# Staying Safe Online

Toby Kohlenberg
CISSP, GCIA, GCIH, GPEN, CICP

1

## Introduction

- Toby Kohlenberg
  Senior Information Security Technologist
  for a Fortune 50 company

*That means I spend all my time dealing with this stuff.*

2

## Agenda

- Introduction
- Overview
- The Proper Attitude
- Preventing Problems
  - Email
  - Web Browsing
  - Social Media
- Avoiding Being a Problem
- Detecting Problems
- Recovering from Problems
- References
- More technical security options

3

## Overview

- The Internet is a dangerous place
  - Just like the freeways
- There are basic things you can and must do to protect yourself.
  - This is not optional
  - Just like being a defensive driver
- This is a chess game that never ends*
  - You have live opponents who are constantly adapting to whatever you do
- Focus on prevention
  - Recovery can be a lot of work in the best of cases
- Prepare for recovery. Something bad happens to everyone at some point. Preparation makes the difference.

4

## The Proper Attitude

- Technology doesn't change the basics
  - Nothing is free
  - If it seems too good to be true, it is.
  - If you aren't paying for the product, you are the product
  - Be suspicious*
- Epidemiological model is highly applicable
  - Anyone you interact with might be infectious
  - The behavior of your trusted circle can (negatively) impact you
  - Universal Precautions are essential

5

## The Proper Attitude

- Any website you go to is a "stranger". If a stranger comes up to you and:
  - Warns you that you are in danger
  - Offers you large sums of money
  - Tells you something about yourself that you think no one should know
- You should be HIGHLY suspicious.
  - In this case that means close your browser, don't click on any links, don't click on anything except the button to quit the application

6

## Prevention (in general)

1. The proper attitude
2. Automatic patching
3. Good passwords
   - Complex or Long*
   - Different passwords for different sites
   - Password vaults are okay*
   - Don't tell people your passwords
     - Unless you would give them your house/car/safe deposit key
4. Up to date Antivirus
   - That is configured to scan regularly

- **Backups**

7

## Prevention (in general)

- Don't install software you don't need (uninstall what you don't use)
- Personal firewall
  - On your computer
  - For your home/office network (there is one built into most home routers)
- Don't plug in devices if you don't know what's on them (or where they came from)
  - Flash drives, CDs, floppies, …
- Use WPA2 for your wifi network. It is default on all new wireless routers.

- **Backups***

8

## Prevention – Social Engineering

- Some common scams to avoid:
  - Microsoft will never call you about a problem with your computer
  - No one will contact you to ask for help transferring money
  - Your friends probably aren't suddenly stuck in a foreign country asking for money
  - Asking you to use Western Union is probably a scam
  - Websites cannot tell if your computer is slow or has a virus
  - Commercial software shouldn't come from other sources and shouldn't be free

9

## Prevention - email

- Don't trust anything you aren't expecting
  - Don't click on links
    - Select, copy, paste
  - Don't open attachments you didn't explicitly request
  - If you get a link or an attachment from a friend that you didn't request, call them and ask if they meant to send it to you.
  - If you get a link from your bank saying "There has been a security issue please click this link" – DON'T
    - Your bank and all other providers will direct you to their website and offer phone support.
    - Do NOT click any links. Instead, enter the URL in the address bar directly.
  - Use Foxit PDF* reader instead of Adobe

10

## Prevention - email

- Spam
  - Think twice before giving your email address to websites
    - Use disposable email addresses any time you don't want to hear from the website again (or any of their advertisers)
  - Don't post your address
    - In google groups
    - In mail lists
    - On websites
    - If you need to post your address, modify it:
      - toby00@gmail.com = easy to find
      - My first name zero zero at gmail dot com = hard to find
  - Use an email service that offers good filters

11

## Prevention – Web

1. Use Chrome or IE10 or Firefox 19 (all latest versions)
   - Use the safe web surfing plugins from your Antivirus vendor (or try the WebOfTrust plugin)
2. Use Private Browsing Mode* for anything sensitive you might do
   - Banking, medical, etc…
3. DO NOT DO ANYTHING SENSITIVE FROM A PUBLIC HOTSPOT

- Don't ever give any website your email password.
- Don't click on pop-ups
- Look at the URL, if it looks weird*, DON'T CLICK IT
  - Weird; anything except: www.something.tla/….
  - Avoid .ru .cn .cm .cc .biz .ro
  - Test it here: http://www.virustotal.com/

