LegalSEC SUMMIT 2017

SOCIAL NETWORKING'S EFFECT ON BUSINESS SECURITY CONTROLS

Jon Hanny
Director of Information Security and Assurance, Buckley Sandler LLP
Gaurav Chikara
Senior Security Engineer, Cooley LLP

AGENDA

- Social media attack overview
- Stages of an attack
- Attack simulation
- Prevention and detection
- Security recommendations

SOCIAL MEDIA: COMMON ATTACKS

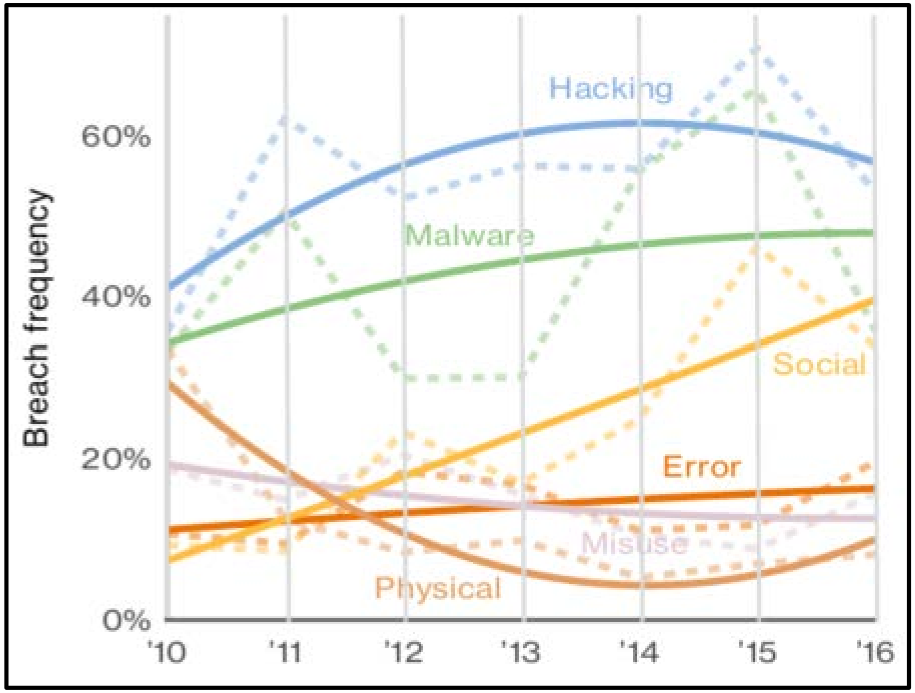
- Account Takeover
- Impersonations
- Phishing
- Customer scams
- Information leakage
- Hashtag/traffic hijacking

HOW BAD IS IT REALLY?

- LinkedIn
  - 2012
    - 6.5 million encrypted passwords posted on Russian crime forum
  - 2016
    - 167 million login credentials
    - 160 million compromised accounts had unique email addresses
- Facebook
  - 2013
    - Year-long breach exposed 6 million users
- Twitter
  - 2016
    - 32 million Twitter credentials stolen (Twitter was not breached)
    - Credentials stolen by malware infecting browswers

HOW BAD IS IT REALLY?

- 43% of breaches were social attacks
- 66% of malware via malicious email attachments
- 7.5% fall for phishing emails



STAGES OF A SOCIAL NETWORKING ATTACK

- Target a company
- Identify users in target company
- Identify users to target
- Target via information online
- Target via password guessing
- Target via personal email
- Gain access to the target users’ system(s)

TARGET A COMPANY: WHY?

