Cybersecurity
Protecting Yourself, Your Business, Your Clients
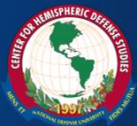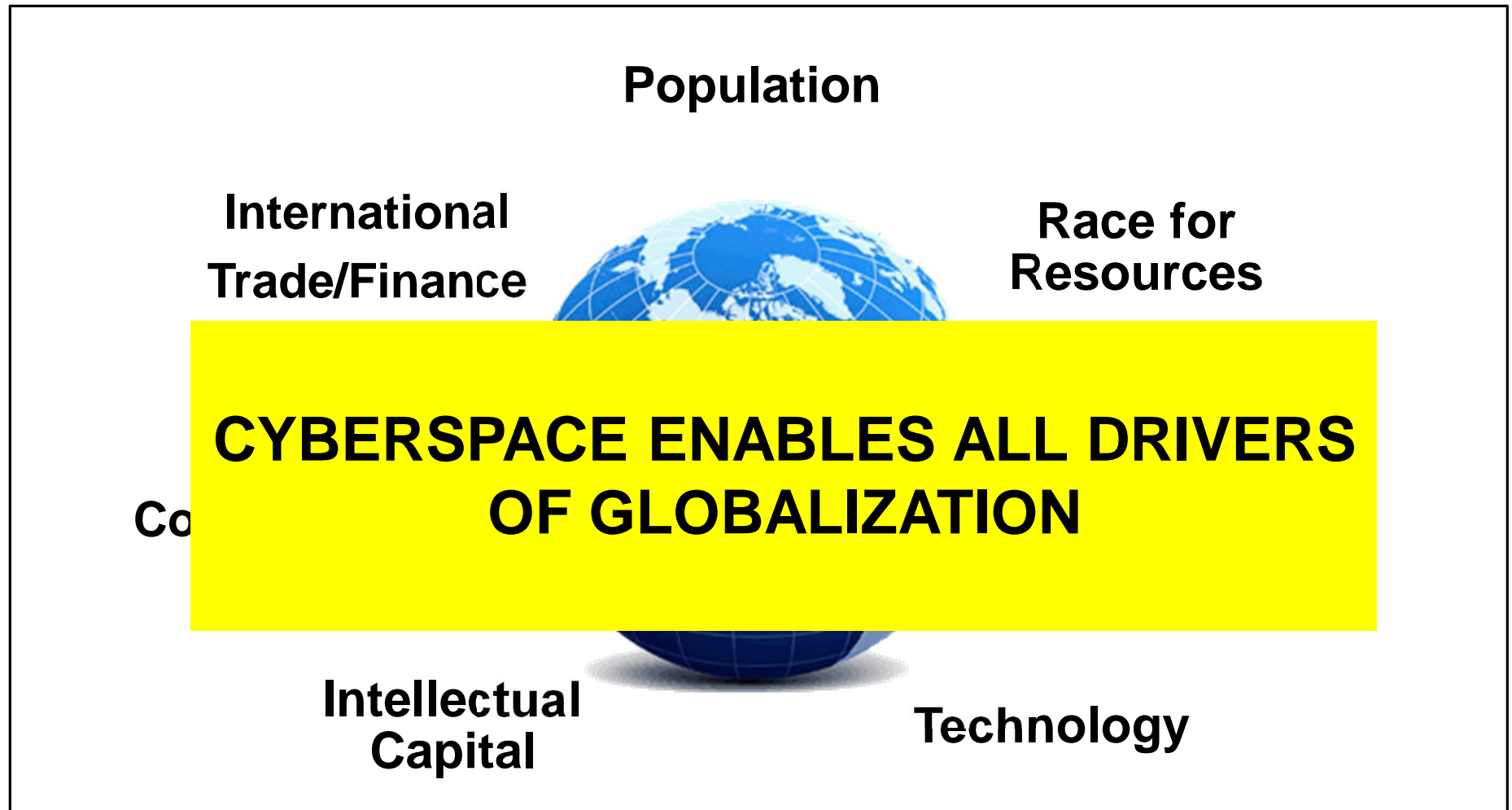
Global Summit of Women
June 7, 2014

Celina B. Realuyo
Professor of Practice of National Security Affairs
William J. Perry Center for Hemispheric Defense Studies
National Defense University
professorcelina@gmail.com

The Drivers in an Age of Globalization

Population

International Trade/Finance

Race for Resources

Co...

