Keeping our Kids & Parents Safe in a Digital World

Karen Fedyszyn

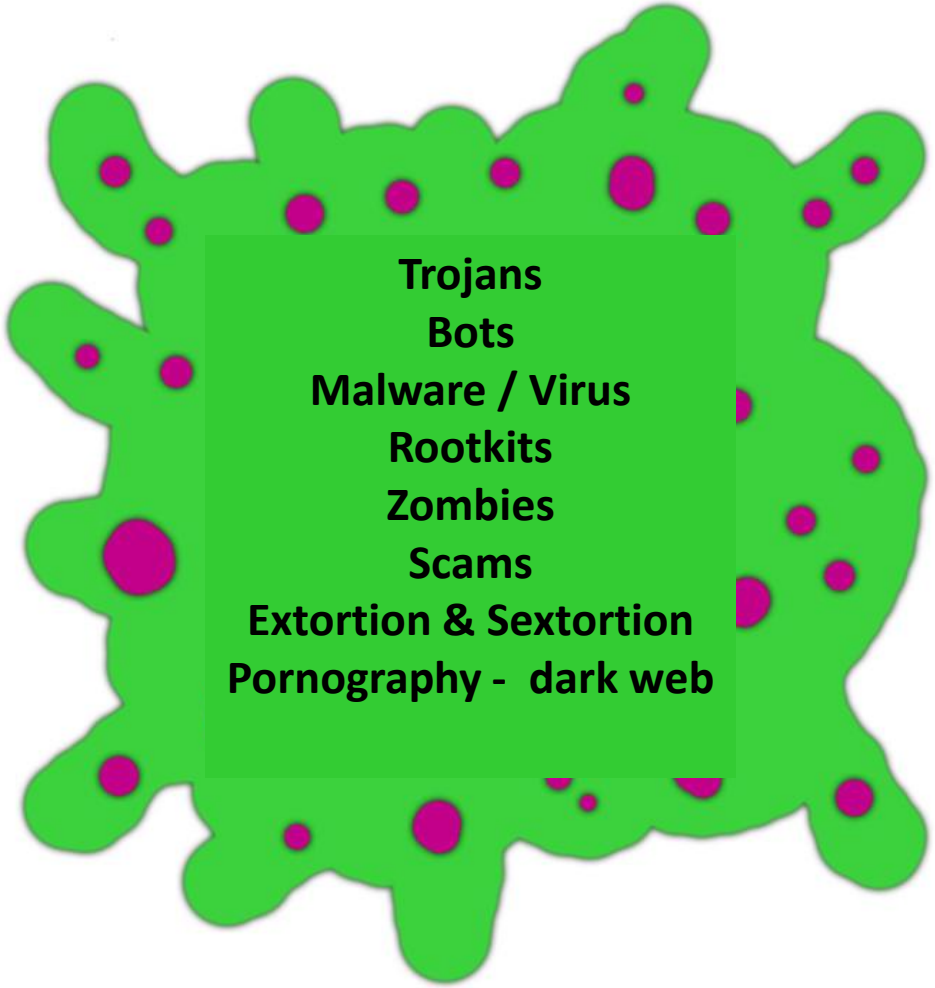
May 2020

Overview:

- Importance of Digital Protection
  - Establishing a cooperative approach with Kids – contract, monitoring, time out
  - Establishing a supportive approach with parents – knowledge, coaching, back up
- Self protection
  - Passwords
  - Identity
  - Profiles
  - Cameras – Computer, Security devices…
  - Listening systems – Alexa, Siri…
  - Streaming
  - personal reveal
- Social Media
- Home protection – your networks, firewalls, black list, passwords, voice systems
- Public protection – usb ports, set up a hotspot, use vpn
- Advanced monitoring
- Setting a good example

Why is Digital Protection So Important?

- Children faces many dangers online:
  - Cyberbullying – 33% of kids on social media have experienced
  - Cyberpredators – social media & gaming alike
- Seniors are of big concern:
  - They have a nest egg
  - Prey on honesty (police, fire dept) and / or fear (IRS, INS)
- Biggest concerns:
  - Publishing regrettable posts
  - Posting private information
  - Phishing & Smishing
  - Falling for scams
  - Downloading malware
  - Becoming a victim



A Cooperative & Supportive Approach

- Need to have open & honest conversations
  - Come to me with any issue, I will not judge, I am here to help & protect you
  - Explain the types of risk that are out there (predators, extortionists)
- Know the systems & apps being used
  - Familiarize yourself with user accounts & privacy setups
  - Talk to them about why they need to select certain settings
- For Kids:
  - Mobile device contract
  - Make sure they understand the reason for any monitoring tools
  - Establish rules & any “reviews” early on
- Talk about the need to keep things confidential & private to protect them
  - Don’t publish your kids names on your own accounts until they are teens

