



# Online Safety

**Janice Antoniette Forster, MIT, MBA**

*BOT, Philippine eLearning Society |*

*TBI Manager, Silliman University*

*[janicevforster@su.edu.ph](mailto:janicevforster@su.edu.ph)*



# Online Safety

- the process of using the services and resources of the Internet in a safe and secure manner.
- Why is it important? It's not paranoia. The world is a dangerous place, both on and offline. An ounce of prevention is worth a pound of cure



The combination of the safety concerns of the physical world and the new risks presented in the virtual world complicate the safety concerns you face when dealing with the Internet.



**damaged**



**stolen**



**lost**



**HACKER**





the number of people who can be a threat to you exponentially increases with the population of Internet users.





This information isn't meant to scare you from going online, but is intended to introduce you to potential threats and ways to protect yourself from those threats.





Awareness is  
the greatest  
agent for  
*change*

# Cybercrime Prevention Act of 2012



The Cybercrime Prevention Act of 2012, officially recorded as Republic Act No. 10175, is a law in the Philippines that was approved on September 12, 2012. It aims to address legal issues concerning online interactions and the Internet in the Philippines.

[Wikipedia](#)

**Bill introduced in the Senate:** Same title as final [law](#)

**Date passed by conference committee:** May 30, 2012

**Signed:** September 12, 2012

**Signed by:** [Benigno Aquino III](#)

ADVERTISEMENT

MG POWERED GARAGES

**FORWARD WITH ALL FRONTLINERS**

FOR AS LOW AS **ZERO** DP WITH 3-MONTH HOLIDAY PAYMENT SCHEME

SUV **MGRX5**

Learn More

NEWS OPINION SPORTS LIFESTYLE ENTERTAINMENT BUSINESS TECHNOLOGY GLOBAL NATION

INTERNET



# In the Know: The cybercrime law

Philippine Daily Inquirer / 05:31 AM February 19, 2014



EDITORS' PICK MOST READ

NEWSINFO

AFP warns Facebook: 'Enemies of the state'



Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, was signed into law by President Aquino on Sept. 12, 2012.

Its original goal was to penalize acts like cybersex, child pornography, identity theft and unsolicited electronic communication in the country.

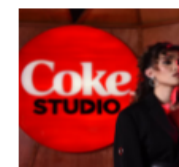
However, a provision expanding the scope of libel law to cover Internet posts was opposed by various groups, which asked the Supreme Court to issue a temporary restraining order (TRO) and a status quo ante order.

The cybercrime law could see Internet users sentenced to up to 12 years in prison for posting defamatory comments on Facebook or Twitter.

Online libel was not part of the original bill proposed by the Department of Justice (DOJ) but was one of the amendments inserted by the Senate as proposed by Sen. Vicente Sotto III.



NEWSINFO  
DENR probes mining firms in Manila Bay who sand project



ENTERTAINMENT  
KZ Tandingan taking it one step at a time

ADVERTISEMENT

HORRIS GARABES  
Since 1924**FORWARD  
WITH ALL  
FRONTLINERS**

I Agree

HR LIFE | LEADERSHIP



14/07/2016 Thu 11:49 in All markets by Anthony Wong

## Ranting about Pokémon Go, staff fired for “rude behaviour” on Facebook



The survey further revealed that more than half of employers (54%) have found content on social media that caused them not to hire a candidate for an open role. Here are 11 reasons why:

- Candidate posted provocative or inappropriate photographs, videos or information: 39%
- Candidate posted information about them drinking or using drugs: 38%
- Candidate had discriminatory comments related to race, gender, religion: 32%
- Candidate bad-mouthed their previous company or fellow employee: 30%
- Candidate lied about qualifications: 27%
- Candidate had poor communication skills: 27%
- Candidate was linked to criminal behavior: 26%
- Candidate shared confidential information from previous employers: 23%
- Candidate’s screen name was unprofessional: 22%
- Candidate lied about an absence: 17%
- Candidate posted too frequently: 17%



## 8 criminals who bragged on social media and got caught.



**CHIP DWYER**  
Aug 10, 2016 @ 2:40 AM



The best criminals know not to brag and flaunt their money, because it always draws unwanted attention from the law. But most criminals aren't very savvy,



# What is the Internet?

- When people talk about the Internet, they often refer to it as a single entity as the “web” or the “cloud”
- In reality the Internet is a complex network of devices that communicate with one another to send your requests or data from point A to point B.



- With cloud computing your information may be hosted at sites all over the world instead of in a group of physical servers.
- Unfortunately, this means you never know where your email, attached files, or other data is being stored. While this might not seem an issue at face value, it is problematic when you realize that **some** countries have **less stringent data protection and privacy laws** than others.





- When you visit a site, data is transmitted between the client and server, allowing you to interact with others and/or access content like Web pages, code in pages that perform some function, online apps, file sharing, online games, and so on.





Some of the common online threats you might face in doing this include:

- Personal safety issues (e.g. cyberstalking, cyberbullying, online predators)
- Information security issues (e.g. phishing, identify theft, and scams)
- Computer threats (e.g. hackers, viruses, and other malicious software)
- Content issues (e.g. onbscene or offensive content)



- A 2012 survey found that 90% of consumers have had no training or classes on protecting their computer or information (WeLiveSecurity, 2012).



# What is a Cybercriminal

- A person who conducts some form of illegal activity using computers or other digital technology such as the Internet. The criminal may use computer expertise, knowledge of human behavior, and a variety of tools and services to achieve his or her goal.





- The kinds of crimes a cybercriminal may be involved in can include **hacking, identity theft, online scams and fraud, creating and disseminating malware, or attacks on computer systems and sites.**



# CyberStalking



- Cyberstalking is stalking or harassment carried out over the internet. It might target individuals, groups, or even organizations and can take different forms including slander, defamation and threats. Motives may be to control or intimidate the victim or to gather information for use in other crimes, like identity theft or offline stalking.



EDITION: AS



VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO HARDWARE MORE NEWSLETTERS ALL WRITERS

MUST READ: iPhone, iPad, Mac apps merging? Apple SDK will create iOS apps that work on Mac

# Infographic: 80% of robbers check Twitter, Facebook, Google Street View

Stats show that robbers check social networks to see if you're home.



By Boonsri Dickinson | November 1, 2011 -- 18:33 GMT (02:33 GMT+08:00) | Topic: Innovation



You might remember this incident from last year: Until they were caught, [three robbers in New Hampshire](#) checked Facebook status updates and managed to get away with \$200,000 worth of stolen goods after breaking into 50 homes.

