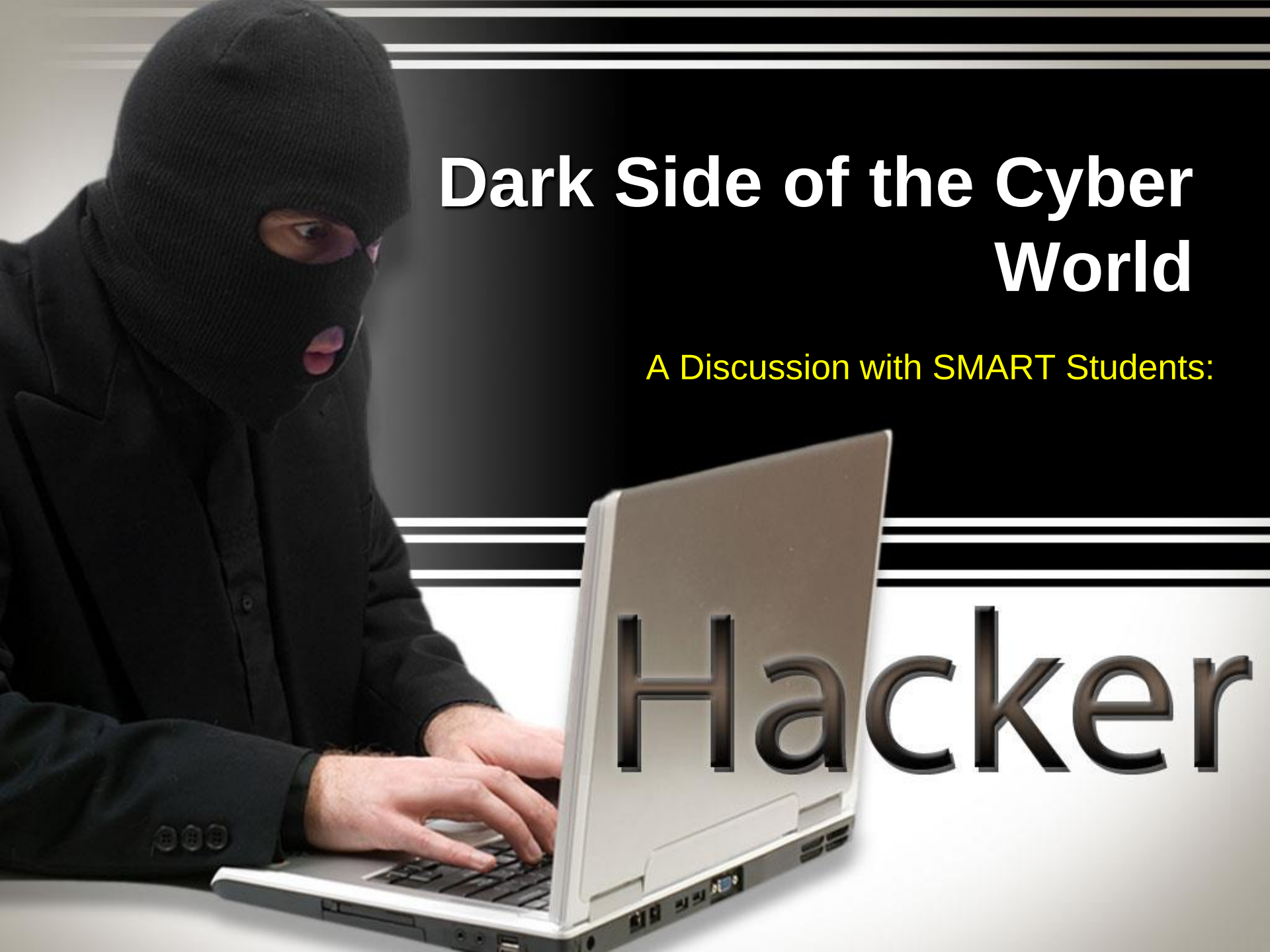
You Won!!!