Self Protection - Accounts, Passwords & Recovery:

- Don’t use actual names
- Separate professional & personal accounts
- Complex passwords are important
  - Come up with shorthand
  - Don’t use the same passwords ☹
  - Treat anything with $$ extra special
  - Face recognition is not right for everything
- Be thoughtful of how you establish recovery
  - Separate the key master and the gate keeper
  - Don’t tell friends or care givers access information

If you have to use words, be creative:

a = @

e = 3

i = 1 or |

o = 0

u = >

S = $

B = &

K = %

P = 9

Self Protection – Profiles, Personal Reveal, Identities:

- What platforms do they use for what purpose?
- No revealing personal data or names
- Be familiar with their profiles & settings
  - Personalities – because it's not just reality
  - Separate personal profiles from any business or celebrity pursuits
- Discuss rules for accepting followers / friends
  - No strangers
  - Friend of friend only those you know
  - Conflicts with growing a huge following
  - Review friends & connections regularly
- Private messages - never responding to strangers
- Don't use location services
  - Not even on pictures – geolocation identification
- Don't do online polls!

Self Protection – Connections, Friends, & Follows:

- Open connecting should be restricted to adults
  - Tweens – limited to friends
  - Teens – expanded network
  - Seniors? – Keep them from contacting the government
- Private vs Public profiles – depends on platform
- Make sure your children understand cyberbullying
  - Connecting with the wrong people can cause depression & anxiety
  - Anything we say can come back to us later
- Stalkers
- Never respond to messages from strangers
- Parents should follow and friend every account for their children

Self Protection – Cameras, Streaming, IoT:

- Cameras should be blocked when not in use
  - Extra level of protection if anyone has gained access to the device
  - Youngest children should never use them
- You should approve any videos or streaming
  - Done in the open
  - Not behind bedroom door
- IoT – Internet of Things
  - Strong passwords on all wifis
  - Cameras and home services on separate wifi
  - Turn on warning messages for anything connecting to your network

And if we have the time….

SOCIAL MEDIA!!!

Social Media – Instagram:

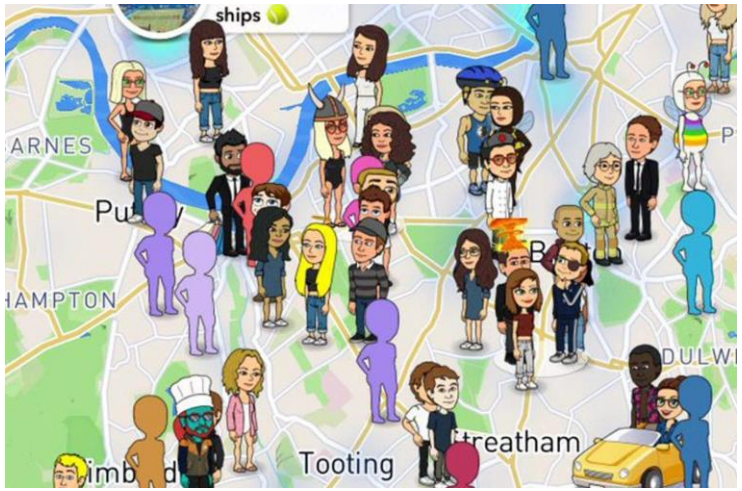
- Just passed 1 Billion users
- 13 Year old requirement
- Average age of users is 25-34
- Security features
  - 2 factor authentication – use it across 2 devices
  - Set account to Private
  - Actively block accounts
  - Restrict who can comment
  - Set activity status to off
  - With posts – do not add location
  - No geolocation data on photos! This is huge!
- Don’t tag themselves

Social Media – Facebook:

- Let’s face it, the kids aren’t here
- But what we publish about them can shine a light on them
  - Adorable pictures
  - Their names
  - School details
  - Events
  - Friends
  - It’s very easy to do these things
- Automatically publishing to multiple platforms (Insta, Twitter…) can now overlap with platforms they use and link them to your social media presence
- Be picky about who you connect with
- Review your connections – do you know them?