Intellectual Capital

Technology

CYBERSPACE ENABLES ALL DRIVERS OF GLOBALIZATION

The Universe of Cybersecurity Threats

Cybercrime

Hactivism

Cyberterrorism

CYBER SECURITY

Nation States

Targets and Types of Cybercrime

Targets

- Against individuals (identity theft or harassment)
- Against property (attacks on or theft of property – IPR)
- Against the nation state

Cyberspace Domain for Criminal Activities

- Financial Crime/Identity Theft
- Child Pornography
- Counterfeit
- Online Gambling
- IPR theft

Increasing Risk of Cybercrime

The Reasons

• Outdated legal framework against cybercrime

• Private sector reluctance to report incidents

• Inadequate cybersecurity systems

• Lack of awareness of threats

• Strong economic development

• Attractive targets: banks, energy sector,   critic
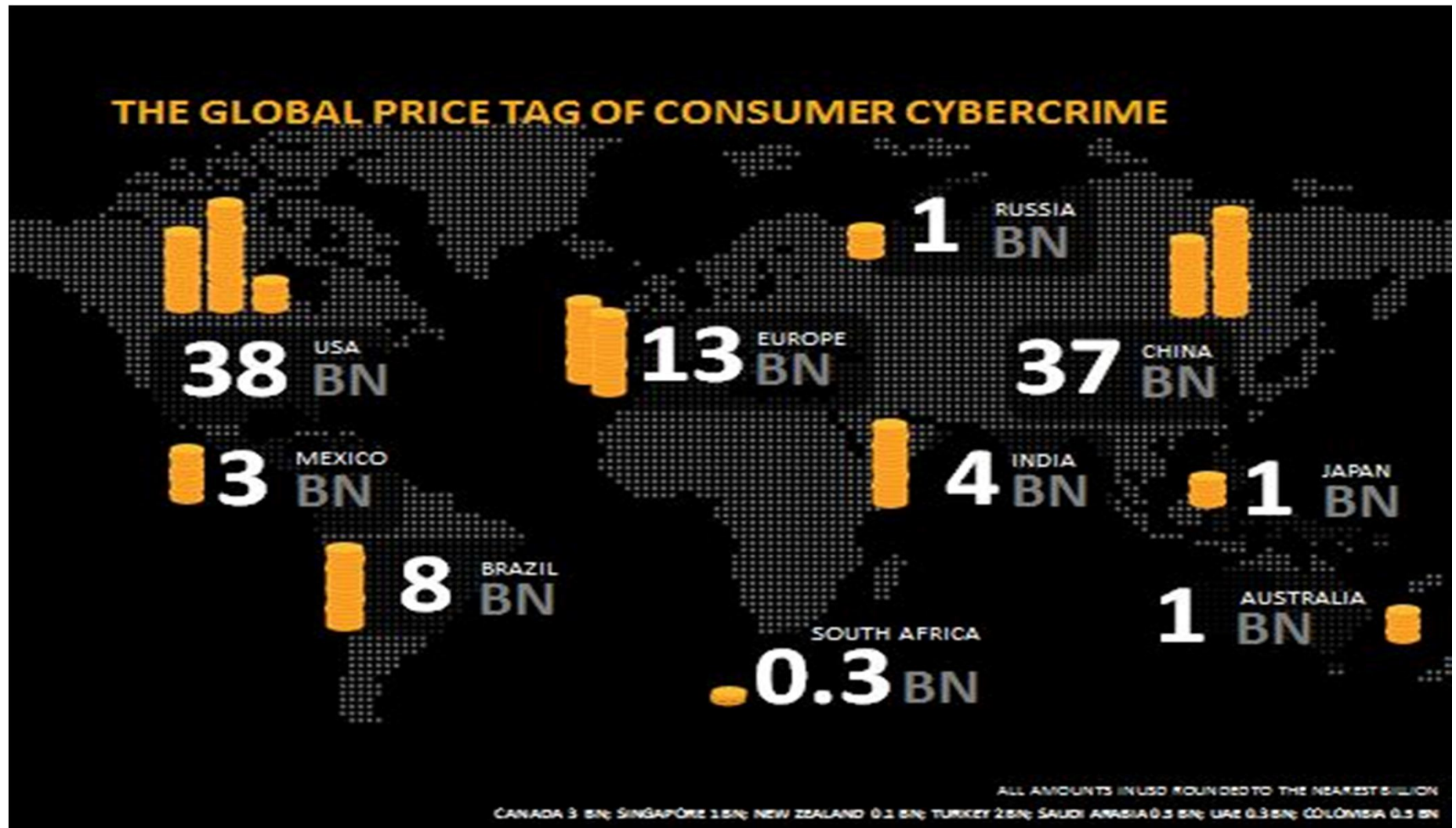infrastructure, tourism, international businesses