“It is my great pleasure to inform that you have won the latest model of Ferrari Car and 4 Bed Room Villa in Palm Jumeirah for attending this Seminar…

To Process and deliver your Car and Villa please send your contact details, parents bank account number and a processing fee of 2000 AED to me urgently today……. “

Dark Side of the Cyber World

A Discussion with SMART Students:



Agenda

- Internet, Cyber, Trends..
- Children on Cyber World
- What are the Cyber Security risks
- What you can do to stop?
- How do you respond?
- Be a SMART Child on Cyber!

Key Words

- Cyber
- Cyber Crime
- Cyber Security

Some interesting Videos…

- http://www.youtube.com/v/EhV93zG8xlA
- http://www.youtube.com/v/9nEwX7BUYdY
- http://www.childnet.com/resources/digizen-game
- http://infosecawareness.in/cartoon-videos/identity-theft/
- http://infosecawareness.in/cartoon-videos/online-chatting/
- http://www.youtube.com/v/C8hkDfAMXYI

E-Children

- A recent Study reveals that Children (3-5 years) are more skilled at using smartphones/devices than tying their shoes
- It’s a birth right now!...
- Not any more …a Luxury!

The Danger!

- Like Outside world… there are bad people in Cyber World too (We are but Good, Right? ☺ …)
- Almost every activity what is happening in the real world is now online
- You may put yourself and your parents in danger, if doesn't’t use it properly…

Why More Safety/Security issues?

- All are using Internet or
- Are SMART now
  - Smart Phones
  - Smart Devices – IPAD, Galaxy TAB, etc…
- More activity on internet – friends, communication, buying, selling, and payments, etc.
- More Bad people migrating to Cyber – easy and hidden

How the Children can be at Risk?

- Content
- Contact
- Conduct

What is the Danger?

- Cyber Bullying
- Misusing the Children and that will spoil the future
- Financial losses to parents
- Private Data disclosed by children online, including family photos
- Downloading of viruses/worms etc.. That could even control the camera on your phone/laptop. !

Motivation for Cyber Crime

- Money
- Revenge
- Curiosity
- Fun
- Praise seekers

What are the Bad things?

- Phishing
- Internet Scams
- Malware (virus, worms etc.)
- Cyber stalking
- Cyber bullying
- Online Predation
- Inappropriate content

