

Safer Social Networking

Ilene Klein, CISSP, CISM, CIPP/US
November 2013

Information Security and Privacy Office

City of Phoenix



Agenda

- Social networking risks
 - Things you can't control
 - Malware, privacy policies
 - Things you can control
 - TMI and over sharing
 - Reputation and lifestyle, personal safety, burglary risk

- Protection strategies



Pop Quiz

- Why do bad guys attack social networking sites, like Facebook and Twitter?





Pop Quiz

- Why do bad guys attack social networking sites?
- That's where the people are!
 - Facebook: 1.15 billion users
 - Twitter: 500 million total users
 - LinkedIn: 238 million users
 - Instagram: 130 million users
 - Pinterest: 70 million users
 - Snapchat: 5 million





Pop Quiz

- What do bad guys want?





What Do Bad Guys Want?

- Money
 - From ID theft / fraud
 - From sending spam
 - From selling ads or info about you to marketers





What Do Bad Guys Need?

- For ID theft / fraud
 - Your personal info
 - Your account credentials
 - Your money (by tricking you into giving)

- For sending spam
 - Your email account / credentials
 - Control of your PC

- For ads and marketing
 - Info about you – demographics, likes, hobbies, friends, location



How Do Bad Guys Get It?

- Your personal info and/or account credentials
 - Phishing scams
 - We lost your password, please give it to us
 - Keystroke loggers
 - Hack attack / password crack / password guess
- Control of your PC
 - Virus / worm / malware
- Your money
 - Scam
 - I'm stuck in Canada, please wire money
 - I'm a Nigerian prince, help me get money out of my country
 - I've encrypted your computer, wire me money
- Info about you
 - Spyware
 - Info you provide (posts, mail lists, location)
 - Info collected (sites visited, items purchased)



Common Social Media Scams

- Free giveaways, like for a new iPhone
 - But you have to give up personal info or download a program/app
 - Goal: ID theft or infect your device
- Viral videos
 - But you have to install a new video player
 - Goal: infect your device
- Keep current on Facebook scams, check out ***facecrooks.com***



Anatomy of a Pinterest Scam

- Bad guys create an ad for a freebie and post it all over Pinterest
- You click on the link
 - You're asked to re-pin the photo (and spread the scam)
 - You must enter personal details or sign up for a service

- Don't fall for too-good-to-be-true offers
- Don't blindly trust requests for personal info
- Be wary of "fun" surveys
 - They're often gathering info about you to sell to marketers or to guess your passwords





Twitter Hack – February 2013

“We detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users.”

- **Lessons:**
 - Use long, strong passwords – at least 10 mixed characters
 - Use different passwords for different things
 - Banking, social media, email, work...



How Are Social Nets Using Your Info?





Privacy Policies and Terms of Use

- Sites must post their privacy policy and terms of service
- In privacy policies, look for
 - What information about you is collected
 - How is it used
 - With whom is it shared
- In terms of service, look for
 - Conditions for using site / app / software
 - Ownership of any content you post / submit
- FYI... Researchers say Google's latest terms and conditions are more difficult to understand than Anglo-Saxon saga Beowulf



Quiz: Would you use this IM service?

From an instant messaging site

Terms of Use / Privacy Policy:

[...] By using our service/website you hereby fully authorize [redux] to send messages of a commercial nature via Instant Messages and E-Mails on behalf of third parties via the information you provide U.S.. This is not a "phishing" site that attempts to "trick" you into revealing personal information. Everything we do with your information is disclosed here. If you are under eighteen (18), you MUST obtain permission from a parent or guardian before using our website/service.

[...] We may temporarily access your [IM] account to do a combination of the following:

1. Send Instant Messages to your friends promoting this site.
2. Introduce new entertaining sites to your friends via Instant Messages.



Too Many Permissions

- Samsung and Jay-Z created an app that lets users hear Magna Carta Holy Grail three days before its release
- App wants the following permissions
 - To modify and delete contents stored on your phone
 - To prevent the phone from sleeping
 - To view a list of all running apps and accounts set up on the phone
 - For your location, via the GPS
 - For full network access
 - To see who you're talking to on the phone
 - To run at startup and to test access to protected storage
 - To control the phone's vibration
- The app sends/posts to your contacts every time you listen to a song
 - You must log into your Twitter or Facebook account before listening



Facebook Privacy Policy – Ilene's Personal *Opinions*

- Facebook's privacy policies are confusing
 - But better than they used to be
- Facebook shares info about you with its partners
- Facebook has gotten into trouble over its privacy policies
- **You cannot control privacy policies – but you can control what info you provide**
 - Just consider everything you post available to the world

Data Use Policy

Date of Last Revision: December 11, 2012

Information we receive and how it is used

- Information we receive about you
- Public information
- Usernames and User IDs
- How we use the information we receive
- Deleting and deactivating your account

Sharing and finding you on Facebook

- Control each time you post
- Control over your timeline
- Finding you on Facebook
- Access on phones and other devices
- Activity log
- What your friends and others share about you
- Groups
- Pages

