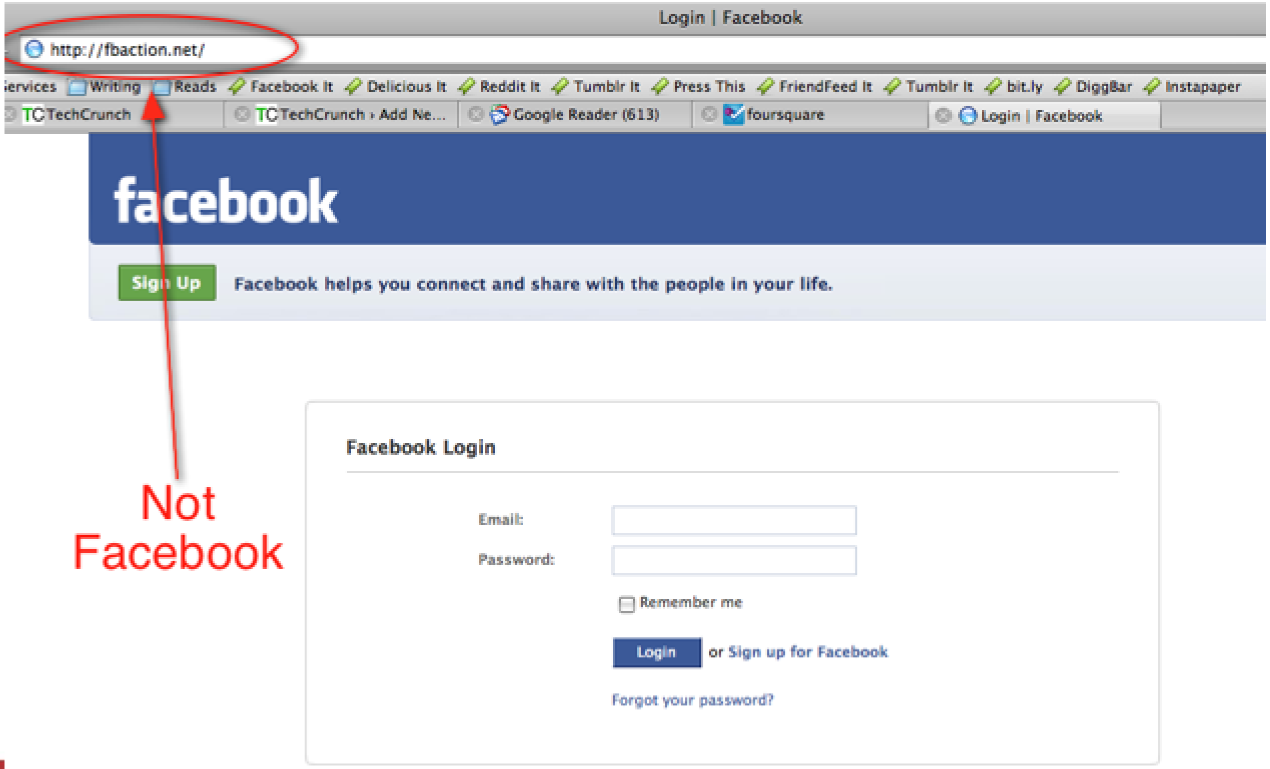
Security Awareness Episode 4: Phishing and Ransomware

https://www.youtube.com/watch?v=D_yAYhjNE-0 (2:33)

# Some security tips…

## Access only authentic verified URLs

Don't click any suspicious link.



Facebook helps you connect and share with the people in your life.

Facebook Login

Email:

Password:

□ Remember me

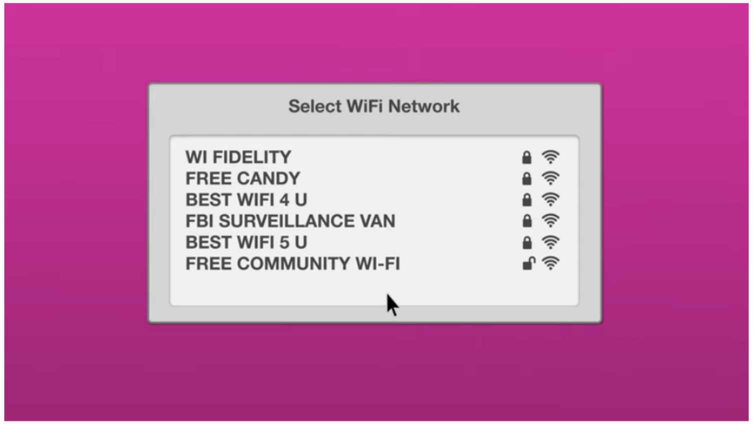
Login or Sign up for Facebook

Forgot your password?