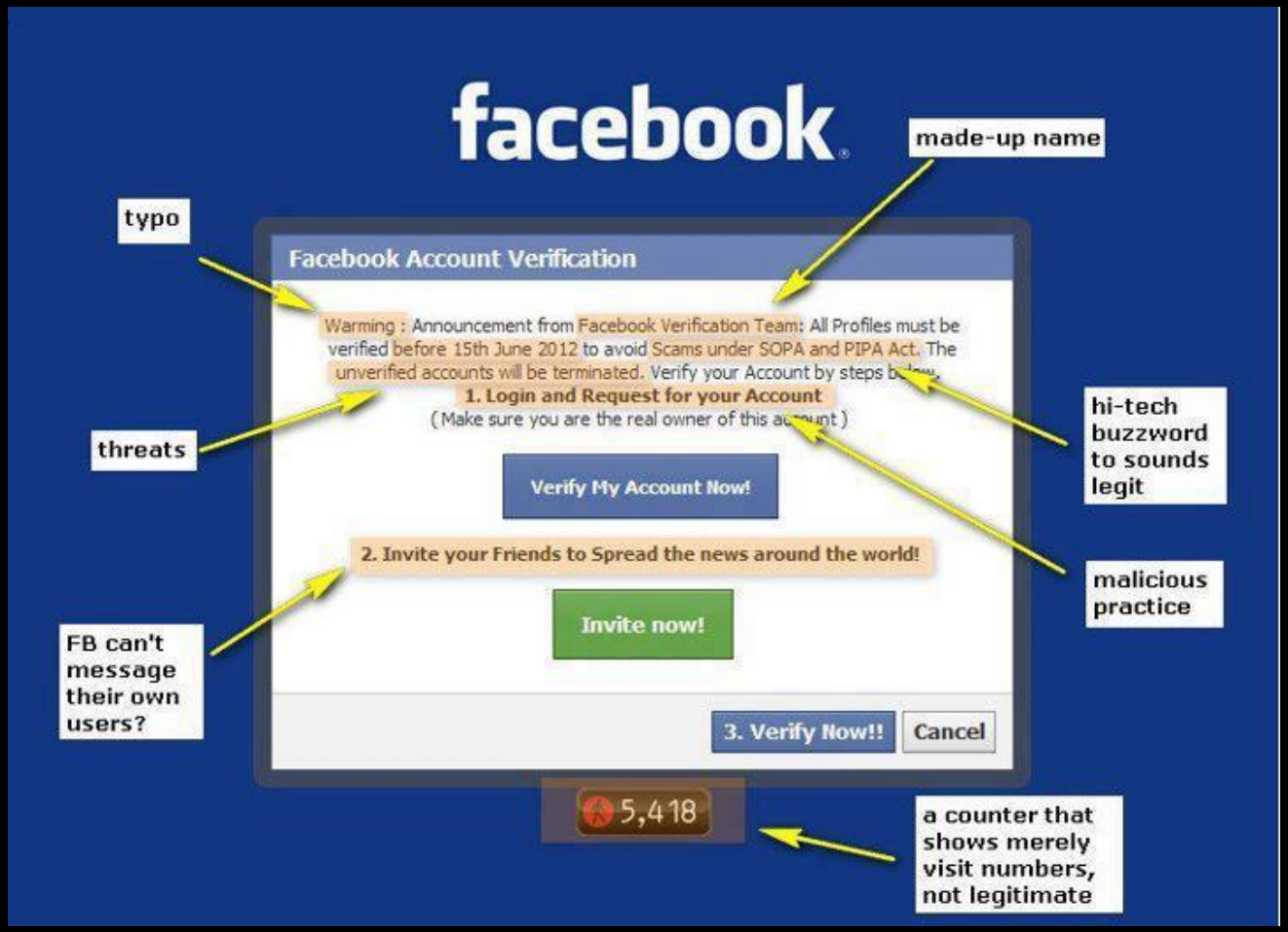
How do the bad guys work?

- Find kids through social networking, blogs, chat rooms, instant messaging, email, discussion boards, and other websites.
- Seduce their targets through attention, affection, kindness, and even gifts.
- Know the latest music and hobbies likely to interest kids.

How the Bad Guys Work?

- Listen to and sympathize with kids' problems.
- Try to ease young people's inhibitions by gradually introducing in appropriate content into their conversations or by showing them explicit material.
- Might also evaluate the kids they meet online for future face-to-face contact.

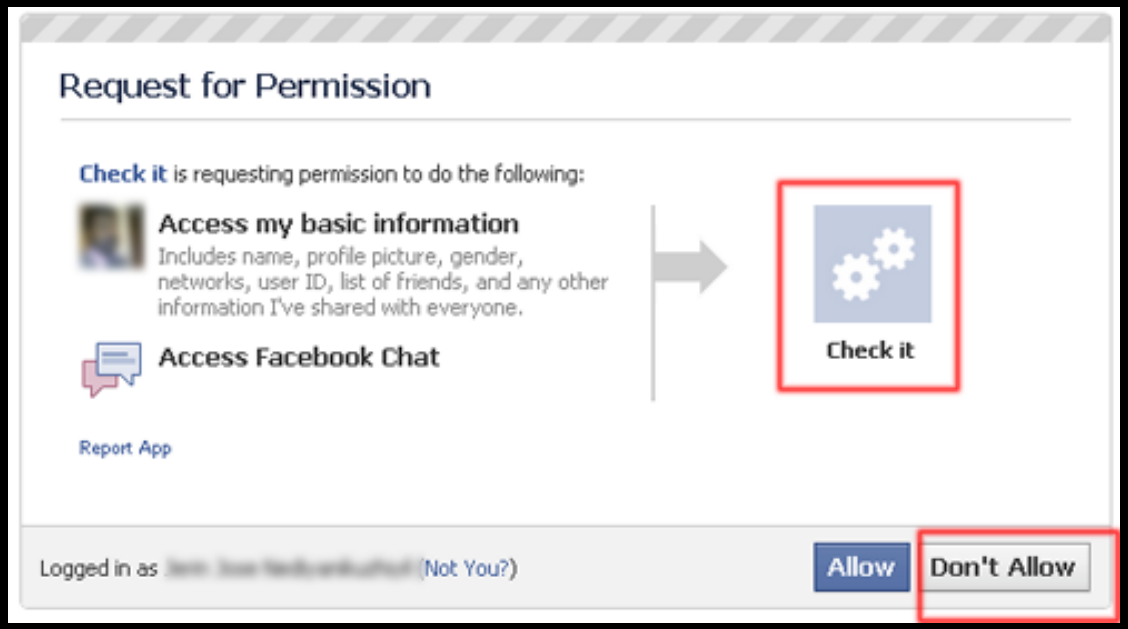
Suspicious Notices in FB or other social media