Other websites and applications

- About Facebook Platform
- Controlling what information you share with applications
- Controlling what is shared when the people you share with use applications
- Logging in to another site using Facebook
- About social plugins
- About instant personalization
- Public search engines

How advertising and Sponsored Stories work

- Personalized ads
- Ads + social context
- Sponsored stories
- Facebook content

Cookies, pixels and other similar technologies
Some other things you need to know



Facebook Can Use You in Ads

- Facebook says that it can freely use a your name, photo, comments, and other information in ads
 - As long as it shows the ad only to people who already have rights to see the underlying information
- Example: if you compliment Starbucks' pumpkin spice latte in a post that can be viewed by your Facebook friends, the coffee company can pay Facebook to broadcast that comment to all of your friends to improve the chances that they see it
 - Called a sponsored story
 - It's valuable to advertisers because it looks like a product endorsement from a trusted friend rather than a traditional ad



More Recent Facebook Privacy Policy Changes

- People can search for any existing users on Facebook, including those who had disabled this search option in their Facebook privacy settings
 - “Your name, gender, username, user ID (account number), profile picture, cover photo and networks (if you choose to add these) are available to anyone since they are essential to helping you connect with your friends and family”
- Teenagers can post status updates, videos and images that can be seen by anyone, not just their friends or people who know their friends
- By default, new accounts for teenagers will be set up to share information only with friends, not friends of friends as before (good!)



Facebook Privacy

- Wall Street Journal has a good article describing Facebook privacy settings
 - <http://online.wsj.com/article/SB10001424127887324880504578300312528424302.html>
- Instructions for locking down your Facebook privacy settings
 - <http://facecrooks.com/Internet-Safety-Privacy/how-to-lockdown-your-facebook-account-for-maximum-privacy-and-security.html>
 - <http://gizmodo.com/5986399/how-to-lock-down-your-facebook-privacy-before-graph-search-strikes>
 - http://www.csoonline.com/slideshow/detail/123265/Six-steps-to-better-Facebook-privacy-management?source=CSONLE_nlt_update_2013-10-13



Facebook “Likes” Reveal More than You Think

- 2013: Cambridge University analyzed “likes” of more than 58,000 Facebook users (study volunteers)
- They were able to “automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private”
 - Race (African Americans vs. Caucasians), 95% of cases
 - Gender, 93% of cases
 - Sexual orientation for males (88%) and females (75%)
 - Political party (Democrat vs. Republican), 85% of cases
 - Religion (Christian vs. Muslim), 82% of cases
 - Substance use 73% of the time
 - Relationship status 65% of the time



Sites Teens Use Instead of Facebook

- Snapchat
 - Users send “Snaps” — photos or videos — that last between 1 and 10 seconds as set by the sender
- Pheed
 - Users create and share videos, photos and voice tracks, plus make live broadcasts and share posts of 420 characters or less
- PicsArt
 - Users edit photos, draw, and share art
- Tumblr
 - Users blog and post photos and videos
- Vine
 - Users share videos that are six seconds or less



Things You Can Control





Signs of the social networking times.



Think Before You Post

- Millersville University refused to give Stacy Snyder a teaching credential
 - Stacy was weeks away from graduating
- School officials saw Stacy's photo on MySpace
 - Labeled "drunken pirate"
 - School accused her of promoting underage drinking





Reputation and Lifestyle

- CA company, Social Intelligence, searches social networks to help companies decide if they want to hire you
 - Systematically trolls social networks for evidence of bad character
 - Looks for racy photos, comments about drugs and alcohol...
- Evaluates you in categories
 - Poor judgment, gangs, drugs and drug lingo, demonstrating potentially violent behavior...

**SOCIAL MEDIA SCREENING
AND RESEARCH.**





Think Before You Post

- On Facebook, wife learns of husband's 2nd wedding
- Police charge deadbeat dad with 3 felony counts after seeing Facebook picture of him “rolling in money”





Fired for Posting on Social Media

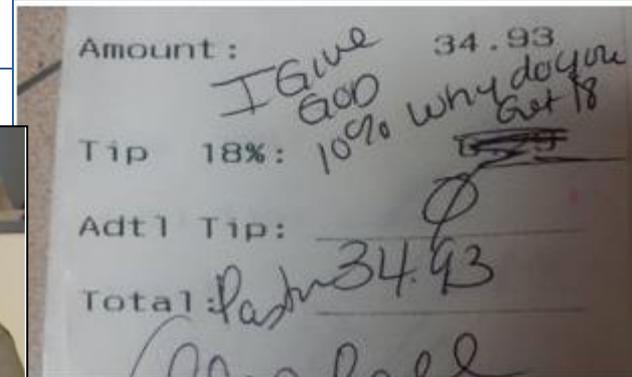
Applebee's defends firing of waitress who posted pastor's 'God' receipt

facebook

TEACHER RESIGNATION



"Now I remember why I stopped teaching! Kids... they are all germ bags!"