Social Media – SnapChat:

- Teenage platform de Jour
- Photos are only seen by intended recipient for a few seconds
  - The mistake most make is thinking these are gone forever, they are not
  - Teach your kids to take a pause before they publish anything
    - Can someone be hurt by this?
    - Would someone misunderstand this?
    - Could this hurt me in the future (college application)?
  - Sexting is a common problem – understand what sextortion means
  - But the viewer can screen shot the photo, so there's no control
- Snap Map is dangerous
  - Enable "Ghost Mode"
- Creates a very personal experience with chosen friends
  - Mostly teens



Social Media – Twitter:

- Kids use it to keep up on news and celebrities
- Most kids are set to public tweets
  - They need to be aware that something can spread far and fast
  - Never comment in the heat of the moment
- It’s a very negative place
  - Lots of hostility being posted
  - Very overwhelming
  - Not safe for kids
  - Could end up with poor self image issues if something goes wrong

Social Media – TikTok:

- Acquired Musical.ly in 2018
- The very goal is to connect with strangers and build followers
- 13 Year old minimum
- Up to 60 second video
  - Add soundtracking & filtering
  - There is no filtering by age groups
  - TikTok does take down offensive videos regularly that violate the guidelines
- 60 million US users (800 million world wide) and growing fast
- Owned and operated by a Chinese company
- It’s made some unknown people very famous, very fast
  - There are risks to this
- No self reveals – can be used to find you, your parents, etc.

Social Media – WhatsApp:

- Originally created with small business owners in mind
- Used by 1B people in 180 countries
- Often used to keep in touch with friends and family internationally, not needed within US communications
- Users send text messages, audio messages, videos, and photos
  - to one or many people
  - no message limits or fees
- 16 and older
- Free platform, significantly cheaper than text messages
- Can also be accessed via your computer

Social Media – Discord:

- Originally used by gamers for chat
- use text, voice-chat, and video-chat
- Discussion groups are “public” and “private” servers
- Only join private groups where you know the people IRL!
- Use groups that are moderated only
- Lots of dangers of cyberbullying
- Sit and listen while your child is using this so you understand the types of conversations they engage in
- Used extensively in gaming groups and very hard to monitor

Social Media - YouTube:

- It’s the new TV
- For younger kids, log them into your account
- Viewer or Producer?
- Know who they follow
- Receive system emails to your account
- Review browsing history
- Talk to them about what they see, what interests them?
- Use “Restricted Mode: On” – hides videos flagged as inappropriate
  - Use parent account to control child settings

Social Media - Apps to be Concerned About:

- Whisper – a place to tell secrets
- YikYak – anonymous postings
- Kik – text with pictures, no log
- Snapchat – not appropriate for younger users
- WhatsApp – unrestricted global access, but fine when used correctly
- GroupMe – group chats
- Chatous – matches strangers
- Oovoo – free messaging and video
- TikTok, Live.Me, Bigo – Video creation, some risky stuff
- Down, Badoo, Tinder, Grindr – Dating & Hookups – without filters this can be alarming!
- Vaults – Photo, Secret Calculator
- Hot or Not – stranger meet up
- Down – strangers near by
- Games – Fortnite, Minecraft – issue exists only with their open communication channels

Home & Montoring….

Internet – At Home Setup:

- Separate login per person
- Secure your wifi
- Required administrator approval for changes and new installations
- Keep software patched & antivirus current
- Update Operating Systems in a timely fashion
- Kid specific:
  - Family computers in common areas
  - Screen Time Limits
  - Kid safe browsers:
    - Zoodles
    - Maxthon
    - Chrome with “supervised profile” enabled
    - Restrict unlimited internet access
  - Talk to your children about what to do if they find themselves uncomfortable

Advanced Monitoring:

- Everyone should use “find my phone”
  - Great for lost devices
  - Quick visual when you can’t reach them
  - GPS locator is not always accurate
- Life 360 is great for families
  - Protect and keep connected
  - Set perimeters and alerts
- Bark
  - Customize the way you want to handle filtering, alerts
  - Set specific words for alerts
  - Daily blog reviewing issues & concerns
- Make sure your family member knows they are being monitored so this doesn’t impact their trust

Setting a Good Example:

- Don’t post while you are on vacation
  - Someone could be tracking you or your kids
  - Makes you at risk for robbery
- Make thoughtful social media posts, don’t be a loose cannon
- Don’t refer to your children by name online
  - Be thoughtful of the pictures you post
  - Keep your child’s information confidential
- Don’t do online polls – you can give very personal information very innocently
- Keep our professional and personal profiles separate
  - You don’t need strangers knowing too much about your kids
  - Restrict your personal privacy to friend of a friend
- Spend time with your child online, friend & follow them

What's Next?:

- Questions?

- Karen.Fedyszyn@fortiumpartners.com