- Motive:
  - Headlines
  - Money
  - Retaliation
  - Politics

- Smaller companies have smaller budget for security and hence fewer defenses

IDENTIFY USERS IN TARGET COMPANY

- Searching on internet
  - Using tools to identify the email address
  - Using tools to identify the schema for example if email schema is firstname.lastname@company.com
  - Using websites such as LinkedIn, Twitter, Facebook, Google searches to see what users are doing and also what product company are using.
  - Social engineering and calling the secretary to find information

IDENTIFY USERS TO TARGET VIA INFORMATION ONLINE

- Once target users are identified, the hacker uses tools to gather information on those users
- Several tools are readily available online and information can be gathered from online sites for free or with a cost to have more targeted attacks
- This information will also be used for password guessing attacks against target user accounts on social media sites

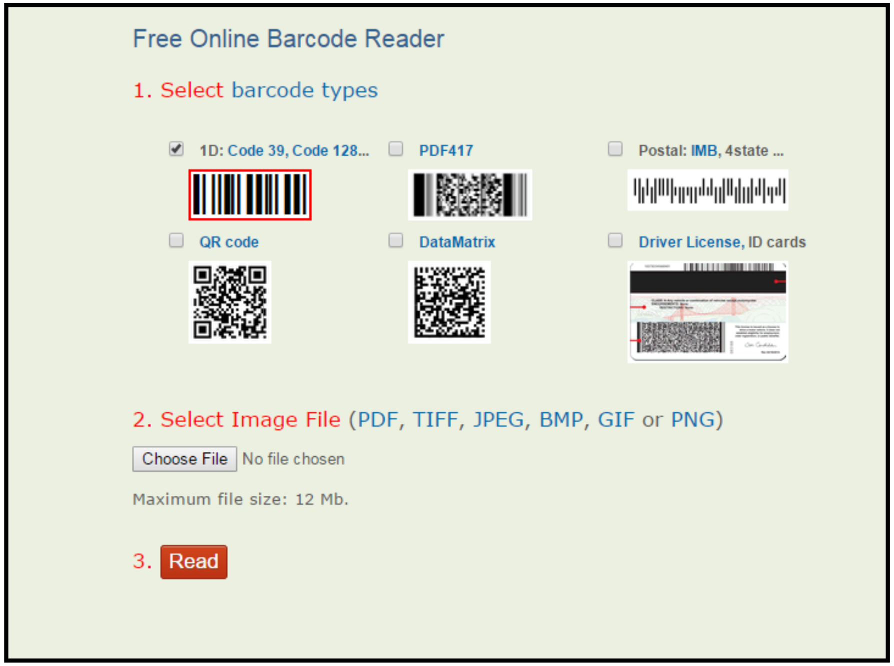
SOCIAL MEDIA SITES: RIPE WITH PERSONAL INFORMATION

- Facebook:
  - Personal information
  - Family members name include there wife and children information
  - Travel history
  - Friends' names
  - Date of birth
  - Spouse/Partner
  - Residency: past and present
  - Relatives and other Family information
  - Interests
  - Photos
  - Unusual information such as boarding passes

ONLINE DATA DISCOVERY

Example: Site to upload the barcodes or QRcodes to gather information

- Reveals information such as:
  - Traveler’s name
  - Frequent flyer number
  - Individual who booked the flight
  - Emergency contact information



Free Online Barcode Reader

1. Select barcode types

☑ 1D: Code 39, Code 128... □ PDF417 □ Postal: IMB, 4state ...

□ QR code □ DataMatrix □ Driver License, ID cards

2. Select Image File (PDF, TIFF, JPEG, BMP, GIF or PNG)

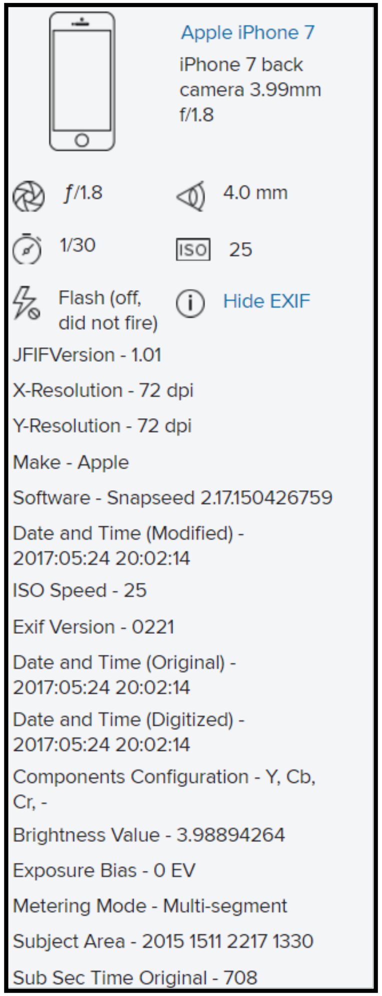
Choose File No file chosen

Maximum file size: 12 Mb.