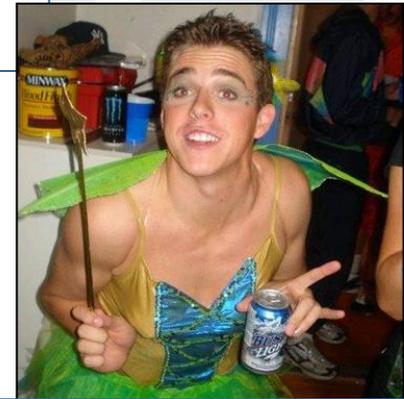


Reddit via Consumerist)

Temp Worker Calls CEO a "Complete Tool"



WI dispatcher
"addicted to vicodin,
adderall, quality
marijuana, MD 20/20
grape and absinthe"



Bank intern's
"family emergency"

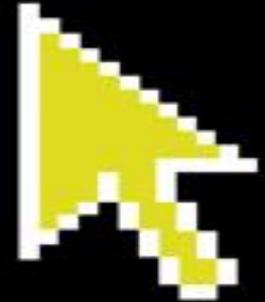


Even “Smart” People Do Dumb Things on Facebook

- A Cuyahoga County, OH prosecutor posed as an accused killer’s girlfriend on a Facebook chat with the alibi witnesses and tried to persuade them to change their testimony
- He admitted doing it and said he did nothing wrong
 - “Law enforcement, including prosecutors, have long engaged in the practice of using a ruse to obtain the truth.”
- He was fired for unethical behavior
 - “By creating false evidence, lying to witnesses as well as another prosecutor, [prosecutor] has damaged the prosecution’s chances in a murder case where a totally innocent man was killed at his work.”



Think Before You Post



Stop.

Think.

Click.



Pop Quiz

- What key piece of info do these folks want to know about you?
 - Stalkers
 - Potential dates
 - Bullies
 - Curious
 - Predators
 - Muggers
 - Marketers

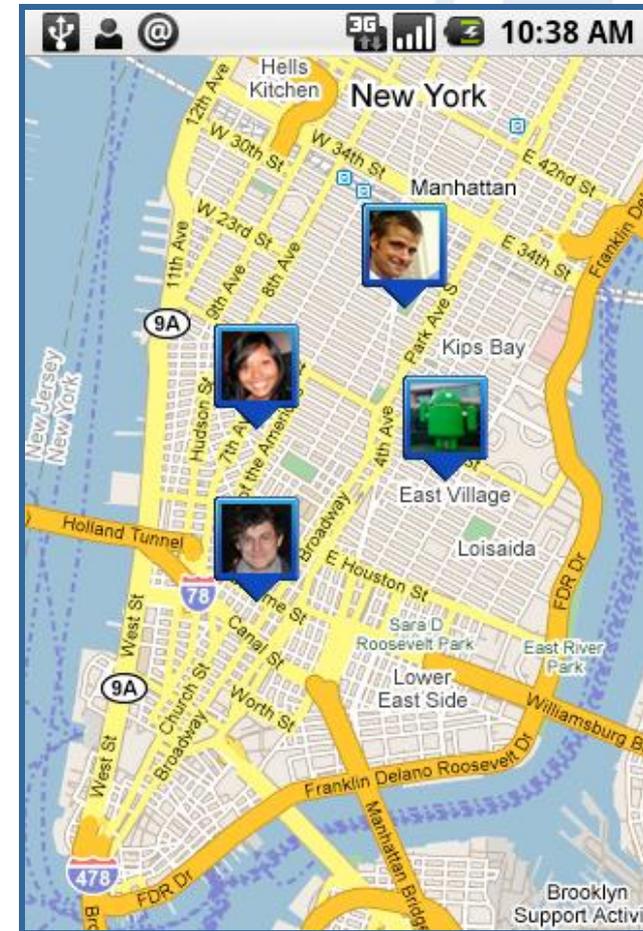




Pop Quiz

Location

- What key piece of info do these folks want to know about you?
 - Stalkers
 - Potential dates
 - Bullies
 - Curious
 - Predators
 - Muggers
 - Marketers





So, where are you?

- I'm on vacation!
- This concert's amazing!



Advertisement for Foursquare featuring the logo, a search bar with the text "Find places, people, tags" and a "SEARCH" button, and a "JOIN NOW" button. The background shows a map with location pins and icons for a crown, a trophy, and a location pin.

Already a member? [Login](#)

Find places, people, tags

**CHECK-IN
FIND YOUR FRIENDS
UNLOCK YOUR CITY**

Foursquare on your phone gives you & your friends new ways of exploring your city. Earn points & unlock badges for discovering new things. [LEARN MORE](#)



So, where **aren't** you?

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "Please Rob Me - Windows Internet Explorer provided by City of Phoenix". The address bar contains "http://pleaserobme.com/". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The toolbar shows "Convert" and "Select" buttons. The main content area features a cartoon illustration of a burglar with a beard, wearing a mask and a striped shirt, carrying a green sack with a dollar sign. To the right of the burglar, the text "PLEASE ROB ME" is written in large, bold, red, stylized letters. Below this, a dark blue banner contains the text "Raising awareness about over-sharing" in white. Underneath the banner, it says "Check out our [quest blog post](#) on the CDT website." The background of the page is light blue with a stylized map pattern and two red location pins with white 'X' marks.