Source:Trend Micro

The Cost of Cybercrime by Country 2013

THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME

1 BN RUSSIA

38 BN USA

13 BN EUROPE

37 BN CHINA

3 BN MEXICO

4 BN INDIA

1 BN JAPAN

8 BN BRAZIL

1 BN AUSTRALIA

SOUTH AFRICA 0.3 BN

ALL AMOUNTS IN USD ROUNDED TO THE NEAREST BILLION

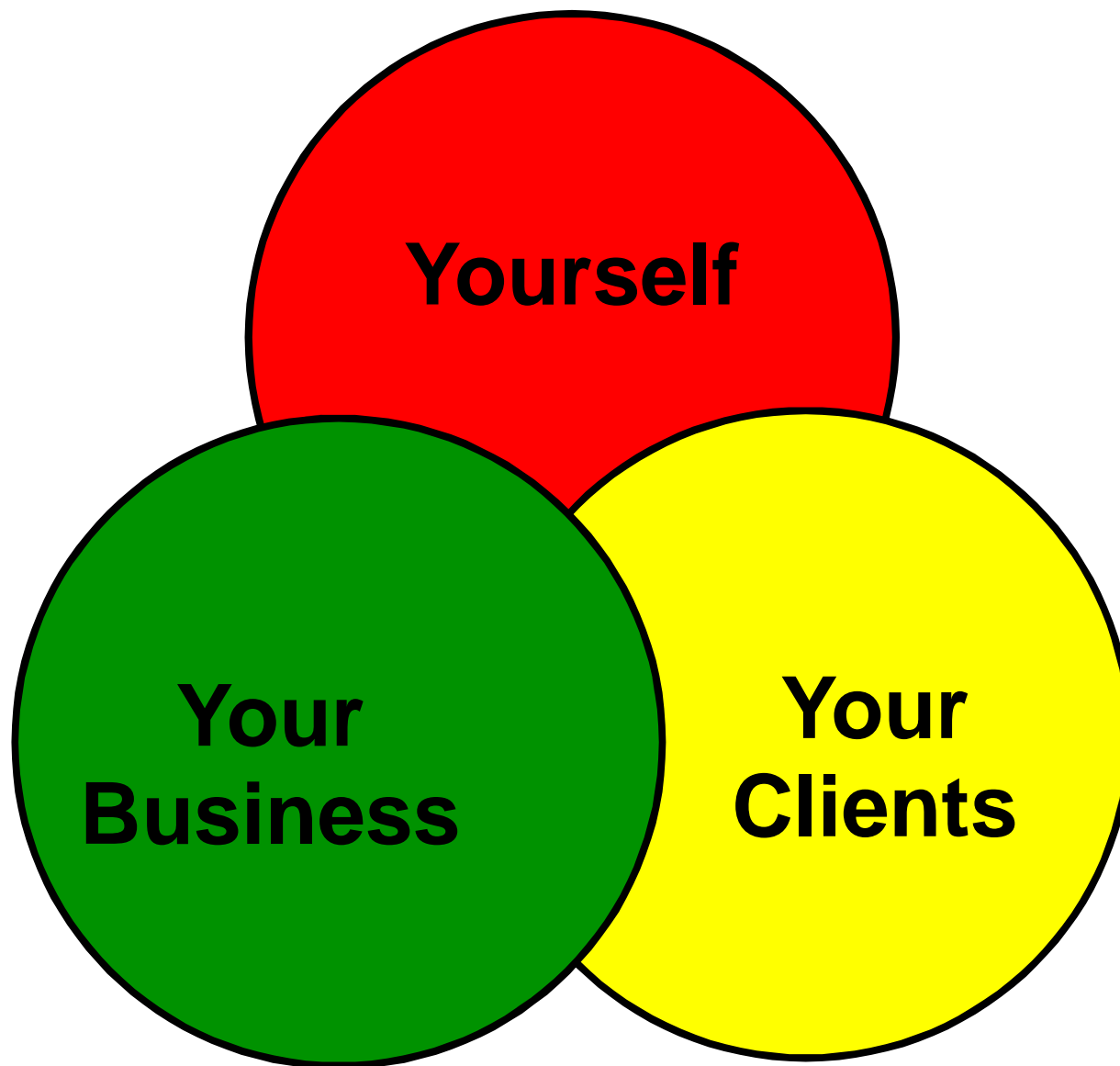CANADA 3 BN; SINGAPORE 1 BN; NEW ZEALAND 0.1 BN; TURKEY 2 BN; SAUDI ARABIA 0.5 BN; UAE 0.3 BN; COLOMBIA 0.5 BN