Not Facebook

# Common Security Mistakes

## Using public WiFi



Select WiFi Network

WI FIDELITY 🔒
FREE CANDY 🔒
BEST WIFI 4 U 🔒
FBI SURVEILLANCE VAN 🔒
BEST WIFI 5 U 🔒
FREE COMMUNITY WI-FI 🔓

Security Awareness Episode 8: Wi-Fi

https://www.youtube.com/watch?v=RQttayB5ymA (2:05)

- Public wifi – for searching and reading only. **Never login** to any account to do online transactions
- Wifi hacking toolkits – can access from a distance

# When using public WiFi

1. Don’t use Internet banking or type in your bank card info
2. Turn off Wi-Fi if you don’t use the Internet

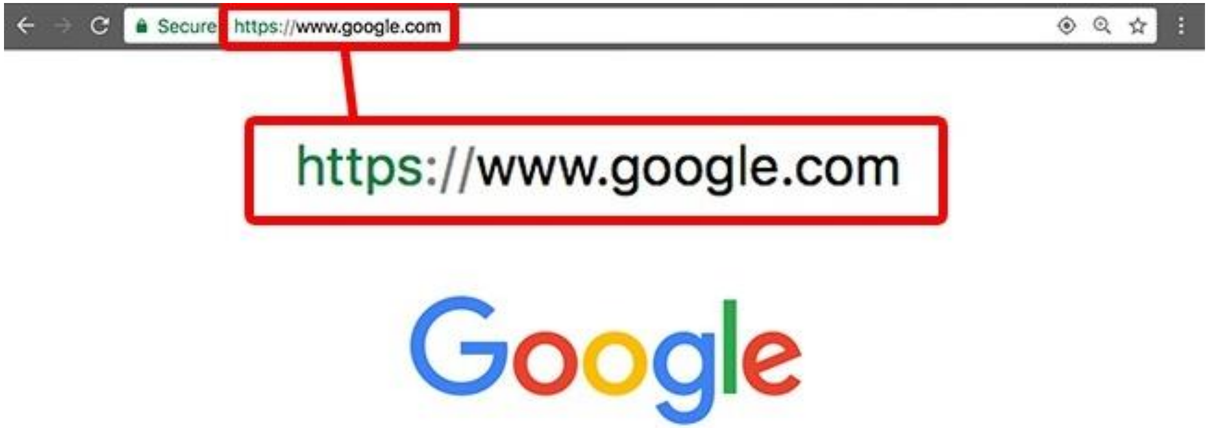
   Will resolve three issues:

   - rapid discharge of your battery,
   - automatic connection to a fraudulent network,
   - annoying ad emails
3. Connect using VPN
   - allows you to stay anonymous while online
4. Don’t let your device remember the network
5. Pay attention to the name of the network

BRIGHT SIDE

# When using public WiFi

6. Install a good antivirus software, and always update it
7. Choose networks with two-stage authentication
8. Keep your password encrypted
   - Can use a password manager that encrypts information in it
9. Check the website’s URL



# Common Security Mistakes

Browsing on unsecured connections

If the network isn't secure,

- and you log into an **unencrypted site**
- or a site that uses encryption only on the sign-in page
- other users on the network can see what you see and send.
- They could hijack your session and log in as you.

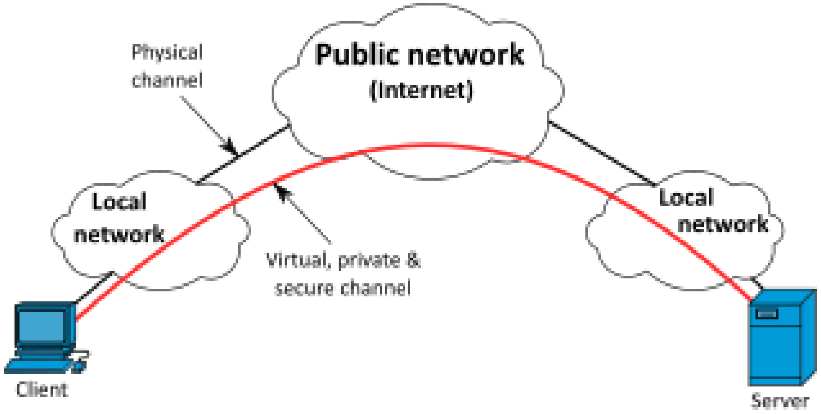
http://
http://
VS
Secure
https://
Secure
https:/

# Some security tips…

## Use VPN (Virtual Private Network)

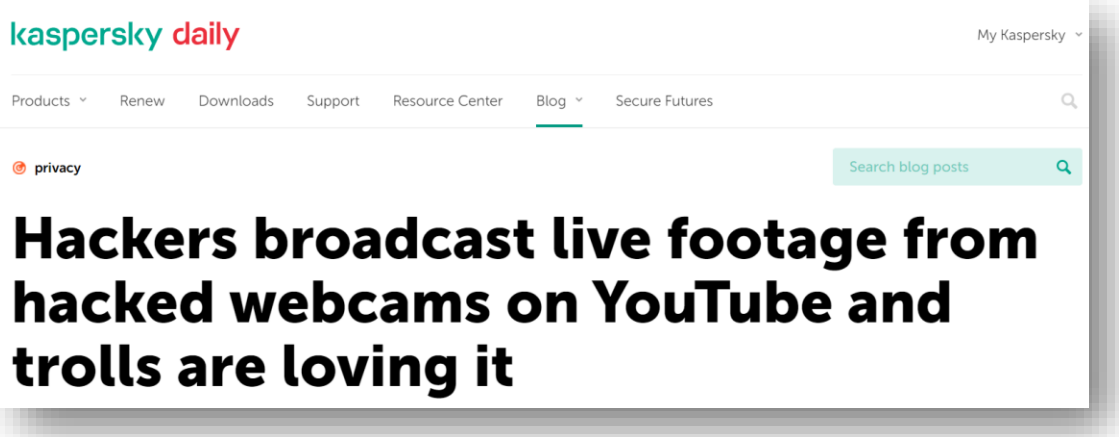
- send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- established using an encrypted layered tunneling protocol
- VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security.