3. Read

ONLINE DATA DISCOVERY

- Sites can reveal user information
  - Flicker
  - Snapchat
- Flicker photo metadata example



Apple iPhone 7
iPhone 7 back camera 3.99mm f/1.8

ƒ/1.8
4.0 mm
1/30
ISO 25
Flash (off, did not fire)
Hide EXIF

JFIFVersion - 1.01

X-Resolution - 72 dpi

Y-Resolution - 72 dpi

Make - Apple

Software - Snapseed 2.17.150426759

Date and Time (Modified) - 2017:05:24 20:02:14

ISO Speed - 25

Exif Version - 0221

Date and Time (Original) - 2017:05:24 20:02:14

Date and Time (Digitized) - 2017:05:24 20:02:14

Components Configuration - Y, Cb, Cr, -

Brightness Value - 3.98894264

Exposure Bias - 0 EV

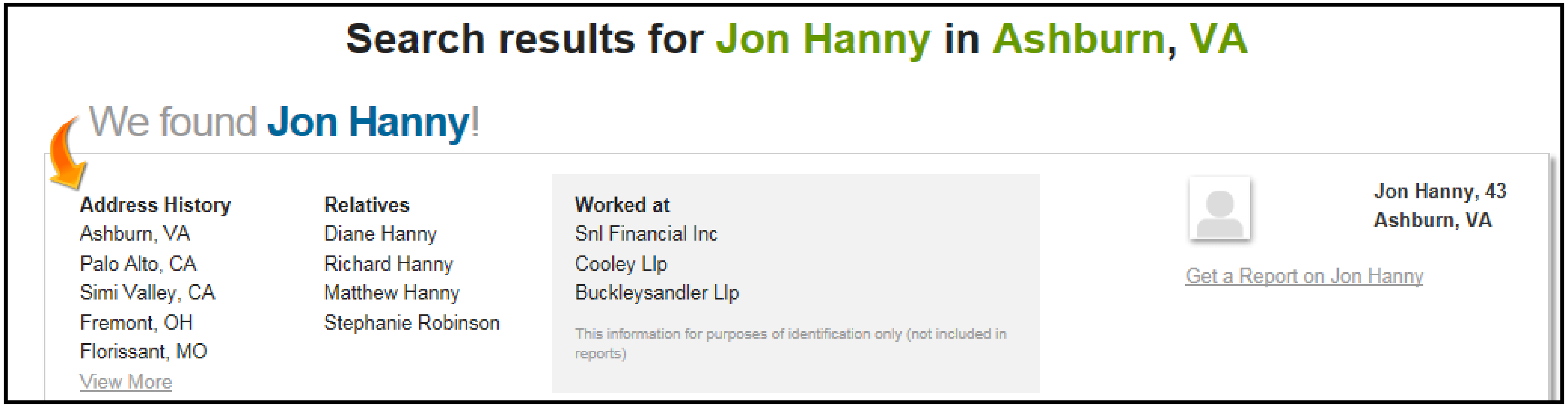
Metering Mode - Multi-segment

Subject Area - 2015 1511 2217 1330

Sub Sec Time Original - 708

DEMO: IDENTIFY TARGETS USERS

1) Demo: theh
2) Demo: Sn1
3) Building a list using free provided internet tools such as intelius.com, whitepages.com, instantcheckmate.com, Nuwber.com, onerep.com



Search results for Jon Hanny in Ashburn, VA

We found **Jon Hanny**!