Source:2013 Norton Cybercrime Report

Source: Celina B. Realuyo, WJPC
RealuyoC@ndu.edu

CYBERSECURITY: HOW VULNERABLE ARE YOU?

SOCIAL MEDIA – ARE WE SHARING TOO MUCH?

ADVANTAGES AND RISKS OF
GPS PHONE LOCATION SERVICES

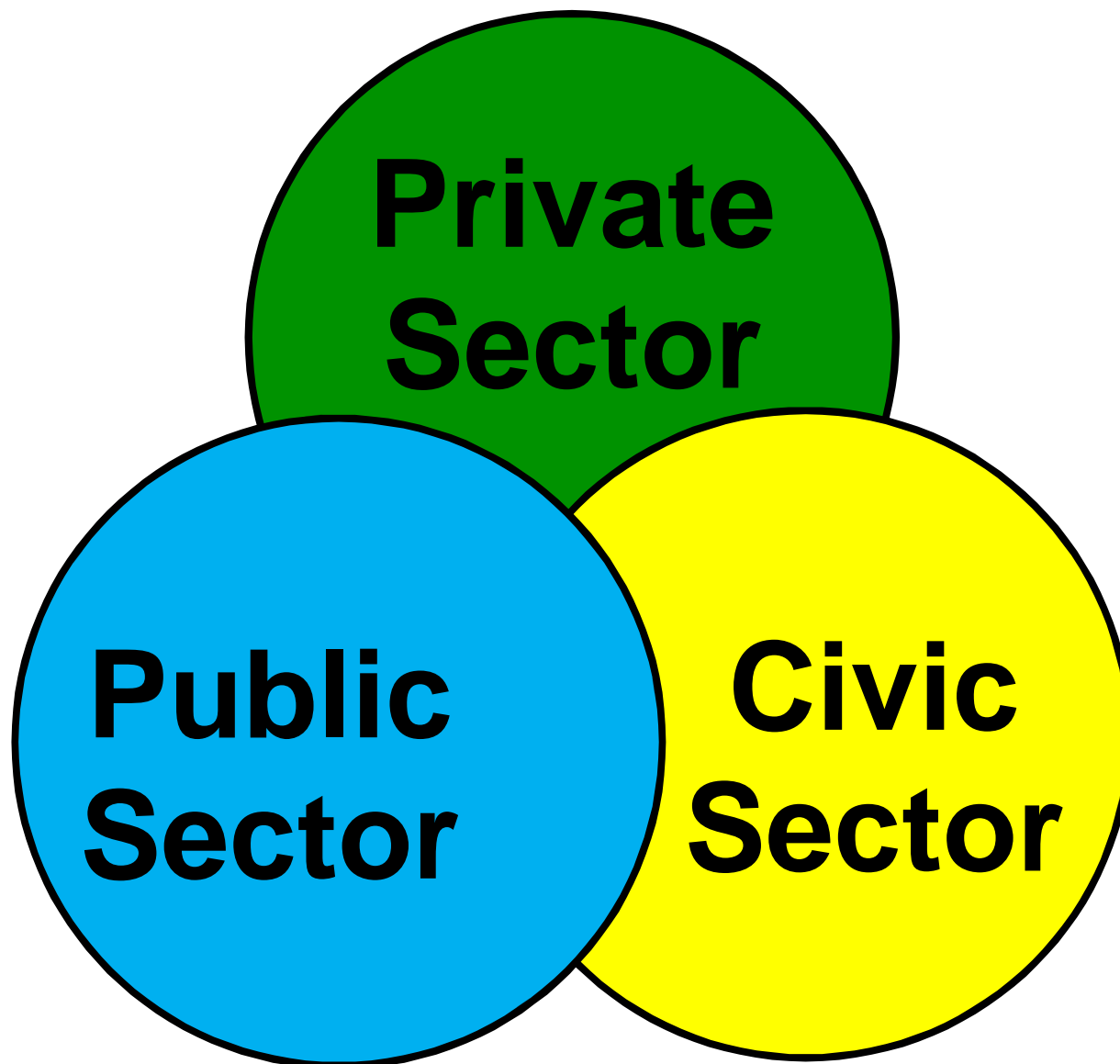# Large Personal Data Breaches and Reputational Risk

Five Recommendations to Enhance Cybersecurity

1. Beware of disclosing too much information online
2. Monitor your personal and business transactions regularly
3. Invest in protecting your business operations in cyberspace
4. Safeguard your personal, business, and client data
5. Address any cyber breach immediately and transparently

CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

Some nice videos

CyberWatch: Febelfin – Belgium Federation of Financial Sector:

http://youtu.be/F7pYHN9iC9I

https://www.youtube.com/watch?annotation_id=annotation_2 02513&feature=iv&src_vid=F7pYHN9iC9I&v=Rn4Rupla11M

A Hacker in action:

http://www.liveleak.com/view?i=807_1383224319

Some rouge data about cyber war, cyber losses, etc.

http://www.youtube.com/watch?v=PIELVMQhvXc

How many of you have more than one device to conect to Internet?

How many of you know how to protect it?

STOP.THINK. CONNECT .™

STOP. THINK. CONNECT.™ is the global cybersecurity awareness campaign to help all digital citizens stay safer and more secure online.

The message was created by a coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG).

- **STOP:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

- **THINK:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

- **CONNECT:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Visit http://www.stopthinkconnect.org for more information

STOP | THINK | CONNECT™
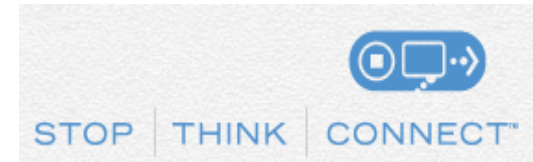
Keep a Clean Machine.

Protect Your Personal Information.

Connect with Care.

Be Web Wise.

Be a Good Online Citizen.