## RECOMMENDED FOR YOU

EIU Report: Managing Application Development

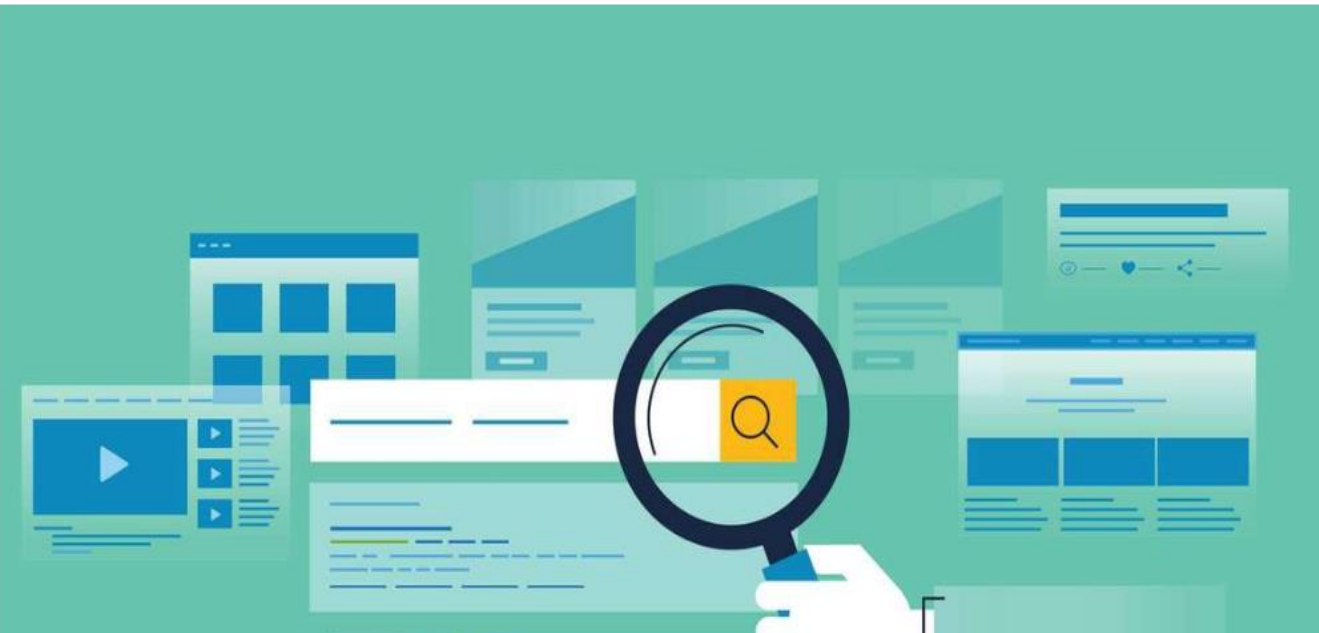
Resource Center provided by Google Cloud



# 70% of employers are snooping candidates' social media profiles

By Lauren Salm | June 15, 2017

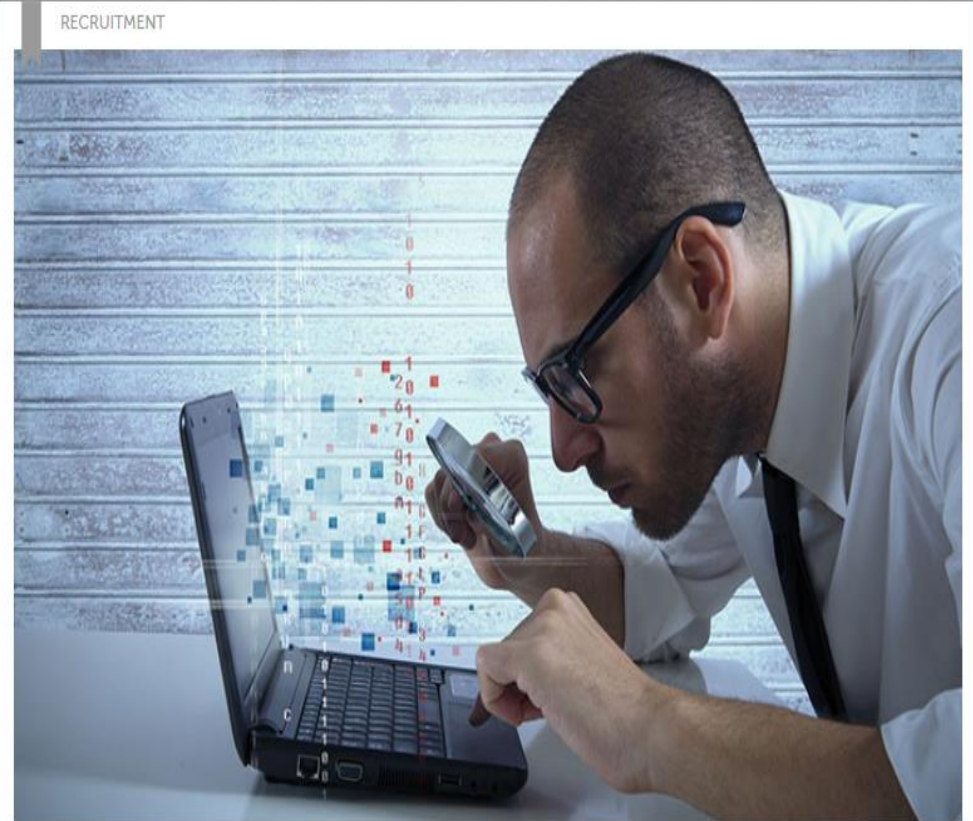
Share:   



## 1 In 10 Young Job Hunters Rejected Because Of Their Social Media

ERIK SHERMAN  
Jun 4th 2013 7:10AM

 SHARE  



19/06/2017 Mon 11:05 in All markets by Jerene Ang

## 11 reasons to reject a candidate based on social media

# Don't be too quick to accept a friend request



## Never Friend Strangers



# SPRINGFIELD NEWS-SUN



Support Local Journalism. **Subscribe today for 99¢.**

## Criminals use social media in choosing their victims

Community News | Updated Nov 07, 2011

By Katie Wedell, Staff Writer

Don't give your specific location or vacation information online



# IDENTITY THEFT

- The act of stealing a living or deceased person's identity, and using their information for the purposes of fraud. By impersonating another person, they can conceal their own identity, and use the information they have for personal gain
  - Credit card or bank / financial fraud
  - Telephone or utility fraud
  - Rent a house or apply for a mortgage
  - Obtain government documents
  - Provide identification in your name during arrest
  - Get medical services





NEWS

Filtered By: News

WATCH

# Guro, nabaon sa utang nang walang kamalay-malay dahil sa ID na ipinost niya sa FB

Published February 26, 2016 9:20pm

Isang guro ang nagkautang ng malaking halaga sa tatlong bangko matapos siyang mabiktima ng identity theft. Ang salarin, nakakuha ng mga impormasyon sa biktima dahil sa indentation card na ipinost nito sa Facebook.