Address History
Ashburn, VA
Palo Alto, CA
Simi Valley, CA
Fremont, OH
Florissant, MO
View More

Relatives
Diane Hanny
Richard Hanny
Matthew Hanny
Stephanie Robinson

Worked at
Snl Financial Inc
Cooley Llp
Buckleysandler Llp

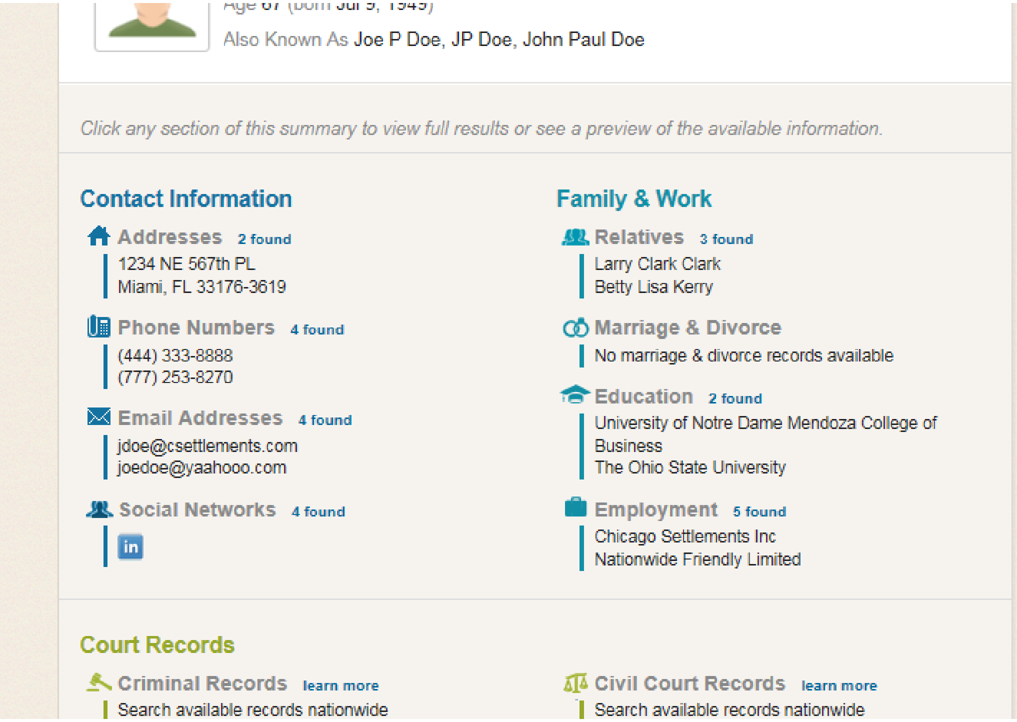
This information for purposes of identification only (not included in reports)

Jon Hanny, 43
Ashburn, VA

Get a Report on Jon Hanny

DEMO: IDENTIFY TARGETS USERS

- Paid version can provide more information here is an example



Age 67 (born Jul 9, 1949)

Also Known As Joe P Doe, JP Doe, John Paul Doe

Click any section of this summary to view full results or see a preview of the available information.

Contact Information

Addresses 2 found
1234 NE 567th PL
Miami, FL 33176-3619

Phone Numbers 4 found
(444) 333-8888
(777) 253-8270

Email Addresses 4 found
jdoe@csettlements.com
joedoe@yaahooo.com

Social Networks 4 found
in

Family & Work

Relatives 3 found
Larry Clark Clark
Betty Lisa Kerry

Marriage & Divorce
No marriage & divorce records available

Education 2 found
University of Notre Dame Mendoza College of Business
The Ohio State University

Employment 5 found
Chicago Settlements Inc
Nationwide Friendly Limited

Court Records

Criminal Records learn more
Search available records nationwide

Civil Court Records learn more
Search available records nationwide

DEMO: BUILDING A PASSWORD LIST

- We can build a password list that we can try
  1) CL Demo
  2) Password profiling : CY DEMO