Yes – It Really Happens

- August 2010, Nashua, NH: 50 home burglaries
- Suspects used social networking sites to identify victims who posted online that they would not be home at a certain time
- Police recovered between \$100,000 and \$200,000 worth of stolen property





Girls Around Me App

- “... scans your surroundings and helps you find out where girls or guys are hanging out
 - Browse photos of lovely local ladies and tap their thumbnail to find out more about them”
- Uses publicly available information retrieved from the Foursquare and Facebook



In the mood for love, or just after a one-night stand? Girls Around Me puts you in control! Reveal the hottest nightspots, who's in them, and how to reach them...



So why are privacy settings important?

We know what you're doing...

a social networking privacy experiment

 Like  32,068 people like this. Be the first of your friends.

 Tweet

6,922

 Follow @callumhaywood

Public Facebook statuses - Status Search - Foursquare location finder - Facebook friend checkins - Contact

[About this tool](#)

Who wants to get fired?

 **Martha G.**
Not the best day ever, hate doing this to my boss
about 57 minutes ago, 1 person like this, posted from Facebook for iPhone, report

 **Anb Shes R.**
I hate the social security building! I hate it even more when its somebody elses business im taking care of on top of tht my boss didnt even send me with all the right stuff --
about 1 hour ago, 5 people like this, posted from Facebook for Android, report

 **Lor W.**

Who's hungover?

 **Todd M.**
thing i worked on and put a lot of soul and effort into: 1 like status about how hungover i was from the night before: 30 likes
about 32 minutes ago, 1 person like this, posted from web, report

 **Kiana J. J.**
Something about today makes me wanna be hungover tomorrow --
about 37 minutes ago, 2 people like this, posted from Mobile, report

 **Fiona L.**
May have a hungover dog and a white leg tomorrow :-/ just caught Tilly lappin up my homebrew plum

Who's taking drugs?

 **Stacey Y.**
If you have to ask the girl at the smoke shop to front you for a 85¢ blunt wrap maybe u shouldnt be smoking weed..... jus saying haha
about 1 hour ago, 18 people like this, posted from Facebook for Android, report

 **Rocky R.**
Hmm looks like ima smoke a blunt and go see a movie days like this I wish I had a good women by my side to help take away this pain cuz the weed and drank just don't cut it no more
about 1 hour ago, 6 people like this, posted from Facebook for Android, report

Who's got a new phone number?

 **Shereen E.**
Text me names got a new phone but same number 07x7x6xxx7x
about 39 minutes ago, 1 person like this, posted from Mobile, report

Thanks to [@dgenerate_dave](#) for helping to fix the July 2013 breaking changes with Facebook's Graph API.

■ www.weknowwhatyouredoing.com



So why are privacy settings important?

- Facebook's new graph search easily uncovers, um, a lot

The top screenshot displays search results for the query: "Single women who live nearby and who are interested in men and like Getting Drunk!". It shows a grid of profile pictures on the left. The first profile is visible with the following details:

- Lives in London, United Kingdom
- Single · Female
- Interested in males
- Likes Getting Drunk!, Tortilla and 8 others

The sidebar on the right, titled "More Than 100 People", includes a "REFINE THIS SEARCH" section with the following filters:

- Gender: Female
- Relationship: Single
- Employer: Add...
- Current City: Add...
- Hometown: Add...
- School: Add...
- Friendship: Add...
- Likes: Getting Drunk! Add
- Live Near: Me
- Interested In: Men

The bottom screenshot displays search results for the query: "Married people who like Prostitutes". It shows a grid of profile pictures on the left. The first profile is visible with the following details:

- Married to [redacted], single [redacted]
- Likes Prostitutes, [redacted]
- Worked at [redacted]
- Lives in [redacted] Pennsylvania

The sidebar on the right, titled "REFINE THIS SEARCH", includes the following filters:

- Gender: Add...
- Relationship: Married
- Employer: Add...
- Current City: Add...
- Hometown: Add...
- School: Add...
- Friendship: Add...
- Likes: Prostitutes Add

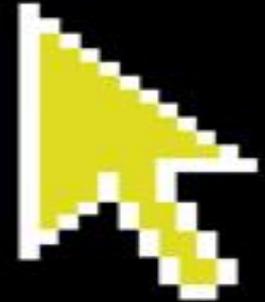


Think Before You Post

- Teen Alexa takes a picture of her brother as he sits on the family jet, devouring a Ritz-worthy buffet on their way to Fiji
 - She posts it on Instagram and points to it via her Twitter account
- On the same Twitter account, Alexa happily details her every move
 - The exact days she would arrive in, say, New York
 - Where she was shopping
 - High school graduation dinner invitation that foretold where (time, date, location) her dad and his wife would be in a couple of weeks' time
- Dad is Michael Dell, head of Dell Computers
- He pays about \$2.7 million a year for the security protection of his family
 - They shut down Alexa's Twitter account



Think Before You Post



Stop.

Think.

Click.