TIPS & ADVICE: Good Online safety habits
1.- Keep a Clean Machine

On computers /laptops and tablets:

- **Keep security software current**

- **Automate software update**

- **Plug & scan**

On Smartphones:

Take the same precautions on your mobile device as you do on your computer with regard to messaging and online safety.

Mobile devices are computers with software that need to be kept up-to-date (just like your PC, laptop or tablet).

- **Keep security software current**.

On all:

- **Protect all devices that connect to the Internet** from viruses and malware.

TIPS & ADVICE: Good Online safety habits
2.- Protect your personal information

On computers /tablets and Internet:

- **Secure your accounts:** Ask for protection beyond passwords.

- **Make passwords long and strong**

- **Unique account, unique password**

- **Write it down and keep it safe**

- **Own your online presence**

On Smartphones:

Phones can contain tremendous amounts of personal information. Protect your phone like you would your computer.

- **Secure your phone**

- **Think before you app**

- **Only give your mobile number out to people you know and trust**

- **Learn how to disable the geotagging feature on your phone** at http://icanstalku.com/how.php#disable

TIPS & ADVICE: Good Online safety habits

3.- Connect with Care

Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.

On computers /tablets and Internet:

- **When in doubt, throw it out**

- **Get savvy about Wi-Fi hotspots**

- **Protect your $$:** When banking and shopping, check to be sure the sites is security enabled.

On smartphones:

- **Get savvy about Wi-Fi hotspots**.

- **When in doubt, don't respond**

TIPS & ADVICE: Good Online safety habits
4.- Be Web Wise

Stay informed of the latest updates on your device. Know what to do if something goes wrong.

On computers /tablets and Internet:

- **Stay current. Keep pace with new ways to stay safe online**.

- **Think before you act.**

- **Back it up**

On smartphones:

- **Know how to cell block others:** Use caller ID.

- **Use caution when meeting face-to-face** with someone who you only "know" through text messaging

TIPS & ADVICE: Good Online safety habits
5.- Be a Good Online Citizen

Remind you and your kids to maintain the same level of courtesy online as they would in the real world.

On computers /tablets and Internet:

- **Safer for me more secure for all**

- **Post only about others as you have them post about you.**

- **Help the authorities fight cyber crime:** Report stolen finances or identities and other cybercrime.

On smartphones:

It is easy to say things via phone or text message that you would never say face to face.

- **Text to others only as you would have them text to you.**

- **Only give your mobile number out to people you know and trust and never give anyone else's number out without their permission.**

- **Get permission before taking pictures or videos of others with your phone**.

How many of you use Social Nets?
How many of your kids are very active in social Nets?

Social Networking Tips

Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post and take basic precautions before going online.

- **Own your Online Presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing

- **Once Posted, Always Posted:** Protect your reputation on social networks.

- **Post Only about Others as You Have Them Post about You.** It's the golden rule online.

- **When in Doubt, Throw it Out**

- **Make Passwords Long, Strong and Unique**

- **Your Online Reputation can be a Good Thing**

- **Be Honest if you're Uncomfortable**.

- **Keep Personal Information Personal**.

- **Know and Manage your Friends**

Some advices to minimize risks

For parents

- Awareness about not to reveal information to unknown people.

- Stay alert to cyber news and show them to the kids when they happen (continuous alert).

- Show contact ways in the social nets with protection authorities.

- Implement parental control applications in the kids computers, laptops and mobiles for kids between 12-15 years old.

For Kids

- Everybody lie on the web, less or much, but everybody does it.

- Do not trust social nets users for the photos you see.

- Do not date physically with some one that is not of your real friends environment.

- If a friend introduce you someone in a social net, this is not your friend, is only an unknown guy.

- Check your mobile configuration and disconnect the GeoTag.

- Complex password

https://www.youtube.com/watch?v=47vtDPcU14o

THANKS A LOT

IDOIA MATEO
CISO & IT RISK MANAGING DIRECTOR
Santander Group

idmateo@gruposantander.com