DEMO: USING THE PASSWORD LIST

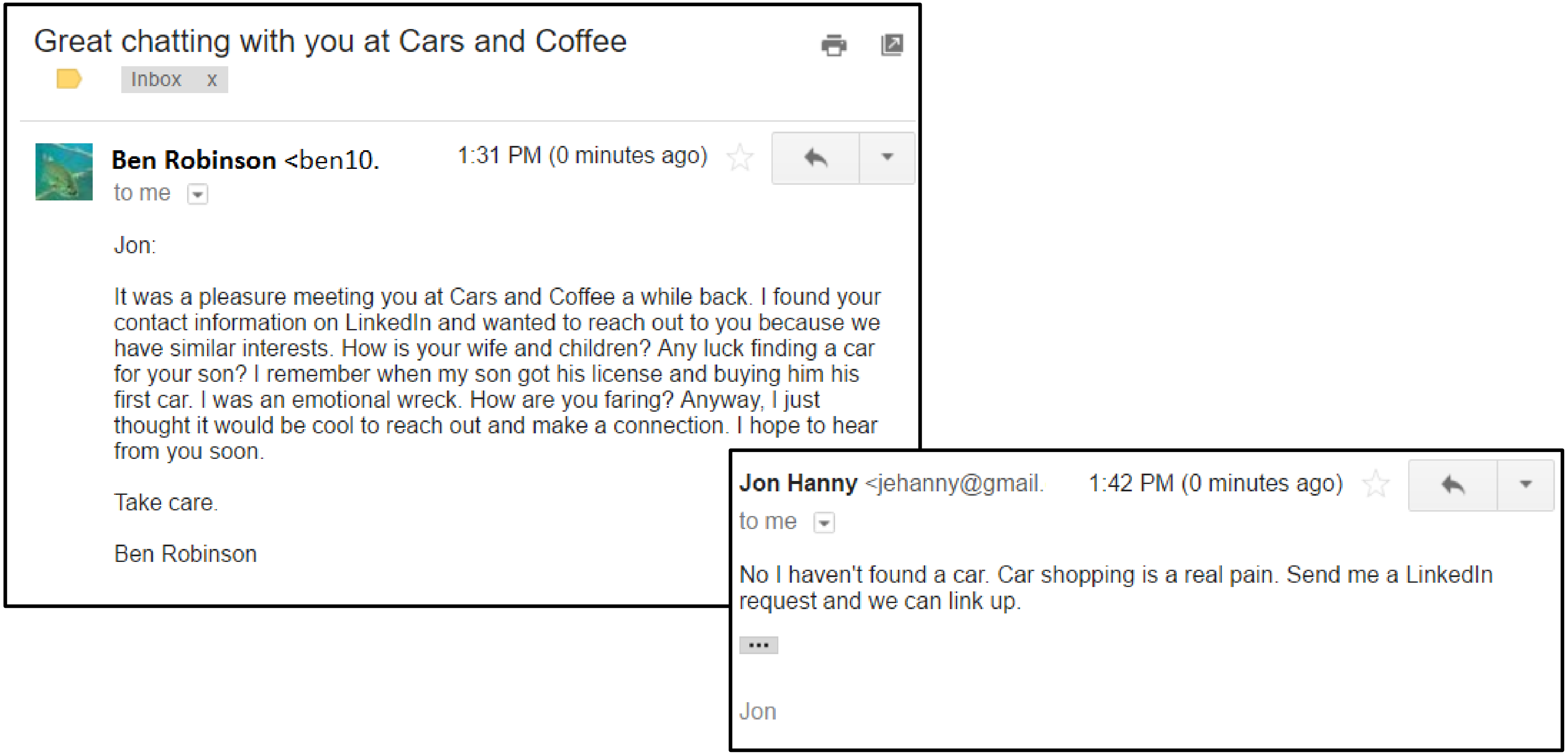
- Using password list on company sites can create too much noise
  - Demo: cred