Social Media Can Be Used for Good

- In the Steubenville, Ohio rape case, witnesses and even the rapists themselves all posted details and accounts of the rape on Twitter and Facebook
- That's how the convicted teenagers that committed the rape got caught
- Because of Twitter, Instagram, Facebook and other media, there is written and visual proof of the actual rape and the blacked out condition of the rape victim
 - But this record is going to live online **forever**



Real Teens – Real Harassment

- Jasmine: Most of my Facebook friends are strangers. I get eight requests a day and pretty much just add anyone who asks. I get messages from strangers all the time and always have a chat with them, until they say something weird or pervy and then they get deleted.
- Emily: I get propositioned by strangers all the time on Facebook. A man I know through someone else, in his 30s, tried to befriend me and sent me obscene messages. He wanted to meet me. Mum went ballistic and made me block him and then she confronted him. Men also send explicit pictures but Mum blocks them straight away.

Jasmine, aged 14

4,204 friends

3,897 are strangers

121 male strangers over 30

7 have asked to meet

30 have bullied her

Emily, aged 15

642 friends

80 are strangers

70 male strangers over 30

30 have asked to meet

50 have bullied her



Sexting

- Sexting: Texting a racy photo of yourself (or just a body part) from your cell phone to another phone, emailing it to a friend, or posting it to your online profile page

Teens caught sexting may be charged with production, distribution and/or possession of child pornography – all are federal crimes.

53% of teens who sext are girls
47% of sexters are boys

17 percent of the sexting recipients report that they have passed the images along to someone else. 55 percent of those who passed the images to someone else say they shared them with more than one person.



THE TRUTH ABOUT TEEN SEXTING

86% OF SEXTERS ARE NOT CAUGHT

48% OF TEENS HAVE RECEIVED A SEXUALLY SUGGESTIVE MESSAGE

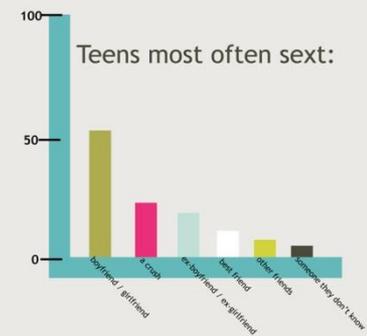
39% OF TEENS HAVE SENT A SEXT

PERCENTAGE OF TEENS THAT HAVE SEXTED NUDE OR SEMI-NUDE PHOTOS OF THEMSELVES:



AND

11% OF YOUNG TEENAGE GIRLS, AGES 13 to 16 HAVE SEXTED NUDE OR SEMI-NUDE PHOTOS OF THEMSELVES.



TO LEARN MORE ABOUT SEXTING AND HOW TO PROTECT YOUR CHILD VISIT: www.uKnowKids.com

References:
PC's in Dreams <http://www.pcindreams.com>
American Osteopathic Association <http://www.osteopathic.org>
The Pew Charitable Trusts <http://www.pewcharitable.org>
Enough is Enough <http://www.enoughis101.org>
Designer: Brigit Gilbert



Sexting: It's not just for kids

Anthony Weiner



Tiger Woods



Brett Favre





I'll Just Use Snapchat...

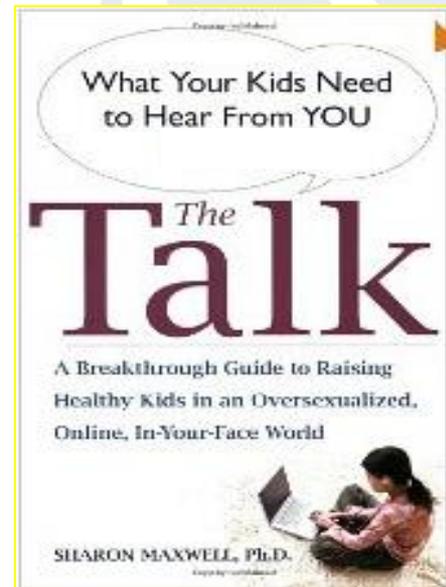
- Snapchat lets a user send a text, photo or video that purportedly self-destructs within 10 seconds of being opened
 - One of the most-downloaded free iPhone apps
- Its messages aren't guaranteed to disappear
 - Anyone receiving a text or photo can within 10 seconds capture a "screenshot"





Have “The Talk” with Kids (and Spouse!)