Always use VPN to remote access your data from public to private LAN.



# Common Security Mistakes

Leaving your webcam open to attack



**Hackers broadcast live footage from hacked webcams on YouTube and trolls are loving it**

# Camera

- Camera on laptop, webcam, and on smartphones.
- **Seal/Cover** if not used.
- When connected to Internet, webcam can be turned ON remotely without your knowledge

# Common Security Mistakes

## Leaving devices unattended

Don't leave mobile devices unattended in public locations.

Don’t leave sensitive information lying around, including on printers, fax machines, or copiers.

When you are away from your desk, either shut down or lock your terminal with password protection.

Set your computer to automatically lock when you are not using it.

# Some security tips…

Do not leave your devices unattended

Protect personal & company data

- Always lock your computer when leaving it.
- Clean desk policy
- Secure your area before leaving it unattended.
- Securely delete and erase all content of old computer, and mobile devices.
- Shred personal or sensitive information
- Post a sign
- Lock the door
- Position away from viewing

Enter your password

Enter the password for winobstest@outlook.com

# Common Security Mistakes

Do not overshare on social media

Protect personal & company data

Oversharing
on
social media

It's good to share ...
but some things
are best kept
to yourself.

Be aware of what you share

# Social Engineering

# on Social Network

Personal information

Seems harmless

Oversharing

Online quizzes

**Oversharing**

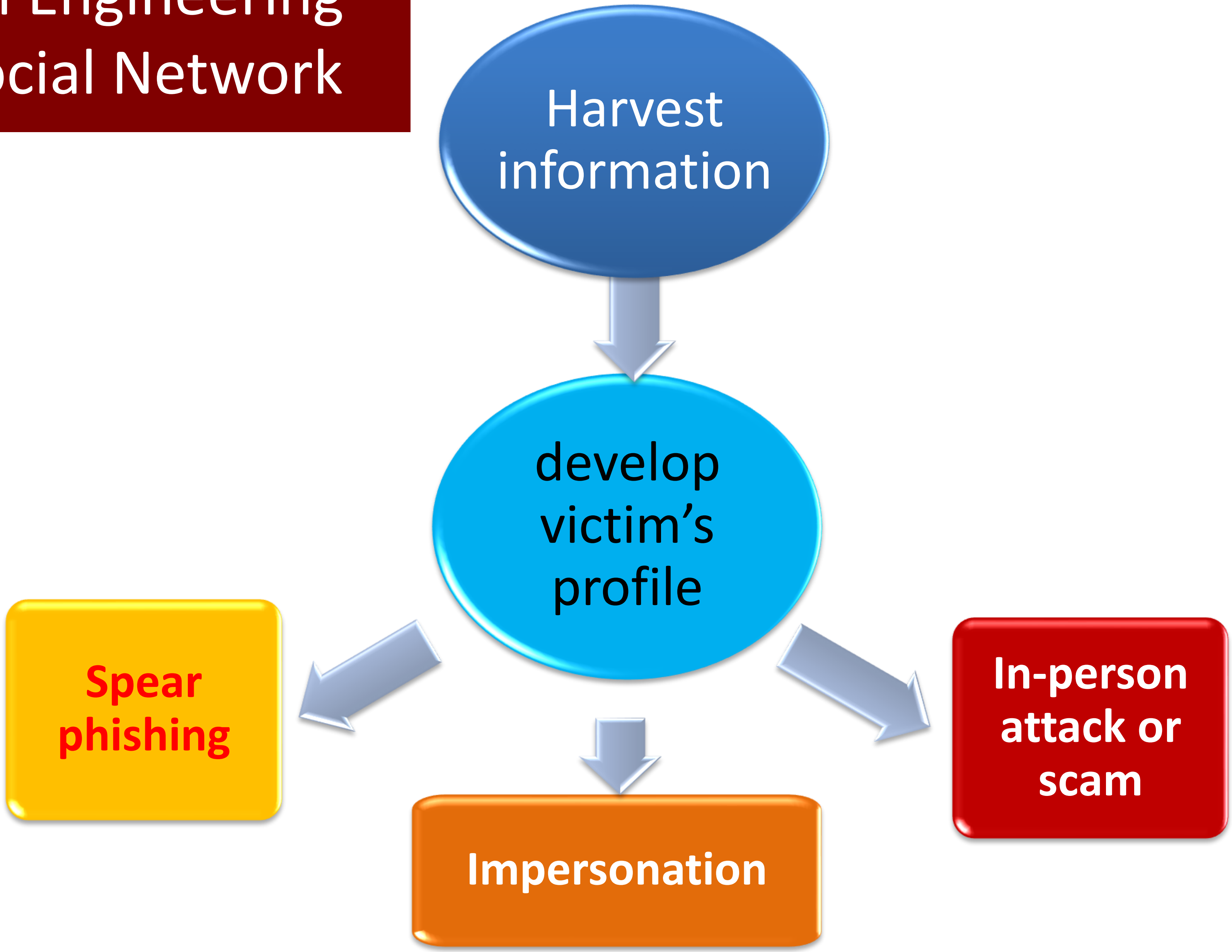
**Social engineering**

# Social Engineering on Social Network

## Be careful of online quizzes on social media, etc.

- What does your password say about you?
- What does Wiki say about you?
- Know your personality based on colours
- … and more