Hacker

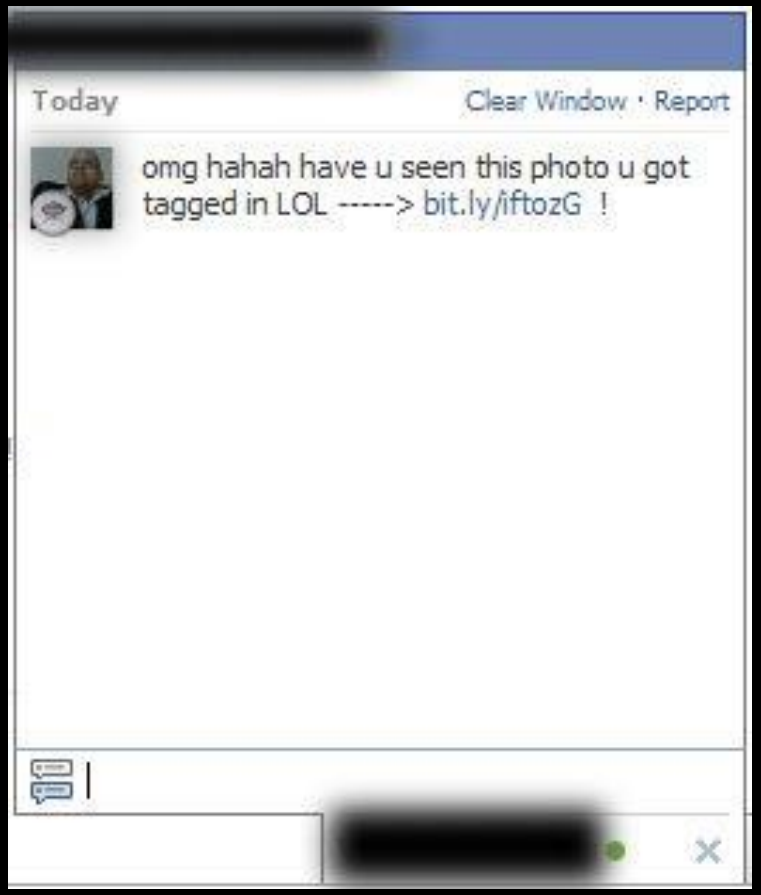
Suspicious!


Zul Asf
KNOW WHEN YOU LOOK AT MY PROFILE USING THIS: http://bit.ly/x0Fxfe
NEW! See who views your profile!
www.profileviews16738.com
Do you want to know who is looking at your photos right now? Find out who looks at your profile the most and what they look at!
Like · Comment · Share · Sunday at 10:29pm


Request for Permission
Check it is requesting permission to do the following:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.
Access Facebook Chat
Check it
Report App
Logged in as (Not You?)
Allow
Don't Allow


Hacker

Suspicious!!


Today
Clear Window · Report
omg hahah have u seen this photo u got tagged in LOL -----> bit.ly/iftozG !

How to be Safe?

- Don’t reveal personal or financial information in an email
- Before sending sensitive information over the Internet, Check the security of the web site
- Pay attention to the web site’s URL
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly and/or google about it.
- Keep a Clean machine

How can you protect yourself?