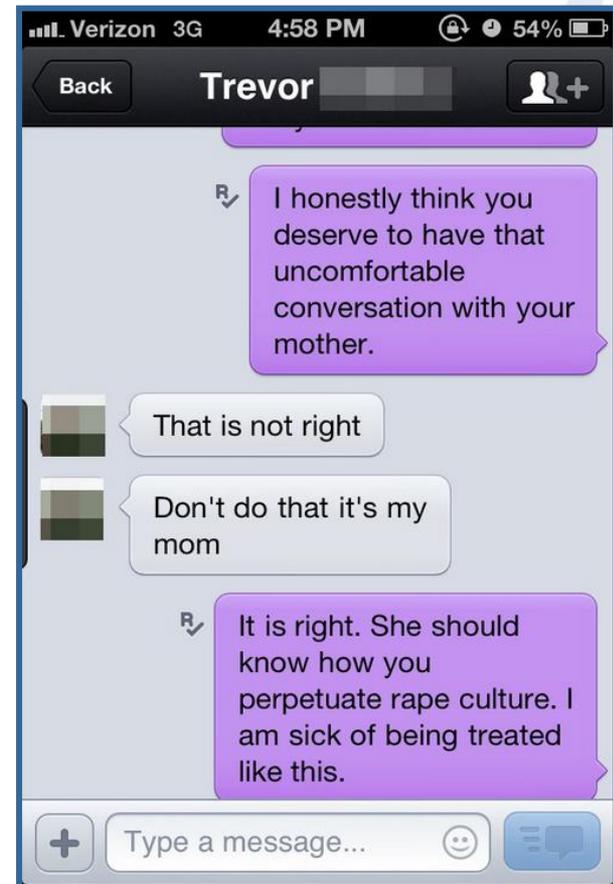
- **Old: Sex Education; New: The Technology Talk**
 - Make it a conversation, not a lecture
- Key points
 - Online actions have real-world consequences
 - Be careful when posting – you can’t take it back
 - They can’t hide behind what they post
 - Trust their gut if they’re suspicious
 - Predators are out there
 - Some info should stay private
 - Full name, address, picture, location...
 - Never meet an online contact alone and without your knowledge





Here's One Way to Stop Unwanted Pics

- Woman on dating site sends unsolicited picture to sender's mom



summary
safeguards
summation
key
points
review

synopsis



Protect Your Safety

- Practice a little self-censorship
- Keep daily routines, locations, and whereabouts to a minimum
 - Don't "check in" everywhere you go
- If you go on a trip, reveal everything you want **after your travels**
- Talk to your family about good online safety and security habits, including protecting their personal information and their reputation
 - Know what sites your family visits online



Protect Your Family

- Put the family PC in the middle of the living room





Protect Your Privacy and Reputation

- Pick the strongest privacy settings
 - Verify regularly that they haven't changed
- Always assume that anything posted can be seen by friends, family (your mom!), employers, government agencies, health insurance companies, and law enforcement
 - Even sending private messages using a social networking site
- Plug your name into a search engine and make sure what comes up is information you want to share with the world



Pick Your Friends

- Don't blindly accept friend requests
 - "Friends" can often see more info than everybody (public)
- Only link to people you actually know
 - Like on LinkedIn
- Remember, not everyone who can see your online information has your best interests in mind
 - Predators, thieves, con men...
- Don't post potentially sensitive information about other people
 - Understand and respect your friends' privacy preferences



Protect Your Computer

- Don't download tools or software updates when prompted to do so after clicking a link from a social networking site
 - Go to the software vendor's site using a known URL
- Preview shortened URLs
- Don't click on links that promise shocking or embarrassing videos
- Review the list of apps and sites that you granted access to your social networking accounts
 - Deauthorize services you no longer use
- Keep antivirus and security patches up-to-date

Preview a TinyURL

Don't want to be instantly redirected to a TinyURL and instead want to see where it's going before going to the site? Not a problem with our preview feature.



Protect Your Accounts: Passwords

- 75% individuals use same password for social networking and email
- What's the risk?
 - Social networking sites are notorious for being hacked (passwords stolen)
- Use one password only for social networking
 - Don't use Facebook to sign in to other websites / services
- Make it long and strong
 - 10+ characters, mixed alpha, numbers, special characters
- Learn more: see Password Cracking 101 and Password Management 201, phoenix.gov/infosec Resources page





Protect Your Accounts: Choose Strong Security Questions

- 2012: Mitt Romney's free email account was hacked
- 2008: Sarah Palin's free email account was hacked
 - The hackers guessed the answers to security questions to change the accounts' passwords
- Don't post info that could be used to guess your password-reset security questions
 - Favorite pet, old schools, old addresses or neighborhoods, where you were born, parents' names, first car...



Protect Your Company: Follow Your Company's Policy

- Criminals and competitors can use sensitive info you post against your company
- Example: Competitor uses info you post about work to embarrass your company, employees, or products
- Example: Bad guy uses information you post to craft phishing emails that contain authentic details about your company
 - Coworkers are more likely to think emails are legit and click on links or open attachments
- Example: Tech Support posts a question on a techie blog and describes your computing environment in great detail
 - Hacker now knows which exploits to use to attack



Great Moments in Parenting





Thank You!

- For more information, please visit phoenix.gov/infosec

City of Phoenix
OFFICIAL WEB SITE

Residents
Businesses
Visitors & Newcomers

Public Safety
Transportation
Culture & Recreation

City Government
Employment
Sustainability

99F Fair | 5:10 PM | May 30, 2012
Live Streaming
watch

Information Security and Privacy

Home > Public Safety > Information Security & Privacy

Police
Crime Prevention
Fire
Fire Safety
Personal Safety
Home & Health
Information Security & Privacy
Info for Everybody
Info for Business
Resources
About Information Security & Privacy Office
Traffic Safety
Homeland Security
Public Safety Statistics
Online Games & Activities
Community Outreach

Related Links

- ▶ CNET Personal Security Dashboard
- ▶ CSO Online Daily Dashboard
- ▶ MS-ISAC Digital Dashboard
- ▶ MS-ISAC Dashboard - Text Version
- ▶ Security Wizardry Radar

Click on a word to start.