# Social Engineering on Social Network



# Privacy Issues

- FOURSQUARE automatic posts have led to physical altercations, break-ins, and other types of crime as a result of people making their posts public instead of restricting them to just those they really want to see them.
- **FarmVille** and **Texas Hold'em** reportedly sent facebook user information to at least 25 advertising and data firms.
- Until July of 2012, **Instagram** had a privacy vulnerability that exposed private photos to anyone without requiring authorization.

Vamosi, R., Protect your online privacy (without reading all the fine print). *PCWorld*, March 30, 2011. http://www.pcworld.com/businesscenter/article/221104/protect_your_online_privacy_without_reading_all_the_fine_print.html.
‡ Ragan, S., Instagram patches privacy vulnerability that exposed private photos. *Security Week*, July 12, 2012. http://www.securityweek.com/instagram-patches-privacy-vulnerability-exposed-private-photos.

# Some security tips…

## Protect personal & company data

- Safely dispose of personal information.
  - Shred, burn.
  - Beware of **dumpster diving**
    - to get info from your trash
    - Personal data
    - Company data

# Common Security Mistakes

‘It won’t happen to me’

# Why Physical Security?

Not all threats are “cyber threats”

Information one  commodity that can be stolen without being “taken”

Physically barring access is first line of defense

Forces those concerned to prioritize!