# Public warned vs. con artist using name of PNP chief

By Christopher Lloyd Caliwan, Philippine News Agency on September 22, 2020



Using stolen identity data, the poser who was not identified, created a fake social network account with the name "Camilo P. Cascolan" on Facebook to further bolster his criminal misrepresentation and impersonation scheme. (File photo: Camilo Pancratius)

**MANILA** – The Philippine National Police (PNP) is going after a con artist posing on Facebook as its chief, Gen. Camilo Cascolan, and warned the public of a modus using his name.

PNP spokesperson Col. Ysmael Yu said the police zeroed-in on a cyber con artist who misrepresented Cascolan in an internet-based scam.

Using stolen identity data, the poser who was not identified, created a fake social network account with the name "Camilo P. Cascolan" on Facebook to further bolster his criminal misrepresentation and impersonation scheme.

Investigators of the PNP anti-cybercrime group (ACG) have identified the owner and creator of the fake account and have called the attention of Facebook over the fake account's violations, particularly to



# Fake emails on Netflix billing information are circulating in the Philippines, cyber security group warns

By Jeline Malasig - September 17, 2020 - 3:51 PM

[Share](#) [Facebook](#) [Twitter](#)

 [SEARCH](#)

  
**753,591**  
Fans

  
**202,572**  
Followers

## LATEST

The Apple Mask (yes, it exists!) looks neat, fits snugly and stays in shape

Your bank transfers via GCash will cost you a little bit by October

Julia Barretto praised for standing up to Jay Sonza via cybercrime rap

Missing flavors of Thailand? Celebrity chef

# How Game Apps That Captivate Kids Have Been Collecting Their Data

A lawsuit by New Mexico's attorney general accuses a popular app maker, as well as online ad businesses run by Google and Twitter, of violating children's privacy law.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, AARON KROLIK and MICHAEL H. KELLER SEPT. 12, 2018



- Biometrics
- Precise location of devices
- Internet Provider
- Hours spent on games etc.

# Cyberbullying



- is bullying that takes place over digital devices like cell phones, computers, and tablets.

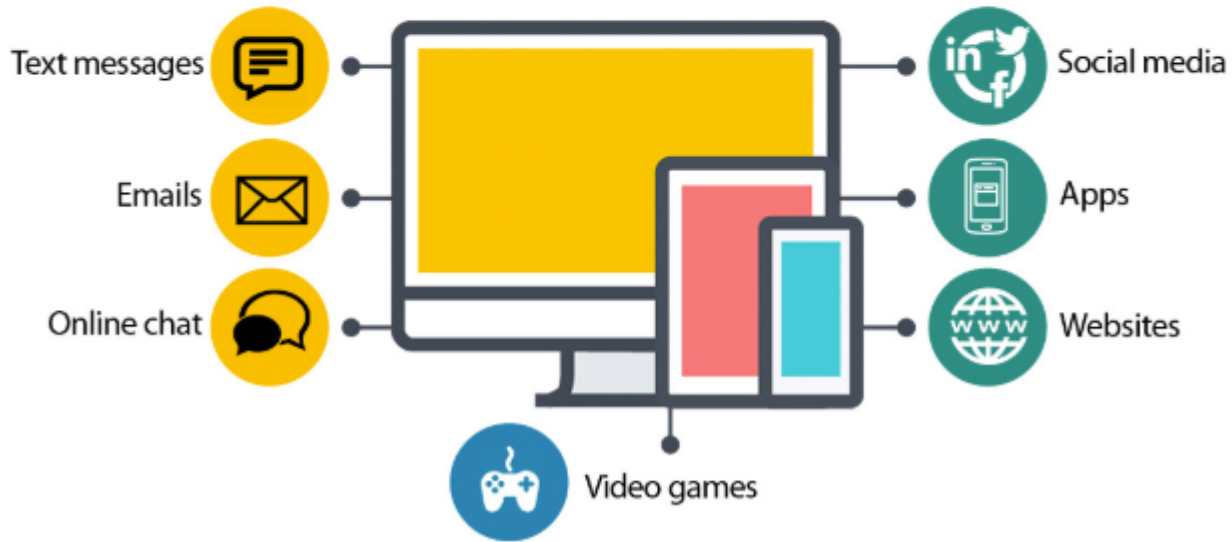




# Are you a Victim?

## WHAT IS CYBERBULLYING?

Rumors, embarrassing pictures, harassing messages and creating fake profiles sent through:



- Bullying is repetitious, unwanted, aggressive behavior that involves a real or a perceived power imbalance.
- Both kids who are bullied and those who bully may develop serious lasting problems.

# Microsoft study finds 4 in 10 consumers in Asia Pacific involved in bullying incidents

September 25, 2020 | Microsoft Asia News Center



### Related Posts

- [Microsoft Premonition in the global fight against disease outbreaks >](#)
- [Microsoft study finds 4 in 10 consumers in Asia Pacific involved in bullying incidents >](#)
- [Digital capability surges, helps keep 3.2 million Australians working through the pandemic >](#)
- [CEO Satya Nadella's virtual visit to Australia >](#)

## *Online bullying has real-world consequences. Think before you post*



**By Liz Thomas, Regional Digital Safety Lead, Microsoft Asia Pacific**

With COVID-19 necessitating remote work and learning, results from a new Microsoft study released in September 2020 remind us all to be mindful of how we treat others online.

[Research results](#) show that 38% of consumers in 32 countries around the world say they've been involved in a bullying incident as the target of the bullying, someone who displayed bullying behaviors, or as a bystander. This is experienced by 40% of teenagers and 37% adults.

Across Asia Pacific, a similar proportion of 41% consumers (teenagers and adults) have been involved in bullying. 22% of them said they were the target and 25% a bystander to the bullying.