TARGET USERS VIA PERSONAL EMAIL

- Building trust:
  - Target Users by sending them personalized emails with no bad links
  - Use collected information to formulate emails, using there friends’ and family member names
  - Send emails with Gmail or Yahoo with valid username to build credibility

TARGET USERS VIA PERSONAL EMAIL

- Sample trust-building email exchange



Great chatting with you at Cars and Coffee

Ben Robinson <ben10. 1:31 PM (0 minutes ago)

to me

Jon:

It was a pleasure meeting you at Cars and Coffee a while back. I found your contact information on LinkedIn and wanted to reach out to you because we have similar interests. How is your wife and children? Any luck finding a car for your son? I remember when my son got his license and buying him his first car. I was an emotional wreck. How are you faring? Anyway, I just thought it would be cool to reach out and make a connection. I hope to hear from you soon.

Take care.

Ben Robinson

Jon Hanny <jehanny@gmail. 1:42 PM (0 minutes ago)

to me

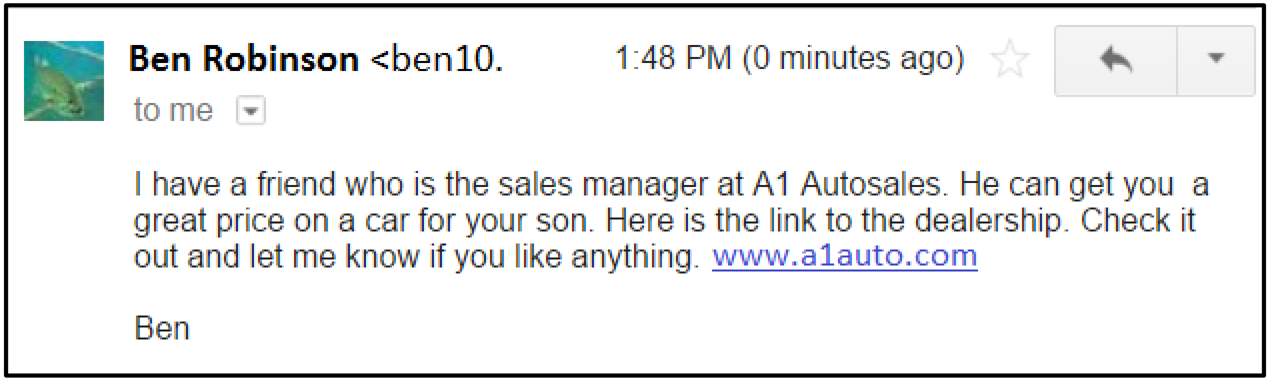
No I haven't found a car. Car shopping is a real pain. Send me a LinkedIn request and we can link up.

...

Jon

DEMO: ATTACK

- After the victim replies, send malicious email
  - Sample email below
  - Link is actually malicious



Ben Robinson <ben10.

to me

1:48 PM (0 minutes ago)

I have a friend who is the sales manager at A1 Autosales. He can get you a great price on a car for your son. Here is the link to the dealership. Check it out and let me know if you like anything. www.a1auto.com

Ben

PREVENTION AND DETECTION

- Technical Controls
  - Email filtering
  - Web filtering
  - SIEM
  - Access control
  - Dark web monitoring
  - Vulnerability/Patch management
  - Anti-Malware/Endpoint protection

DETECTION AND PREVENTION

- Administrative Controls
  - Social Media Policy
  - Awareness Training
  - Insurance

SOCIAL MEDIA SECURITY RECOMMENDATIONS

- LinkedIn
  - – Enforce Two-Step verification
- SnapChat
  - – Lock down the “Who Can…” settings
- Instagram
  - – Enable two-factor authentication
  - – Do not add phone number, location
  - – Set profile to private

SOCIAL MEDIA SECURITY RECOMMENDATIONS

- Facebook
  - Enforce Two-Step authentication
  - Enable “Get alerts about unrecognized logins”
  - Who can see my stuff – friends or custom
  - Who can see my friends list – friends or custom
- Strong passwords
  - Always use strong passwords
  - Each account should have unique password
- Always be mindful of your posts