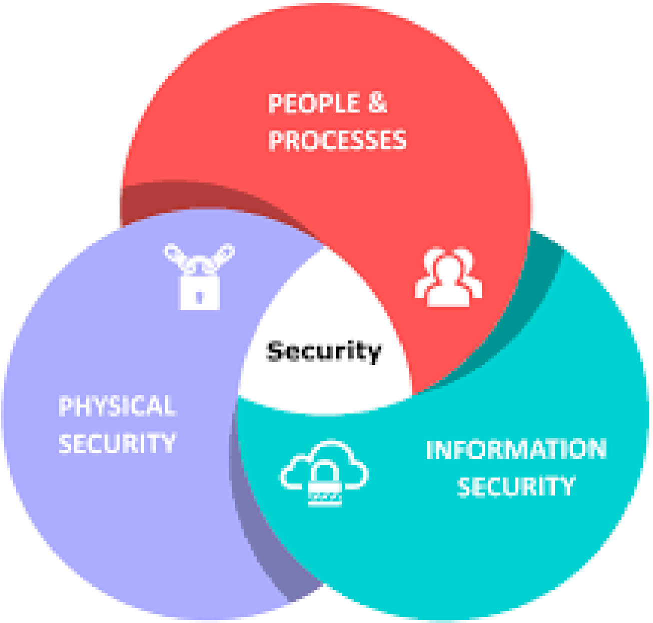
Physical security can be a deterrent

Security reviews force insights into value of what is being protected

PHYSICAL SECURITY THREATS

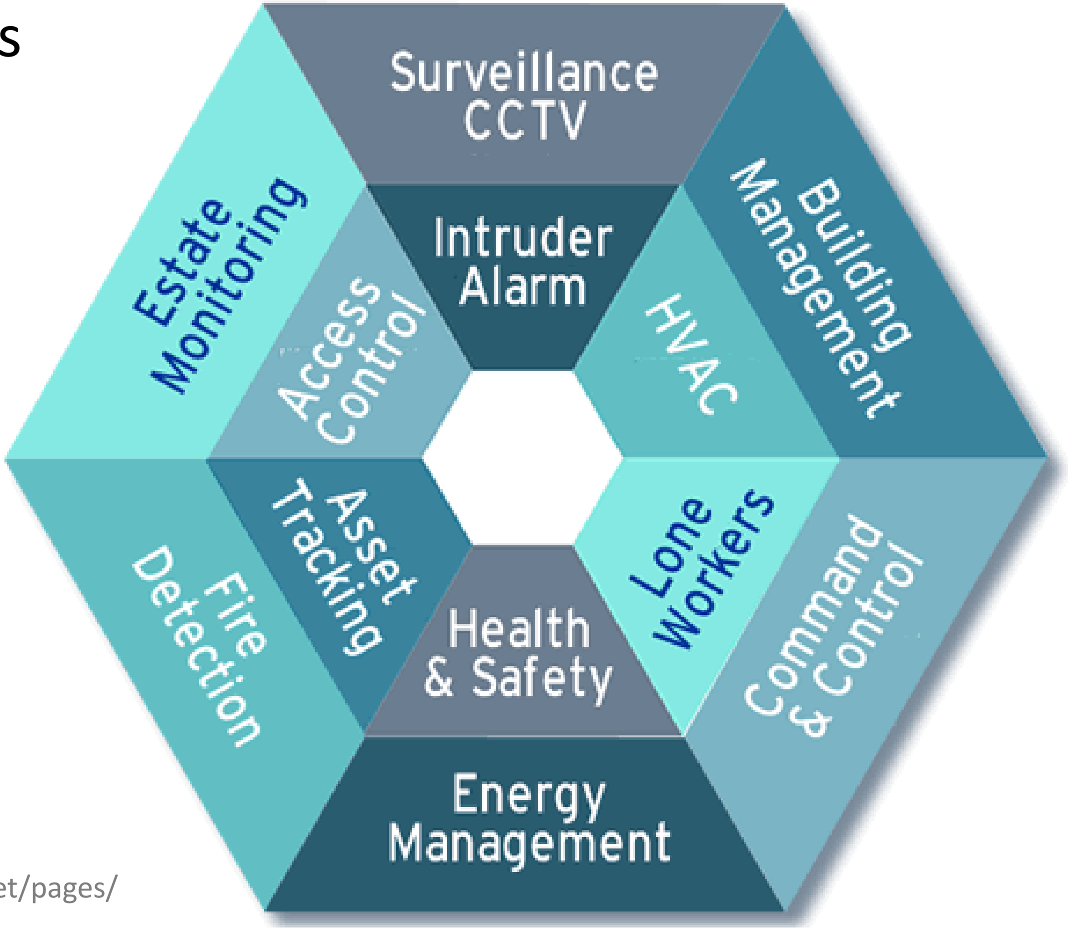
[THAT ARE OFTEN OVERLOOKED]

genieall



# Physical Security

Physically barring access is the **first line of defense**



https://www.visualmanagementsystems.net/pages/core-products/titan-security-portfolio.html

# Preventive Physical Controls

- to prevent unauthorized personnel from entering computing facilities i.e., locations housing
  - computing resources,
  - supporting utilities,
  - computer hard copy, and
  - input data media
- to help protect against disasters (natural or man-made).
  - Flood, weather, lightning, earthquake, tornado
  - Power Failures
  - Fire, pollution

- Backup files and documentation.
- Fences.
- Security guards.
- Badge systems.
- Double door systems.
- Locks and keys.
- Backup power.
- Biometric access controls.
- Site selection.
- Fire extinguishers.
- Handling of trash or scrap

# Creating a Security Culture

## Tips on How to Create a Cyber Security Culture at Work

- Focus on security basics
- Invest in employee awareness training
- Encourage the senior leadership to embody organizational security

[Bisson, 2015]

# Securing your data

**1. Keeping Your Personal Information Secure Offline**

- Lock your financial documents and records in a safe place at home.
- Lock your wallet or purse in a safe place at work.
- Keep your information secure from roommates or workers who come into your home.

**2. Keeping Your Personal Information Secure Online**

- Be Alert to Impersonators
- Safely Dispose of Personal Information
- Encrypt Your Data
- Keep Passwords Private