Respondents were asked about both online and offline bullying, with adults also asked about "bullying", also known as "harassment", both inside and outside the workplace. One in seven adults in Asia Pacific (15%) also reported bullying occurring in their workplace. Workplace bullying is a particular challenge during the current pandemic, with separate Microsoft [research](#) on the future of work highlighting an increased blending of life and work.

### **Microsoft's digital civility research**

Conducted in April and May 2020, the study included a total of 32 geographies, with 4,511 people surveyed across nine countries in Asia Pacific (Australia, India, Indonesia, Malaysia, Philippines, Singapore, Taiwan, Thailand, and Vietnam). This research builds on similar studies about digital civility



- Bully-related suicide can be connected to any type of bullying, including physical bullying, emotional bullying, cyberbullying, and sexting, or circulating suggestive or nude photos or messages about a person.



(Getty/dragana991)

## Teen suicides rise in tandem with cyberbullying – and advocates have had enough

Families and legislators have banded together to fight a scourge that is harming and even killing teenagers

# Online Predators

- are individuals who commit child sexual abuse that begins or takes place on the Internet







PROFILE OF A PREDATOR

GROOMING

WARNING SIGNS

ADVICE TO PARENTS

YOUTH RISKY BEHAVIOR

REPORT CYBERCRIME

STATISTICS

SEX TRAFFICKING

TALKING TO YOUTH ABOUT SEX TRAFFICKING

HELPFUL PARENT'S GUIDES

ALICIA'S STORY OF KIDNAPPING, GROOMING AND SURVIVAL

PORNOGRAPHY 101

MOBILE & WIRELESS 101

## An Introduction

When children go online, they have direct and immediate access to friends, family, and complete strangers, which can put unsuspecting children at great risk. Children who meet and communicate with strangers online are easy prey for Internet predators. Predators have easy and anonymous access to children online where they can conceal their identity and roam without limit. Often, we have an image of sexual predators lurking around school playgrounds or hiding behind bushes scoping out their potential victims, but the reality is that today's sexual predators search for victims while hiding behind a computer screen, taking advantage of the anonymity the Internet offers.



View Alicia's Story



“One Australian study found roughly half of images shared on pedophile sites were taken from social media sites.”

Do you know where your child's | × +

→ × ⌂ nationalpost.com/news/canada/photos-shared-on-pedophile-sites-taken-from-parents-social-media-accounts ☆ ABP 1 📧 ⚙️ 🔍 🗑️

Apps 📁 Silliman-related 📁 HNV 📁 TBI GENERIC 📁 HEIRIT 📁 VSS 📁 PELS 📁 ICI 📁 IACS 📁 Jobs 📁 Researches 📁 Personal

**COVID-19**

Join the mailing list to receive daily email updates. [Subscribe Now>](#)

☰ Sections 🔍 Search **NATIONAL POST** [Subscribe](#)

[News / Canada](#)

# Do you know where your child's image is? Pedophiles sharing photos from parents' social media accounts

*'What you see as innocent, what a healthy, well person sees as innocent, someone with a sexual interest in children turns it into something incredibly perverse'*

Sharon Kirkey

Share

## TRENDING

1 **Lost apple found: 'Elusive' Colorado Orange apple, thought to be extinct, resurrected**

with Video

2 **Rex Murphy: The speech that changed nothing**

# TikTok Is A Pedophile Magnet And Unsafe For Kids, Warns Cyber Security Expert

*"TikTok also received the biggest fine in US history for gathering data on kids and selling it," revealed Susan McLean, former Victorian police cyber safety specialist.*





Through this three month probe, the outlet was able to gather hundreds of sexual comments posted on videos uploaded by teens and kids. Although the company was successful in deleting most of these unsavory comments, they failed to suspend the accounts of users who posted them in the first place, thus going directly against TikTok's own rules of sexual content directed at children. "TikTok does not have the same safety sessions as some of the more well-known apps and routinely do not remove accounts that have been flagged as potentially a predator," explained McLean.

Tik Tok has an absolutely massive pedophile problem and a big YouTuber needs to make a video to address it.

— Jason 🧑‍🎄 (@ItsNOSAJ) [30 September 2019](#)



ARTICLE

# Everyday pictures of children in a sexualised context

Like other hotlines, the Danish hotline also receives images of children which are not illegal but are problematic because they constitute sexual exploitation of the child. These may include everyday pictures of children being placed in an adult pornographic context, or pictures and films receiving sexual commentary. These images are not protected by law but are a violation of children's right not to be sexually exploited. In an article written on this topic, Save the Children Denmark explains the Copine scale, which describes images of children,



11.05.2020 - by Save the Children Denmark  
Photo by INHOPE, Save the Children Denmark, European Commission

# You don't need to be a computer expert to protect yourself.

- What you do need to do is use the tools and resources that experts have provided. There are a vast number of features, settings, hardware, and software available to prevent an attack, protect your privacy, enhance your security, and/or detect and remove anything affecting or infecting your system.



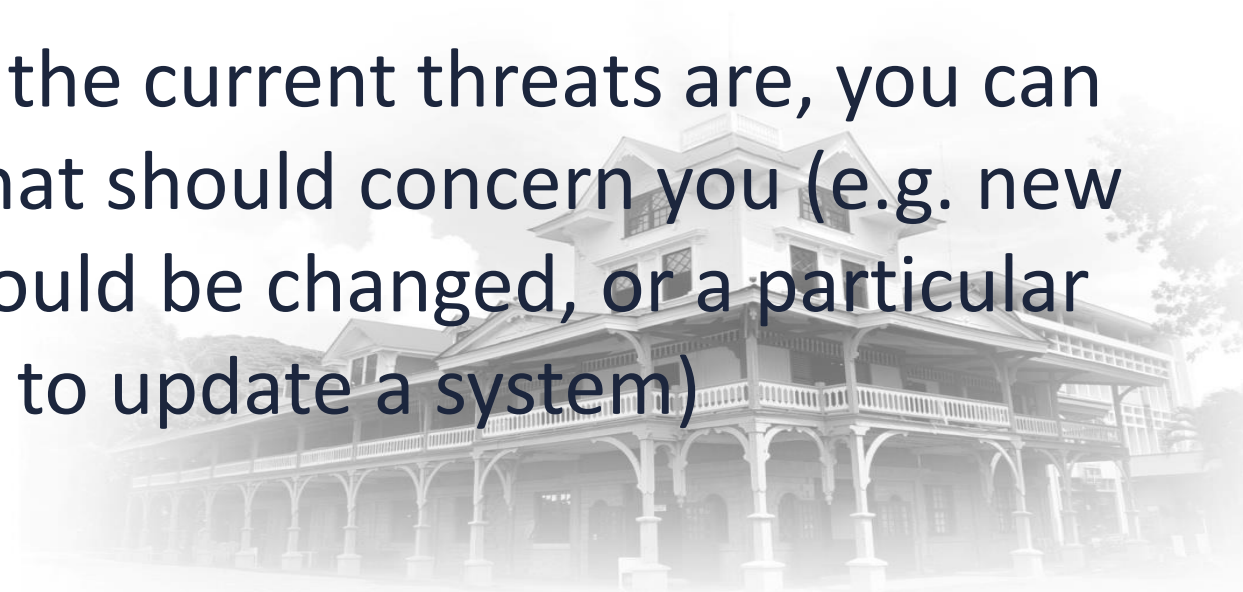
You don't need know everything about computers, but you should know what others have developed to protect you.





