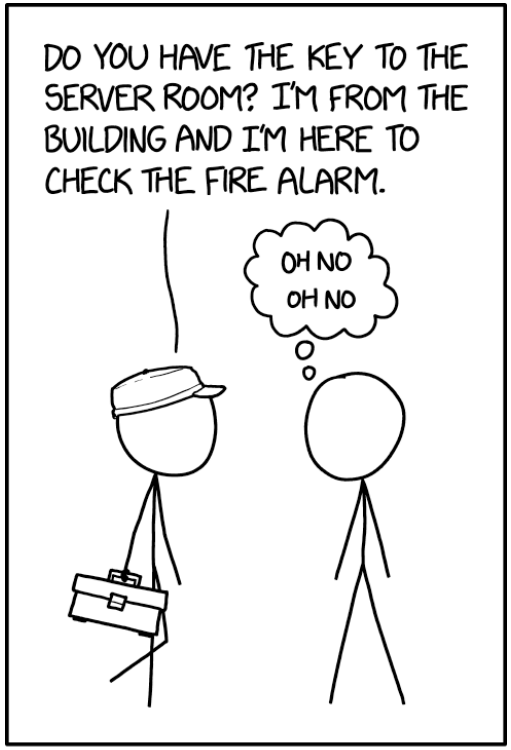
Social Engineering

Obligatory xkcd



Business

- Making items look worse than they are
  - air conditioner sales
  - locksmith
  - car repair
- http://www.cbc.ca/marketplace/
- Phishing
  - Banks
  - Paypal
  - Shotgun approach – millions of attempts yield few successes.

Old School Phone Scams

- Calling when unexpected - phone scams
  - CRA
  - Cruise scams
  - Timeshares
  - Windows Tech Support
  - CSIS scam - http://www.itworldcanada.com/article/csis-spam-scam-returns/377961?sub=375194&utm_source=375194&utm_medium=security&utm_campaign=enews

Social Media

- Valley Florist - google maps showed as closed on Mother's Day weekend
- Feedback on products, generally badmouthing products on shopping sites like Amazon - hard to differentiate from general product reviews
- Catfishing

Social Media

- Photoshopping and posting to Facebook. https://www.pinterest.ca/mariolafond/photoshop-and-fb-failed/
- Picture of Hillary Clinton and a confederate flag - many examples similar.
- Social media posts that trigger an involuntary click.
- Posting links in twitter during news
  - http://deadspin.com/joffrey-lupul-legit-pissed-at-joke-tweet-that-made-it-t-1688923332

Emergency Services

- Pulling the fire alarm
- Swatting
- Reporting bad driving to police
  - Trigger driving infraction ticket

Retail POS

- Lululemon scanner in drawer - hand scanners becoming more common, asking for help can expose vulnerability.
  - Some scanners are tied to inventory, manipulating inventory can cause price changes
  - Mobile POS
  - Some may manage prices

Politics

- Hilary Clinton as above
- Political messaging - Obama attacks, Justin Trudeau attacks, unchallenged social media campaigns.
- Donald Drumpf
- Trump quote about Republicans
- Obama video
- 2016 American Federal Election

Tainted XCode in China

- 4000 apps on Apple App Store infected with XCodeGhost malware. (2015)
  - The tainted version of Xcode was downloaded from a server in China that developers in the country may have used because it allowed for faster downloads than using Apple's servers in the U.S. Because of China's internet firewall, it can take up to three times longer for developers there to download XCode from Apple's American servers, compared with 25 minutes for domestic downloads from within the U.S., company executive Phil Schiller said.
- Has been a concern for compilers for decades

Why me?

- As you move through your careers, you will have more seniority, more responsibility, and greater access.
- You will need to be vigilant to mitigate against attacks, part of which is likely to include a social engineering component.

What to do

- **Hiding yourself**
- When it comes to hiding yourself, there aren't any really guaranteed steps. I do, however, suggest some of the following:
- Don't use your real name, use a variation
- Don't give your real birthday, use something close
- Don't give your SIN. No website should be asking for this
- Don't upload pictures next to your real name
- Consider multiple online identities, for different areas. Try not to cross contaminate.

Google yourself

- Searching for your pictures using Google. Note the likelihood of finding yourself increases as you focus your search.
- Image search in Google
- The steps to find yourself in Google are relatively simple, but always changing due to SEO mitigation. Consider other search engines like (shudder) Bing.

Examples You May Experience

- USB storage drive (thumb drive) outside the parking spot of an administrative assistant's parking spot first thing in the morning, or outside a nurse's parking spot at the beginning of a sift.
- Walking through the private/restricted areas of a business wearing a MTS or Shaw shirt, with a fake identification badge
- Happening to have a suspicious amount of similarity to someone you just met online.

Examples

- Reverse Social Engineering.
- Piggyback Rides.
- Spearphishing
- Whaling (phishing senior or high profile targets).
- Catfishing (secure your social media content).
- Baitclicks.
- Old school – become friends in a bar. With Winnipeg's small tech community, this could be more important than elsewhere.

2020 Top Scams & Median Cost

- Here are the top 10 scams of 2020, based on the number of reports to BBB Scam Tracker (Canadian Better Business Bureau)*
  1. Online Purchases → $96
  2. Employment Scam → $967
  3. Fake Check/Money Order→ $1 697
  4. Advance Fee Loan → $745
  5. Home Improvement → $1 193

2018 Top Scams (cont)

6. Romance → $2 100
7. Cryptocurrency → $1 200
8. Tech Support Scams → $499
9. Travel/Vacation/Time Share → $1 300
10. Investment → $948

* Results likely impacted from COVID restrictions

- Source: https://www.bbb.org/bbbscamtrackerriskreport

Tools of the Trade

- Dictators Handbook, 48 Laws of Power, other social engineering/influence books
- Linguistic Skills
- Consequence free practice – shotgun approach
- Prepared carefully worded text ready to copy/paste
- Law enforcement tactics
- Social media research - linkedin

What to do

- Training, training, training
- Audits/drills
- Culture of support
  - Most success in social engineering/ cyberbullying attacks relies on shame
- Understand the longer you empower them, the more power they have
- Follow online groups like reddit to keep current
- Silence, both as an offensive and defensive weapon

Additional Resources

- reddit.com/r/SocialEngineering
- 4chan and other sites of this nature (shocking at times, less relevant)
- Lurking in chat areas
- Discord social engineering servers
- Good old watching people in a bar