# Securing your data

**3. Securing Your Identification Card Number**

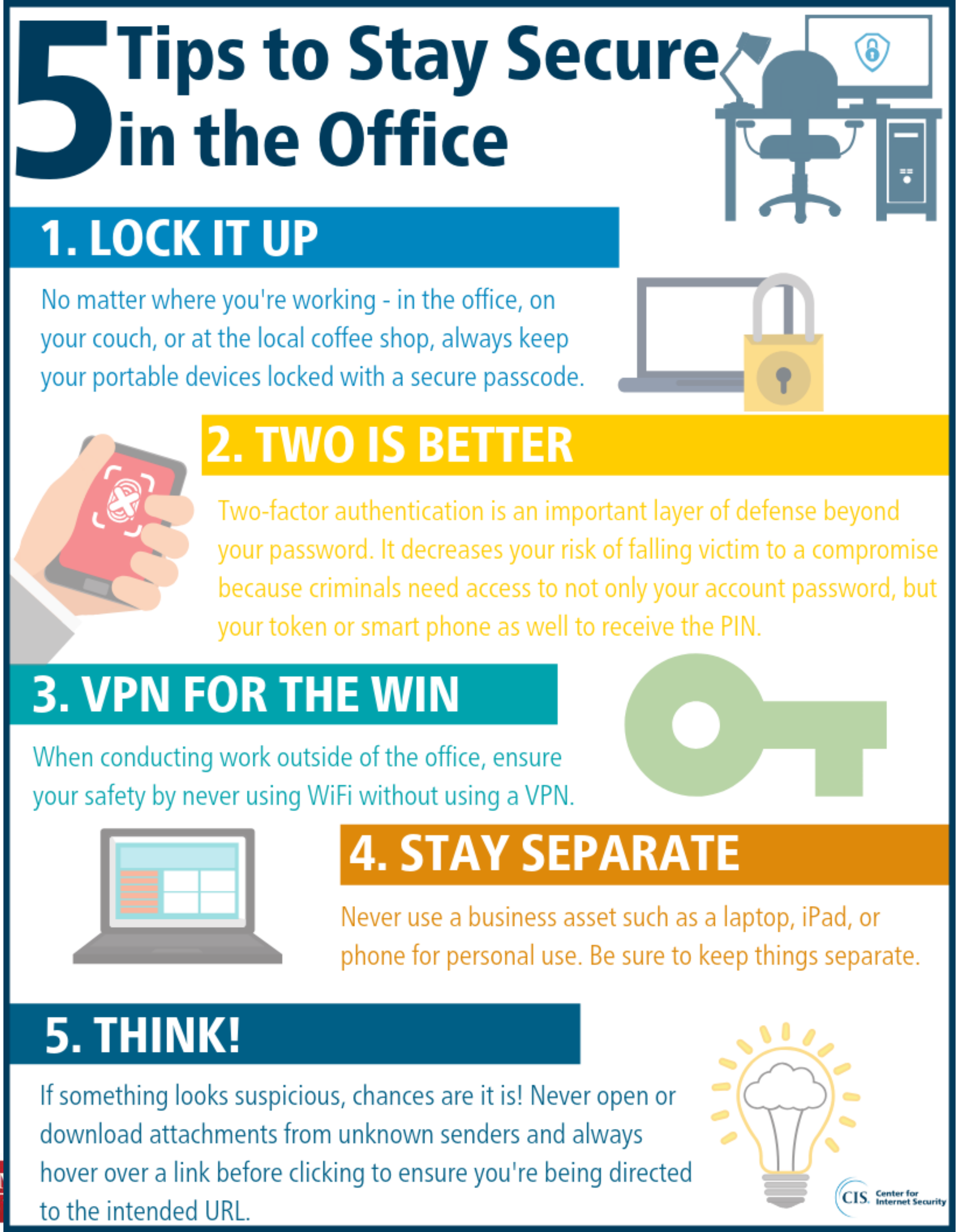
- Keep a close hold on your IC number
- Ask questions before deciding to share it.
- Ask if you can use a different kind of identification

**4. Keeping Your Devices Secure**

- Use Security Software
- Avoid Phishing Emails
- Be Wise About Wi-Fi
- Lock Up Your Laptop

# Some security tips…

- Email - Separate work email from personal email
- Always check access log in my device.
- Backup data regularly – external drive, cloud
- Cloud security - Leakage – personal info (photos, private docs, etc.)
- Read the fine prints



# 5 Tips to Stay Secure in the Office

## 1. LOCK IT UP

No matter where you're working - in the office, on your couch, or at the local coffee shop, always keep your portable devices locked with a secure passcode.

## 2. TWO IS BETTER

Two-factor authentication is an important layer of defense beyond your password. It decreases your risk of falling victim to a compromise because criminals need access to not only your account password, but your token or smart phone as well to receive the PIN.

## 3. VPN FOR THE WIN

When conducting work outside of the office, ensure your safety by never using WiFi without using a VPN.