# Pay attention to what's out there

- stay aware of online threats, just as you might read a newspaper to see what crimes are being committed in your city and neighborhood
- By paying attention to what the current threats are, you can identify if there are issues that should concern you (e.g. new setting on Facebook that should be changed, or a particular vulnerability that needs you to update a system)



# Not All Information Is Valid



- While the Internet is a resource of incredible information, there's also a lot of garbage online
- If you see a story that's particularly humorous, horrifying, or unbelievable, try not to share it with others before doing a little investigation yourself.





# “Jackie Chan dead 2020” : Actor killed by internet death hoax

By Jessica Simpson | Hong Kong | Last updated on September 26, 2020

Translations Français Español Deutsch Italiano Português 中文

Tweet Share



Jackie Chan is the latest celeb to fall victim to a death hoax

JACKIE CHAN »

News of actor Jackie Chan’s death spread quickly earlier this week causing concern among fans across the world. However the September 2020 report has now been confirmed as a complete hoax and just the latest in a string of fake celebrity death reports. Thankfully, the actor best known for his roles in Shanghai Noon, Rush Hour or Police Story is alive and well.

UPDATE 26/09/2020 : This story seems to be false. (read more)

## Jackie Chan death hoax spreads on Facebook

Rumors of the actor’s alleged demise gained traction on Thursday after a ‘R.I.P. Jackie Chan’ Facebook page attracted nearly one million of ‘likes’. Those who read the ‘About’ page were given a believable



Share



# Julia Barretto files complaint against Jay Sonza over pregnancy rumor

**ABS-CBN News**

Posted at Sep 25 2020 01:13 PM | Updated as of Sep 25 2020 04:28 PM

MANILA -- **(UPDATED)** Actress Julia Barretto filed a cybercrime complaint against former broadcaster Jay Sonza at the National Bureau of Investigation (NBI) on Friday, September 25, after Sonza posted that the actress is pregnant with actor Gerald Anderson's child on his Facebook page last September 21.

Barretto, accompanied by her mother Marjorie Barretto, personally appeared before the NBI Cybercrime Division to ask the NBI to investigate the "untrue and irresponsible statements" made by Sonza on his social media account.

'When my car stops in certain area': Kim Chiu reflects on horrific van shooting

September 26, 2020

Sharea users, nag-share ng mga bagay na ipinagpapasalamat nila sa kabila ng pandemya

September 26, 2020

2 more Abu Sayyaf militants yield in Sulu, says military

September 26, 2020

First Gen employees hold 'hi-tech' tree-planting activity, raises funds for indigents in Batangas town

September 26, 2020

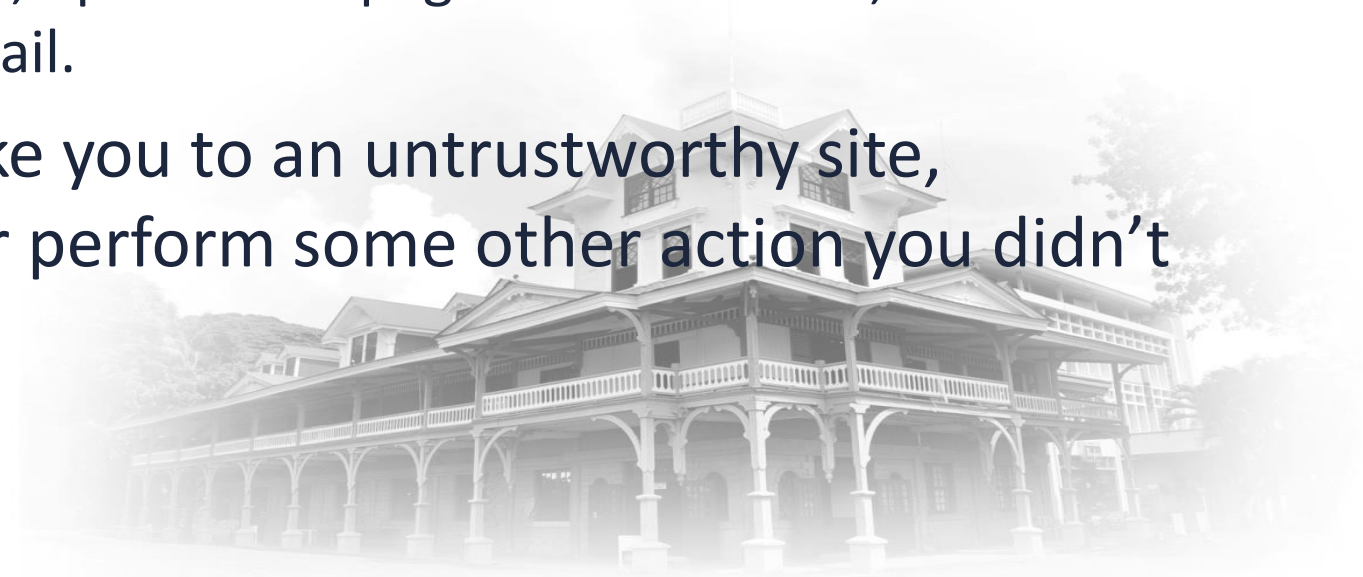
WHO: 2 million coronavirus deaths possible as Europe clamps down

September 26, 2020

iflix review: 'Bad Genius' series doesn't

# Think Before You Click

- A major risk when using the Internet can be the links that you click.
- A *hyperlink* or *link* is a section of text, image, or area of the page that's activated when you click or hover your mouse over it. Clicking the link may take you to another section of the Web page or document, open a new page or document, download a program or file, run code, or send email.
- Clicking it could just as easily take you to an untrustworthy site, download malware or a virus, or perform some other action you didn't expect.