- Never download images from an unknown source-they could be not good to view by you and family and could get your PC or phone go bad.
- Using email filters.
- Telling an adult immediately if anything that happens online makes you feel uncomfortable or frightened.
- Choosing a gender-neutral screen name that doesn't contain suggestive words or reveal personal information.

How can you protect yourself?

- Never revealing personal information about yourselves (including age and gender) or information about your family to anyone online and not filling out online personal profiles.
- Stopping any email communication, instant messaging conversations, or chats if anyone starts to ask questions that are too personal or suspicious (abnormal)
- Have a family agreement on Internet use and post it near the computer to remind you to protect your privacy on the Internet.

Prevention

- Keep shared information to minimum
- Strong and easy to remember passwords
- Privacy settings on social media and games
- Security Software
- Avoid scams

Prevention

Some Quick Tips..

1) If you get a notice of a PHOTO TAG Do not open it....

2) If you get a notification that a friend reported you for offensive behavior etc.. Do not open it.

3) Is a Video saying 99% of People can not watch this for more the 15 Sec. Do not open it.

4) All Messages from your friends via chat saying click this link .. Do not open.

Only way to protect yourself from these is to ignore them and not to click on them.

Online Games Security

- Protect games with strong passwords
- Keep Personal information secret (no telephone number, location etc. to strangers)
- Make up a safe gamer name
- Play fair
- Never meet an online friend in person without safeguard in place (parent)
- No games above your age level
- Make sure your PC/device is always protected with Anti Virus and other security measures

Social Media

- Be Sensitive on what you upload
- Use privacy and security options provided, so that what you post is seen by whom you know only
- Keep your personal details personal

Tweeteee….

- There is no Delete when you tweet
- Never Post Sensitive Information
- Understand the Privacy Policies and Terms
- Posted Information is Permanent
- Verify your contacts
- Secure your Profile
- Practice Good password Management
- Limit the information you expose

Mobile Devices

- Keep security software current
- Protect all devices that connect to the Internet
- Secure your personal information
- Think before you app
- Only Give your mobile number out to people you know and trust
- Learn how to disable the geo-tagging on your phone at. http://icanstalku.com/how.php#disable

Smart Devices

- Do not Jail Break
- Connect only to authorized Wi Fi
- Use auto lock with password
- Download applications from authorized app stores only
- Use privacy options provided by various mobile OS
- Do not accept calls from weird number or Do not give call back.

What to Do?

- Connect with care
  - Get savvy about Wi Fi hotspots
  - Protect your $
  - When in doubt, don’t respond
- Be Web Wise
  - Stay current. Keep pace with new ways to stay safe online
  - Know how to cell block others
  - Use caution when meeting face-to-face

PCs / Laptops

- Install Anti Virus and up date
- Install Personal Firewall, if possible
- Keep the windows (OS) updated with the latest patch
- Avoid installing cracked software
- Keep OS files and Personal files in different HDD partition
- Factory default is good to do a local cleanup
- Factory restore may not wipe all the data, when you dispose or exchange/maintenance, but wiping need to use

Online Shopping

- Check out sellers
- Make sure the site is legitimate
- Protect your personal information
- Use safe payment options
- Keep a paper trail
- Turn your computer off when you are finished shopping
- Be wary of emails requesting information

How do you respond?

- If Somebody harass you online, hostile or sending disturbing materials – block them and report to your parents or friends
- Report improper game and content to the game service
- You may keep your parents in confidence – as they are the most interested in your safety and well being

What to do if you are victim?

- Report it to the appropriate people, including your parents
- If you believe financial accounts may be compromised contact your financial institution and close the account 9s).
- Watch for any unauthorized charges
- Consider reporting the attack to your local police
- When in doubt, throw it out
- Think before you act
- Secure your accounts
- Make passwords long and strong
- Unique account, unique password

Hacked Accounts

How do I know my email or social network account has been hacked?

- There are posts you never made on your social network page. These posts often encourage your friends to click on a link or download an App.
- A friend, family member or colleague reports getting email from you that you never sent
- Your information was lost via data breach, malware infection or lost/stolen device.