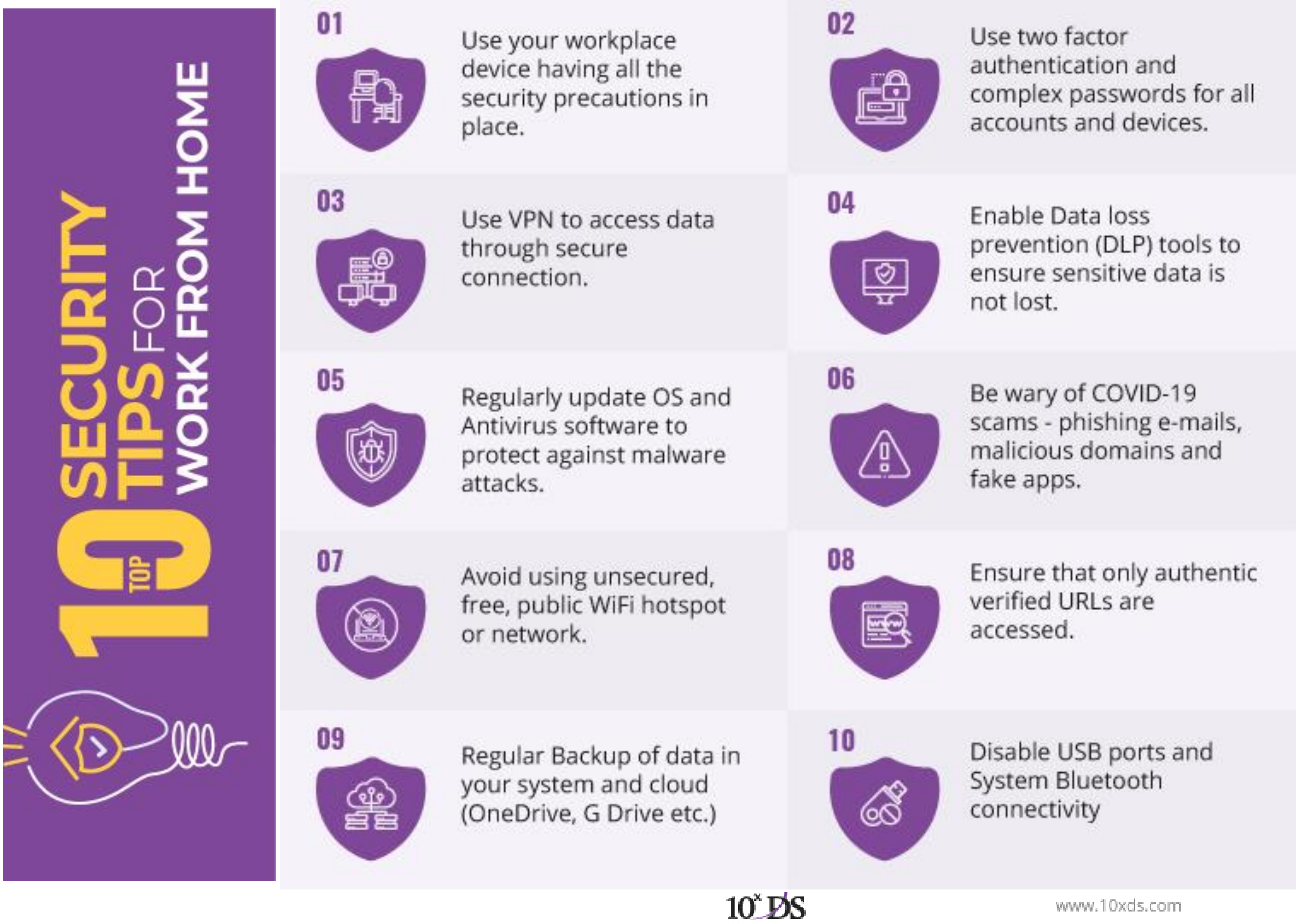
## 4. STAY SEPARATE

Never use a business asset such as a laptop, iPad, or phone for personal use. Be sure to keep things separate.

## 5. THINK!

If something looks suspicious, chances are it is! Never open or download attachments from unknown senders and always hover over a link before clicking to ensure you're being directed to the intended URL.

CIS Center for Internet Security



## TOP 10 SECURITY TIPS FOR WORK FROM HOME

01 Use your workplace device having all the security precautions in place.

02 Use two factor authentication and complex passwords for all accounts and devices.

03 Use VPN to access data through secure connection.

04 Enable Data loss prevention (DLP) tools to ensure sensitive data is not lost.

05 Regularly update OS and Antivirus software to protect against malware attacks.

06 Be wary of COVID-19 scams - phishing e-mails, malicious domains and fake apps.

07 Avoid using unsecured, free, public WiFi hotspot or network.

08 Ensure that only authentic verified URLs are accessed.

09 Regular Backup of data in your system and cloud (OneDrive, G Drive etc.)

10 Disable USB ports and System Bluetooth connectivity

10xDS

www.10xds.com

# To avoid Malware

- **What To Do**
  - Only open email or IM attachments that come from a trusted source and that are expected
  - Have email attachments scanned by antivirus software before opening them
  - Delete all unwanted messages without opening
  - Do not click on Web links sent by someone you do not know
  - If a person on your Buddy list is sending strange messages, files, or web site links, terminate your IM session
  - Scan all files with an Internet Security solution before transferring them to your system
  - Only transfer files from a well-known source
  - Use Internet Security software to block all unsolicited outbound communication
  - Keep security patches up to date

Norton.com

# Spyware

- **How to Avoid Spyware?**
  - Be selective about what you download to your computer
  - Read licensing agreements
  - Watch out for **anti-spyware** scams
  - Beware of clickable ads
  - Keep your Internet browser up to date
  - Scan your computer often