- avoid clicking on pop-up ads or links that seem suspicious
- If an email seems to come from a phony source or has elements that seem dubious, don't click any links
- If you believe the link came from a known source, such as your bank or a store you shop at, go to the site directly with your browser rather than using the link
- inspect most links by hovering your mouse over it

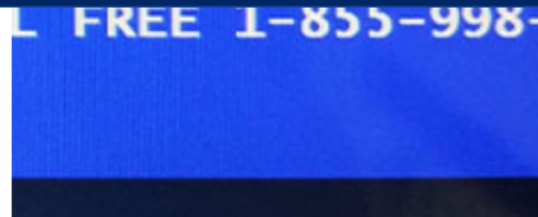




# Tech help scam: Don't click pop-ups warning your system is at risk

BY JAMES GELINAS, KOMANDO.COM • SEPTEMBER 9, 2020 SHARE: [Twitter] [Facebook] [Pinterest]

Picture this: You're browsing the web, minding your own business when suddenly a pop-up appears on your screen. It doesn't look like an ad, but a system alert warning you that a virus has taken over your machine. Wanting to protect yourself, you click the link and get in touch with a tech support agent. Then, before you



# Privacy

- When you visit a site, save a file, or provide information online, you should be secure in the knowledge that only you and authorized users have access to it. Unfortunately, that's not always the case.



# Online gaming may be used to get private information







# Video game companies are collecting massive amounts of data about you

By **ALEX BOUTILIER** Ottawa Bureau Reporter  
Tues., Dec. 29, 2015



OTTAWA—For many of us unwrapping new video game systems this holiday season, the “terms and conditions” will be a vague memory between taking the console out of the box and finally getting to play Fallout 4.

But with more and more video game companies collecting ever greater amounts of data about their customers, privacy advocates are starting to warn about risks to gamers’ personal privacy — as well as the dangers in normalizing surveillance.

# JOURNAL-NEWS

News Local Sports Entertainment Life Subscribers Only Classifieds | ePaper



41°



Log In

Support Local Journalism. **Subscribe today for 99¢.**

Woman believes social media post showing 'large amounts of money' led to home robbery



- When you use the Internet, you should take some time thinking about the level of privacy you expect from different sites, how the information you post online is used, and who can see where you go and what's stored. This will determine the settings you select, the sites you visit, and the browser, apps, and search engines you use.
- Terms of Use or Privacy Policy





- *Tracking cookies* may be stored on your computer as a means of monitoring the sites you visit
- Search engines may store information on your searches
- Online surveys may be used to get you to provide details about shopping habits, etc



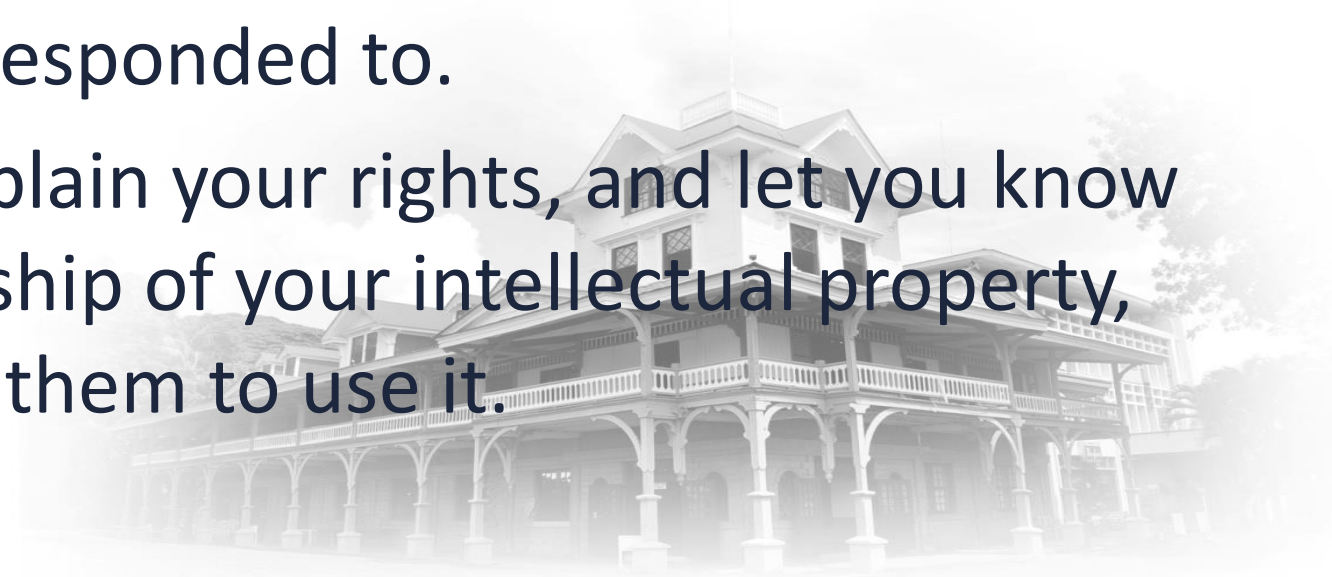
Often, some of the most personal bits of information are facts that we've posted about ourselves.

- Posting your date of birth, address, phone number, where you work or go to school, and other personal details online can expose your private life to strangers.
- The same applies to information in profiles, online resumes, and albums, which should be set so that only those you trust
- When using the Internet, the goal is to keep private information private



# Who has ownership?

- Just because you posted something, it doesn't mean it's necessarily yours.
- The reviews and feedback you give may become the property of the site or blog that you responded to.
- The Terms of Service will explain your rights, and let you know whether you retain ownership of your intellectual property, transfer it to them, or allow them to use it.





# Examples

## The New York Times



3.3 You acknowledge that any submissions you make to the Services (i.e., user-generated content including but not limited to: comments, forum messages, reviews, text, video, audio and photographs, as well as computer code and applications) (each, a "**Submission**") may be edited, removed, modified, published, transmitted, and displayed by NYT and you waive any rights you may have in having the material altered or changed in a manner not agreeable to you. Submissions made to the Services may also be included in our RSS feeds and APIs and made available for republishing through other formats.