What to do if it is compromised?

- Notify all your contacts that they may receive spam messages that appear to come from your account.
- Your computer needs to be assessed and scanned for security risks and make sure all the security software are up to date
- Change passwords to all accounts that have been compromised and other key accounts asap.
- If you cannot access your account because a password has been changed

How to get Less SPAM

- Don’t Post Addresses Online (as much as)
- Avoid common, Guessable Formats
- Limit Sharing of Addresses
- Use Disposable Addresses
- No Email Based Screen Names
- Delete without Opening
- Disable Automatic Content Downloads

How to handle SPAM

- Don’t Forward Spam
- Never Reply or Click the Links
- Never Purchase anything from Spam
- Avoid Opting In
- Read Privacy Policies
- Use a Spam Filter
- Report Spam
- Keep Anti-Virus software updated

How can I find it is Genuine?

- Common Sense
- Too good to happen!

- http://www.hoax-slayer.com/site-search.html

- http://www.scamwatch.gov.au/

- http://www.419scam.org/

If nothing else works…

http://Google.com

Useful Utilities

- http://staysafeonline.org/stay-safe-online/free-security-check-ups/

Be a SMART Child

- **S**afe
- **M**eet
- **A**ccepting
- **R**eliable
- **T**ell

SMARTER

Top tips

- **Protect your online reputation:** use the services provided to manage your digital footprints and ‘think before you post.’ Content posted online can last forever and could be shared publicly by anyone.
- **Know where to find help**: understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it’s never too late to tell someone.
- **Don’t give in to pressure:** if you lose your inhibitions you've lost control; once you’ve pressed send you can’t take it back.
- **Respect the law:** use reliable services and know how to legally access the music, film and TV you want.
- **Acknowledge your sources:** use trustworthy content and remember to give credit when using others’ work/ideas.

Ethics

1. Acceptance
2. Sensitivity to nations and cultures
3. While Doing school work
4. While Using Email and Chatting
5. Pretending to be some one else
6. Use of Bad Language
7. Hide Personal Information
8. While Downloading

Quiz

- Which of the following tips can help you to look after yourself and look out for others when you are using social networks or instant messaging?

    a) Check your privacy settings
    b) Find out how to make an online report
    c) Always treat others with respect
    d) Tell a friend or family member if something upsets or concerns you

- How old do you have to be to have a Facebook account?
    a) 18
    b) 15
    c) 12
    d) 13
    e) There is no age limit
    f) Any age but with parent's permission

- Webcams can let you see and hear who you are chatting to in instant messaging services, but is it possible for this to be recorded?
    a) Yes
    b) No

Quiz

- Using illegal file-sharing program to download or stream content can cause some unwanted side-effects. Which of the following side-effects can happen as a result?

a) You download a computer virus
b) You get pop-ups that are difficult to get rid of Your computer gets slowed down significantly by a file you download
c) You download spyware which means strangers can access the information on your computer
d) You might be exposed to nasty images, such as very violent ones

Quiz

- Gaming can involve live online chat. What tips can help you stay safe when gaming online?

a) Keep gaming friends 'in the game' – don't share personal information with people you've met in games and don't share your social networking profile details or email address
b) Use a strong and unique password
c) Never play online games
d) Know how to report and block people
e) Remember to log out a service after you have finished using it

Quiz

- If you give out your mobile phone number online, which of the following are true?

a) You could start to receive texts from people you don’t know
b) You could be sent premium rate texts that cost you money
c) Your phone number could be used to locate where you are
d) You could start to receive promotional texts for things you don’t want

Quiz

- Which of these can add costs to your mobile bill?

a) Upgrading a free app
b) Dialing an 09 number to vote on a TV show
c) Receiving questions or answers from a quiz service by text
d) Dialing 999 in an emergency

Summary

- Be SMART Child in SMART way
- Use the facilities wisely and securely
- Ensure that you keep your parents in Confidence
- Don’t trust strangers
- Don’t trust unexpected emails, messages, communication
- Don’t believe without validating
- Don’t believe in “too good to be true”