Norton.com

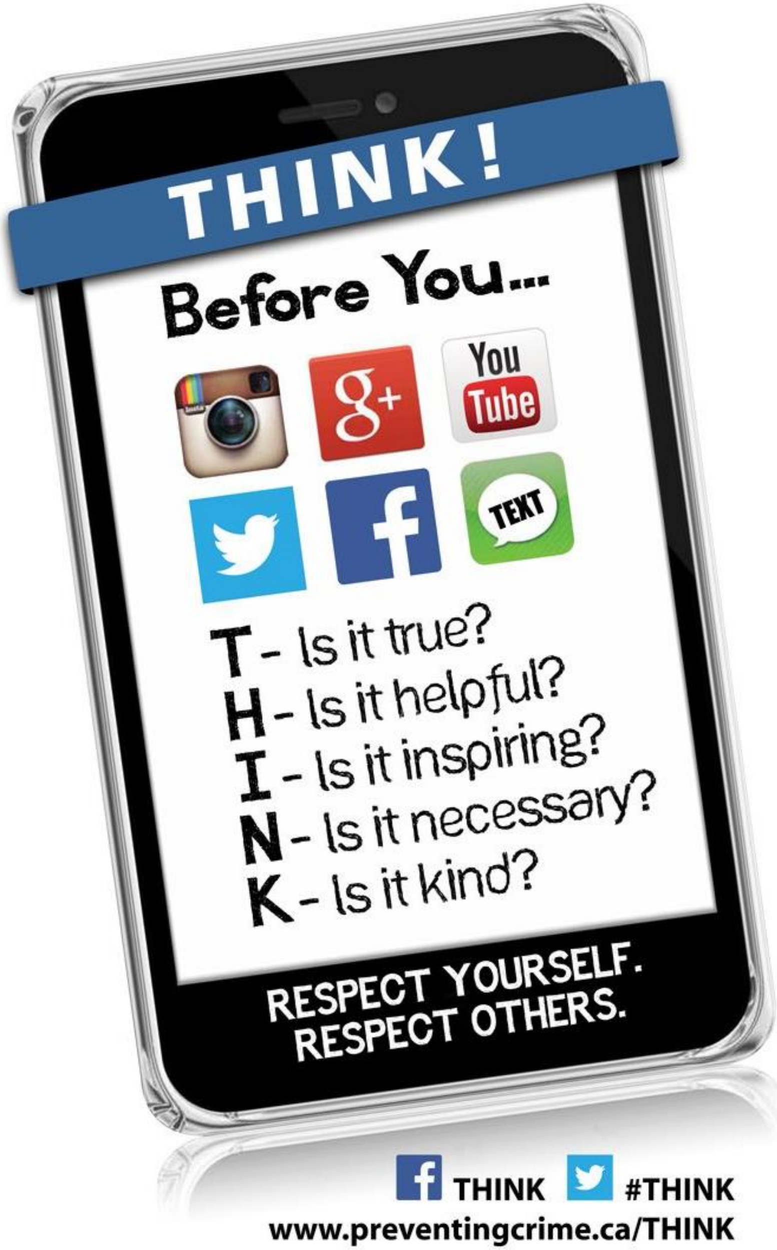
# Camera

Be extra cautious when posting pictures/videos on social media

What goes on the Internet STAYS on the Internet

Everything is ‘**permanent**’
Even after you have deleted it

It can be easily **shared**
and you cannot control it



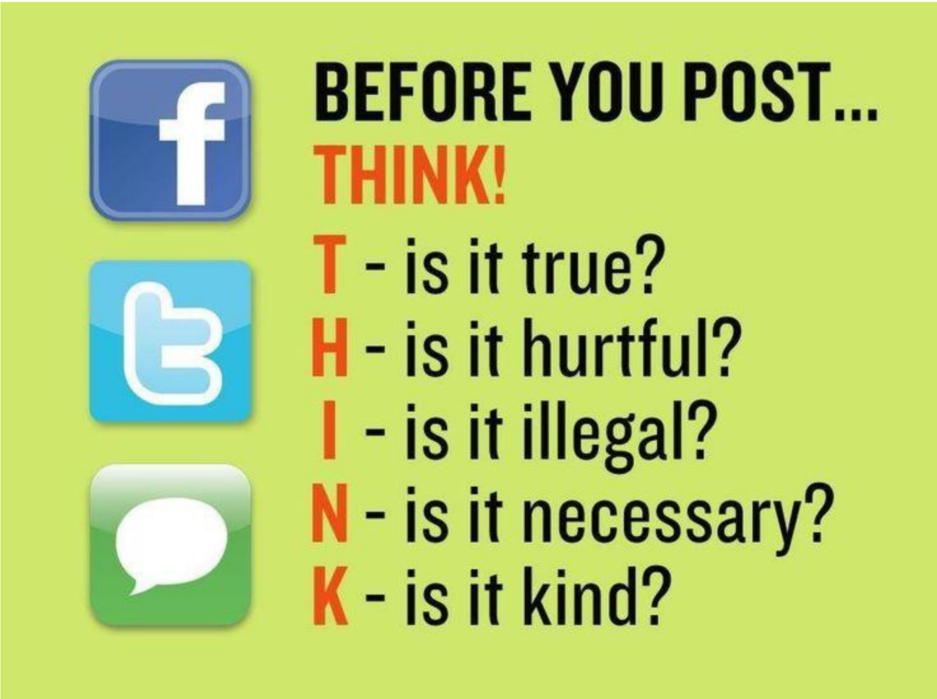
THINK!

Before You...

T - Is it true?
H - Is it helpful?
I - Is it inspiring?
N - Is it necessary?
K - Is it kind?

RESPECT YOURSELF.
RESPECT OTHERS.

THINK #THINK
www.preventingcrime.ca/THINK



BEFORE YOU POST...
THINK!

T - is it true?
H - is it hurtful?
I - is it illegal?
N - is it necessary?
K - is it kind?

# Protect Yourself

1. Be discreet
2. Be skeptical
3. Be thoughtful
4. Be professional
5. Be wary
6. Check privacy policies

CyberSecurity Malaysia, 2011

# Conclusion

- Most security breaches originate internally!
  - Studies show most security breaches by internal employees are not intentional.

- Imperative to educate ALL ICT users
  - of the challenges and threats
  - how the usage can be managed and controlled
  - How the risks can be reduced or mitigated

**The best defenses is security AWARENESS**

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

UNIVERSITI PUTRA MALAYSIA

AGRICULTURE • INNOVATION • LIFE

# Terima Kasih | *Thank You*

izura@upm.edu.my