3.4 You grant NYT a perpetual, nonexclusive, world-wide, royalty-free, sub-licensable license to the Submissions, which includes without limitation the right for NYT, or any third party it designates, to use, copy, transmit, excerpt, publish, distribute, publicly display, publicly perform, communicate to the public, create derivative works of, host, index, cache, tag, encode, modify and adapt (including without limitation the right to adapt to streaming, downloading, broadcast, mobile, digital, thumbnail, scanning or other technologies) in any form or media now known or hereinafter developed, any Submission posted by you on or to the Services or any other website owned by NYT, including any Submission posted on or to the Services through a third party.

We don't sell your personal data to advertisers, and we don't share information that directly identifies you (such as your name, email address or other contact information) with advertisers unless you give us specific permission. Instead, advertisers can tell us things like the kind of audience they want to see their ads, and we show those ads to people who may be interested. We provide advertisers with reports about the performance of their ads that help them understand how people are interacting with their content. See Section 2 below to learn more.

Our [Data Policy](#) explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described below. You can also go to your [settings](#) at any time to review the privacy choices you have about how we use your data.

# Where are your files stored?

- The location of your data plays a big part in your expectations of privacy
- While there are risks saving files to your local hard disk there are serious considerations when they're stored online, a corporate network, or devices owned by the people you've texted, emailed, or sent files to.





## GF NIYA, MAKAKALABOSO DAHIL KINALAT ANG PRIVATE VIDEO NG BF NIYA AT NG KARELASYON NITO!

Raffy Tulfo in Action ✓ 3.3M views • 6 months ago

PAALALA: Huwag maniniwala sa ano mang text o tawag na nagpapakilalang staff ng Raffy Tulfo in Action. Ang lahat ng reklamo ...



## PART 1 | PINAG MARIANG PALAD SIYA SA VIDEO CALL NG KANYANG GF SA FB AT IKINALAT SA SOCIAL MEDIA!

Raffy Tulfo in Action ✓ 4.4M views • 1 year ago

Para sa PART 2, puntahan ang link na ito: <https://youtu.be/m9lBNz3lxTY> Youtube:  
<http://bit.ly/1RaffyTulfoOfficialYoutube> ...





# Transformation

Fear your  
children will get  
in trouble online

Peace of mind  
they can guide  
themselves  
safely



# A common sight.

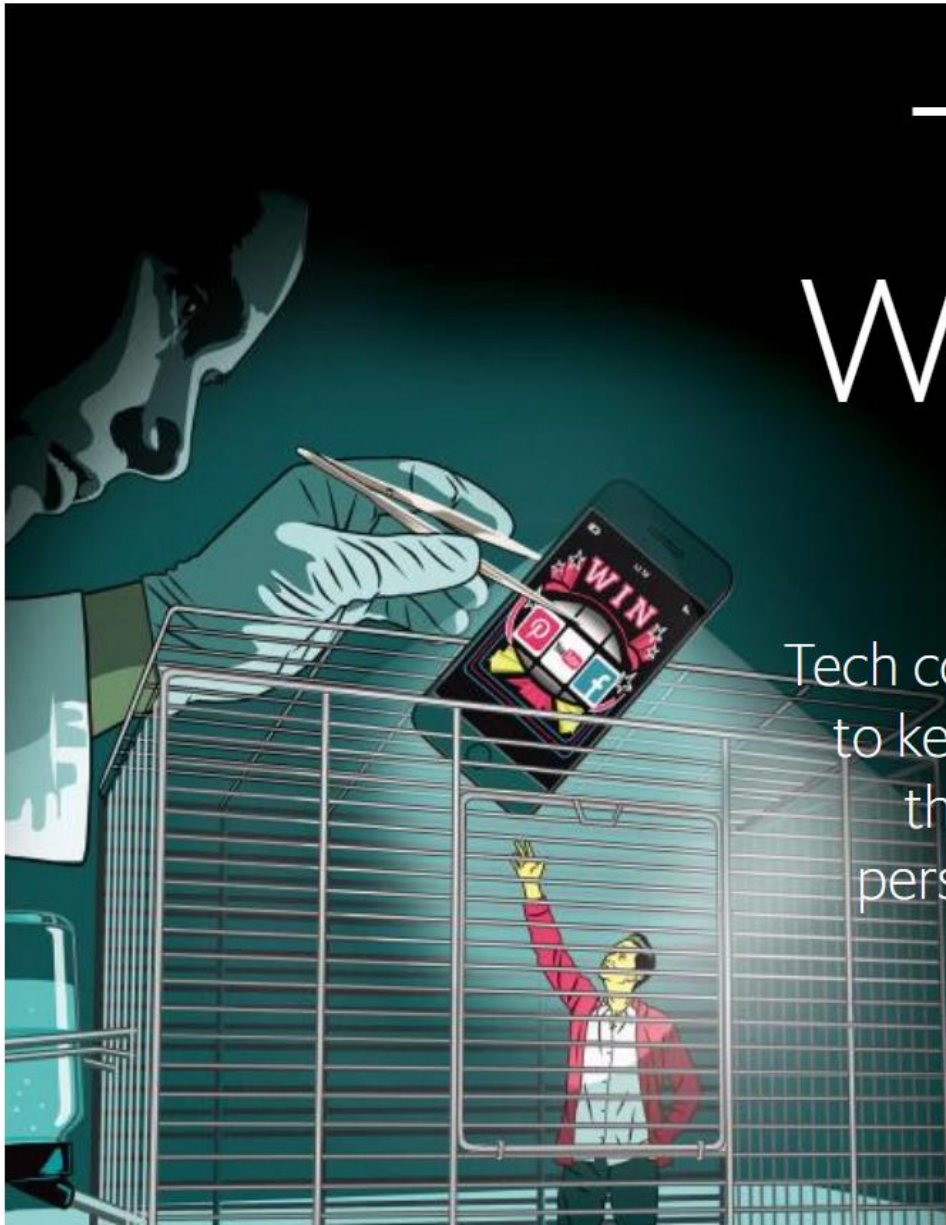




TECHNOLOGY

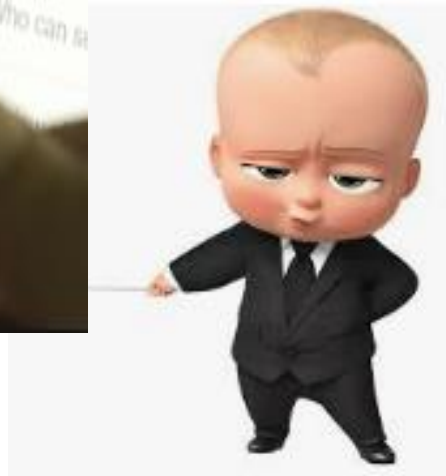
# THE SCIENTISTS WHO MAKE APPS ADDICTIVE