Phishing
Cyber-Bullying
Compliance
Apps
Virus
ID-Theft
PC-Protection
Mobile-Devices
Passwords
Security
Privacy



More Cowbell (Supplemental Info)

City of Phoenix



Social Media Smartcards

Google+ Smart Card

Social Networks - Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family that you post or share in public.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that are otherwise concealed. **Never post Smartphone photos.**
- Use secure browser settings when possible and monitor your account activity.

Managing Your Google+ Profile

Google+ provides privacy and sharing options using Circles. You can share content with family, friends, or colleagues. Content is shared only with the people you specify.



Profile Settings

Apply and save the Profile settings shown below to ensure your profile is secure.



LinkedIn Smart Card

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family that you post or share in public.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that are otherwise concealed. **Never post Smartphone photos.**
- Use secure browser settings when possible and monitor your account activity.

Managing Your LinkedIn Profile

LinkedIn is a professional networking site whose users are employees and employers. Users post and share information about their work and professional life.



Profile Settings

Apply the Profile settings shown with arrows below to ensure your profile is secure.



- Users tend to share information related to their work and professional life.
- LinkedIn profiles tend to be more visible and searchable.
- Paid LinkedIn accounts have access to more information.
- The type of information users can see about each other is more extensive.

G-121911_2000

Twitter Smart Card

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family that you post or share in public.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that are otherwise concealed. **Never post Smartphone photos.**
- Use secure browser settings when possible and monitor your account activity.

Managing your Twitter Account

Twitter is a social networking and microblogging platform with +300 million active users as of 2014.



Followers are people you subscribe to. Private tweets will only be visible to followers you approve.

Hashtags (#topic) are used to mark a keyword. Posts with hashtag are categorized in Twitter search engine. Hashtagged words that become trending topics (ex. #Jan25, #Egypt, #Mentions (@username) are used to tag a user update. When a public user mentions a private account, the link to the private account profile.

Profile Settings

Apply the Profile settings shown below to ensure your profile is secure.

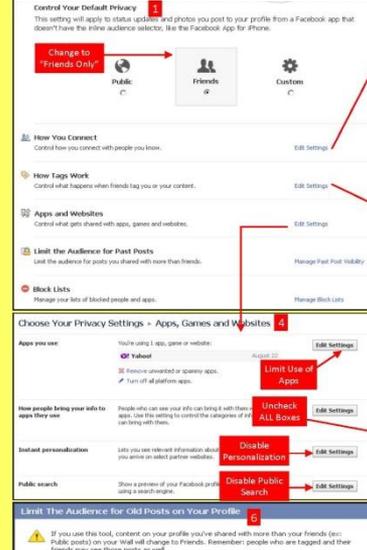


LI121911_1400

Facebook Smart Card

Social Networks - Do's and Don'ts

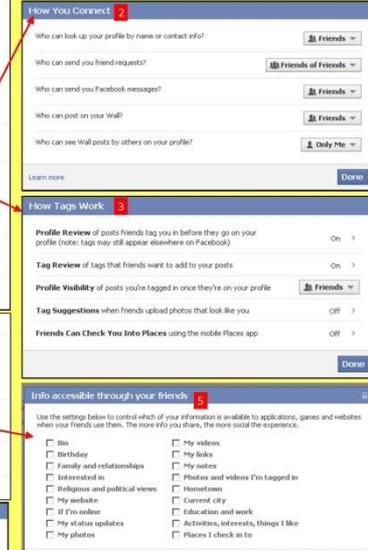
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family that you post or share in public.
- Ensure that your family takes similar precautions with their social media accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.



LI121911_1631

Minimizing your Facebook Profile

Facebook has hundreds of privacy and sharing options. To control how your personal information is shared, you should use the settings shown below (such as Only Me, Friends Only) for (1) Privacy, (2) Connecting, (3) Tags, (4) Apps/Websites, (5) Info Access through Friends, and (6) Past Posts.



FB121211_1800

Available from Air Mobility Command's website
<http://www.amc.af.mil/amcsocialmediahub/index.asp>



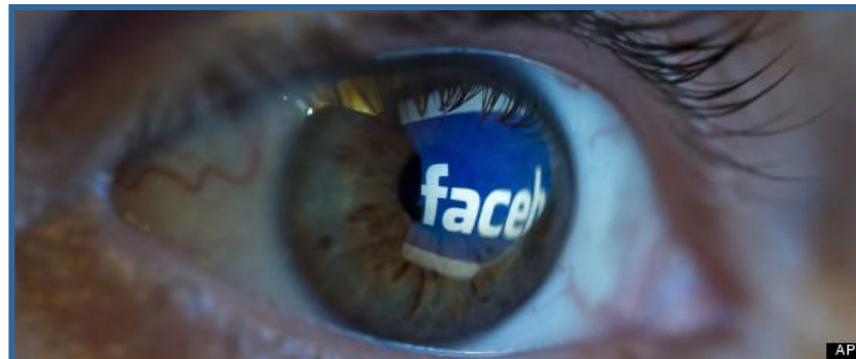
Highlights of Facebook's Proposed Privacy Changes