Tech companies use the insights of behaviour design to keep us returning to their products. But some of the psychologists who developed the science of persuasion are worried about how it is being used





# Use your Privacy Settings



# Social Media gives you the power to control

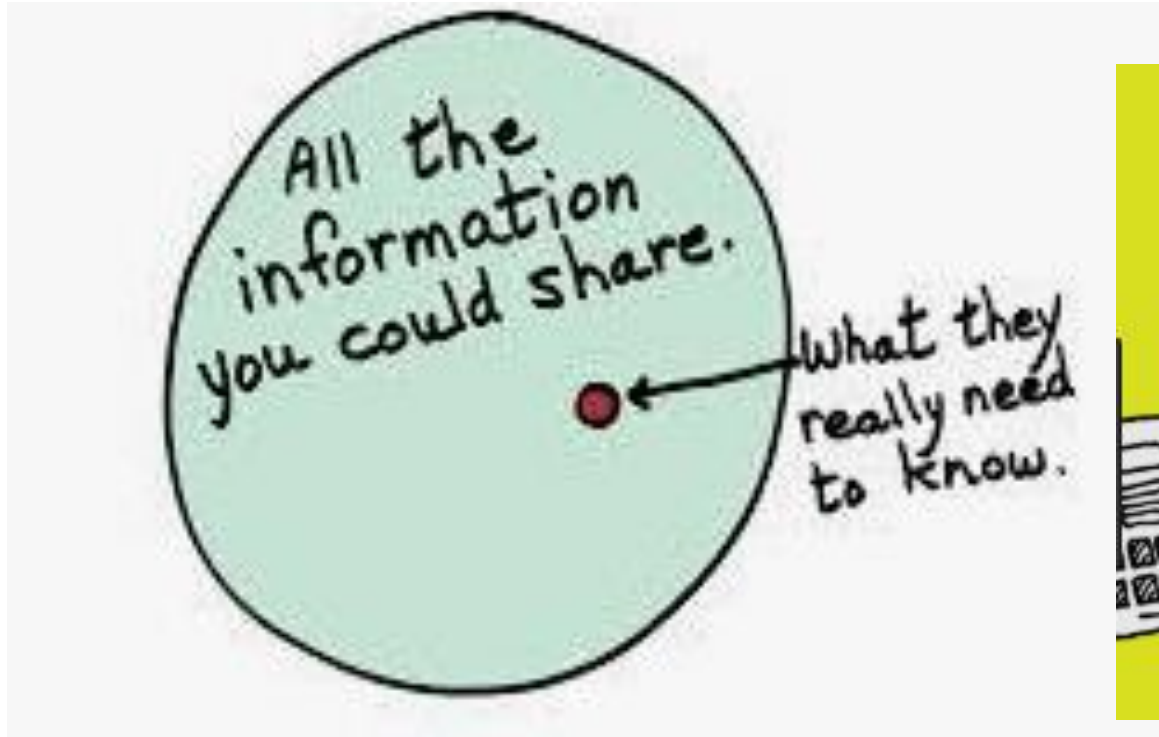
The screenshot shows the Facebook 'Privacy Settings and Tools' page for a user named Victor. The interface includes a search bar, navigation links for 'Home' (with a notification badge '2'), and icons for friends, messages, and a globe. The main content is organized into sections with various privacy controls and their current settings.

Section	Setting	Current Value	Action
Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		<a href="#">Limit Past Posts</a>
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit



# Be careful of what you post

Are you sharing too much?





# Don't post something that you will regret later

**NOT**  
EVERYBODY WILL  
 Like  
the things you  
**SHARE**  
**ONLINE**  
but everybody  
**WILL READ THEM**





# BEFORE YOU POST NITH

## THINK

- **T** – is it True?
- **H** – is it Helpful?
- **I** – is it Inspiring?
- **N** – is it Necessary?
- **K** – is it Kind?









Find a Therapist (City or Zip)



Gwendolyn Seidman Ph.D. Close Encounters



# Do Facebook "Likes" Affect Psychological Well-Being?

Self-esteem and sense of purpose may be key to understanding these reactions.

Posted Oct 20, 2016

f SHARE

TWEET

EMAIL

MORE



When you post a Facebook photo or update, do you feel good each time that notification bubble pops up and tells you that someone has liked your post? Do you feel

# Some things are not supposed to be shared

- Location
  - Home address
  - Birthday
  - Financial information
  - Boarding pass
  - SSS / GSIS number
- Be vigilant to what you are sharing online and become familiar with the consequences of such information sharing



# Create Strong Passwords

- Long and complex
- Practical but not personal
- Make it unique and fresh





# What they need:

- A trusted adult to talk with
- Online monitoring
- Safety education
- An advocate to intervene
- support



## 5 Tips for Staying Safe on Help Yourself



Always question why you are being asked for personal information, why it is needed and what it will be used for and if in doubt don't provide it

1



If you're uncertain about an organisation look for more information about them and their people

2



Keep your computer anti-virus software up to date and install software updates

3



Don't use public Wi-Fi to transfer sensitive information

4



If something sounds too good to be true it probably is - trust your instincts when accessing websites

5



# SETTING UP A DEVICE SAFELY FOR KIDS





# Some Apps & Devices To Monitor Your Kids Online Activity



Mobicip



Nischint



WatchOver



Netgear Parental Router



# When online, be ...

<h1>S</h1> <p><b>Stay Safe</b></p> <p>Don't give out your personal information to people / places you don't know.</p> 	<h1>M</h1> <p><b>Don't Meet Up</b></p> <p>Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.</p> 	<h1>A</h1> <p><b>Accepting Files</b></p> <p>Accepting emails, files, pictures or texts from people you don't know can cause problems.</p> 	<h1>R</h1> <p><b>Reliable?</b></p> <p>Check information before you believe it. Is the person or website telling the truth?</p> 	<h1>T</h1> <p><b>Tell Someone</b></p> <p>Tell an adult if someone or something makes you feel worried or uncomfortable.</p> <p>Follow these SMART tips to keep yourself safe online!</p> 
---	--	---	--	--



# References:

- <https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/>
- <https://en.wikipedia.org/wiki/Cyberstalking>
- <https://edu.gcfglobal.org/en/internetsafety/>
- <https://www.scribd.com/read/322093361/The-Basics-of-Cyber-Safety-Computer-and-Mobile-Device-Safety-Made-Easy#>
- <https://internetsafety101.org/internetpredators>





# Thank you so much.