- Your information may show up along ads for companies that you have “liked”
- You can opt out of your information appearing in social ads, though you can't opt out of your name being attached to Sponsored Stories in your friends' news feeds
 - The only way to avoid that is to not like or share any content from a brand page
- Your name and picture will not appear next to ads to strangers
 - Only your Facebook friends can see that info
- Users won't be compensated for allowing their image to be co-opted by advertisers



Facebook Delays Controversial Privacy Policy Change

- Facebook said it would hold off proposed revisions to Facebook's privacy policy until week of 9/16/2013
- Policy states that Facebook users automatically consent to having their likenesses used by Facebook – unless members say otherwise
- Privacy advocates allege that the new document still violates the agreement by letting Facebook use personal information in ads without sufficient explicit consent from members





Fake Contact Requests

- October 2010 – LinkedIn fake contact requests
 - Email appears to be a contact request sent from LinkedIn – “click to view the request”
 - Users who click on the link are routed to an intermediary website with the notification “Please wait ... 4 seconds”
 - Then users are redirected to Google
 - Malware Bugat is downloaded to PC in the 4 seconds
 - Bugat harvests info during online banking sessions





Why Have a Fake Profile?

- Hide your true identity
- Present a more enticing image
 - “Prettier” people are more popular
- Appear more legitimate or more qualified
- Gather up connections / followers to appear more important
- Gain access to closed forums and/or post misinformation
 - To lurk to learn information
 - To post offensive or wrong information
 - Example: Pretending to be a Pepsi employee and posting “shocking facts about Pepsi ingredients”
- Gather email addresses for spam lists



How to Spot a Fake Profile

- Name doesn't seem "right"
 - Name of a comic or fictional character
 - Example: John Smith from Italy
- Picture looks "wrong"
 - Too professional or informal for profile description
 - Background incongruous with profile description
 - Example: John Smith from Italy's picture shows car in background with AZ license plate
 - Celebrity or stock photo
 - Contains photo company watermark or metadata
 - TinEye and Google offer reverse image search
- Credentials are generic and/or cannot be verified
 - Too good to be true
 - Dates don't add up
 - Example: John Smith graduated in 2004 but has 22 years of experience



Pop Quiz

- Real profile or fake?

Molly Major
Human Resource Manager at Tuttle Enterprises
Phoenix, Arizona Area | Human Resources

Current

- **Human Resource Manager at Tuttle AZ**

Past

- **Military Personnel Management/Program at Air National Guard, Midway Field, AZ**

Education

- **Arizona State University**

Connections 500+ connections

Twitter [mollymajorr](#)

Public Profile <http://www.linkedin.com/pub/molly-major/28/67a/a88>

Suspect Fake Profile: Molly Major
Source: LinkedIn



Fake!

- Spam-y name with alliteration
 - At least it's properly capitalized
- The picture was “one of 30 most beautiful women found on Flickr”
 - (Link no longer active)
- There is no Air National Guard deployed at “Midway Field, AZ”
 - According to Arizona Air National Guard website, there is no “Midway Field” at all
- There is no company called Tuttle Enterprises in or near Phoenix, AZ
 - There's one in Sarasota, FL



CIA's Facebook Program

- CIA's "Facebook" program dramatically cut agency's costs
 - <http://www.youtube.com/watch?v=ZJ380SHZvYU>





More Bad Guy Examples

- Man living in Key Largo, FL posted a picture of his custom, handcrafted fishing poles on Facebook for all his friends to see
 - He even included a great picture of the new hanging racks in his garage where he stored them
 - Thief stole them later that night while he slept upstairs
- Man advertised the great New York vacation his family was taking
 - They came back to an empty house
 - Even the food and the garbage cans were gone



#Draining...

- Take a break from social networking

I am so sick of La. And sick of the lies that come with it. I didn't call off my wedding. Taking a break from social media. #draining

— Miley Ray Cyrus (@MileyCyrus) March 6, 2013



Remember – Don't be a Troll





Online Threats



- 30,000 URLs (websites) are infected every day
 - 80% of those infected sites are legitimate
- 85% percent of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web
- Drive-by downloads have become the top web threat
- **Update your antivirus, operating system, and browser**



Resources

- Wired Safety
 - <http://www.wiredsafety.org/index.html>
- FTC's OnGuard Online
 - <http://www.onguardonline.gov/>
- Kameron Institute Cyber Bullying Solutions
 - <http://kameron.org/Bullying-Solutions>
- Microsoft's Page on Online Predators (with link to Parental Controls)
 - <http://www.microsoft.com/protect/parents/social/predators.aspx>
- PC Magazine's review of parental control software
 - <http://www.pcmag.com/article2/0,2817,2346997,00.asp>
- Electronic Privacy Information Center (EPIC)
 - <http://epic.org/>