12

## Prevention – Web

- Set up 2nd factor authentication on all your important sites (that offer it)
  - Your bank
  - Your password vault
  - Your email account:
    - Gmail
    - Yahoo mail
    - Hotmail
  - Facebook
  - Apple (iTunes, iCloud, etc…)
  - Dropbox
  - WordPress
  - **YOUR BANK**

13

## Prevention – Web

- Set up recovery options on all the websites that offer it
  - Via alternate email addresses
  - Via text messages
  - Via groups of trusted friends
  - With secret questions (MUST REALLY BE SECRETS!)
    - See Sarah Palin & Paris Hilton
- Configure "only use HTTPS" on any website that has one*
  - Google (default now)
  - Facebook

14

## Prevention - Social Media

- Don't say anything you wouldn't want the ENTIRE WORLD to know.
  - See Secret Questions (that aren't secrets)
- See Proper Attitude – you are the product, not the customer
  - Except for facebook games. For facebook games, you are the victim/addict
- Configure the privacy settings to be as restrictive as possible. Pay attention when they change
- Remember, every piece of information you post is valuable.
- Don't ever give any website your facebook password.

15

## Don't be a Problem

- The physical world
  - We expect people to cover their mouths when they sneeze
  - We discourage spreading rumors and gossip
  - There are legal requirements for protection of public health
- Online
  - Check on Snopes before you pass along rumors or gossip
  - Keep your system up to date and uninfected
  - When you get compromised warn people if there is a chance it could have spread to them.

16

## Detection

- Your Antivirus says something is wrong
  - The antivirus that you have installed on your computer.
    - (NOT a popup from a website)
- Your homepage suddenly changes
- Web pages suddenly start going to the wrong places
  - Especially offering free antivirus software, weird looking search pages, etc…

17

## Detection

- You get an announcement from a company you have service from.
  - You go to their website and it is confirmed
  - You check the URL and it is correct
- Friends tell you they are getting messages from you (that you didn't send)
- Your computer suddenly starts running really slowly.
- New software shows up that you didn't install

18

## Recovery - Preparation

- Test your backups and backup process before something goes wrong
  - Make sure all the data you want or care about
- Know how to change your passwords
- Have spare copies of critical information offline
  - Your secret questions
  - URLs that you don't want to have to memorize

19

## Recovery -You have BACKUPS, right?

1. Unplug from the Internet
2. Turn off your computer
3. Call your tech support person

- You will always have to:
  - Change (some of) your passwords
  - Make sure the computer is no longer infected
  - Undo all changes made by the attacker
    - Sometimes your antivirus software can do this for you
- You may have to:
  - Change all of your passwords
  - Completely wipe your computer
    - Reinstall all software from original media
    - Restore all data from backup

20

## References


- Creating passwords
  - *https://www.xkcd.com/936/*
  - *http://lifehacker.com/5830355/xkcd-password-generator-creates-high+security-easy+to+remember-passwords*
- Debunking Urban Legends online
  - *www.snopes.com*
- Source for ongoing updates of what criminals are doing online
  - *http://isc.incidents.org*
- LinkedIn Privacy Guide
  - *http://blog.eset.com/2011/06/22/linkedin-privacy*
- An excellent password vault that runs on everything
  - https://Lastpass.com
- Disposable emails:
  - *www.dispostable.com*
  - *www.mailinator.com*


21

## References

- Private Browsing Mode
  - http://browsers.about.com/od/faq/tp/Private-Browsing.htm
- Details on privacy settings for lots of social networking sites
  - www.mypermissions.org
- A good alternative to Adobe
  - http://www.foxitsoftware.com/Secure_PDF_Reader/
- The most dangerous domains
  - http://us.mcafee.com/en-us/local/docs/Mapping_Mal_Web.pdf
- HTTPS only mode
  - Gmail:
    - http://support.google.com/mail/bin/answer.py?hl=en&answer=74765
  - Facebook:
    - https://www.facebook.com/blog/blog.php?post=486790652130
  - Hotmail:
    - http://windowsteamblog.com/windows_live/b/windowslive/archive/2010/11/09/hotmail-security-improves-with-full-session-https-encryption.aspx

22

## References

- *Backup options*
  - Lots of software options
  - Online
    - Positives
      - Available from anywhere
      - Unlikely to be damaged/lost when the original is
    - Negatives
      - Slower & more expensive with large amounts of data
      - Can be compromised
      - Vendors go out of business all the time
  - *External hard drive (most come with backup software now)*
    - Positives
      - Fast and cheaper with large amounts of data
      - You know who has access to it
    - Negatives
      - If you leave it at home it may be lost/stolen/damaged when the computer is and you can't do backups when traveling
      - If you take it with you it may be lost/stolen/damaged when the computer is

23

## More Technical Security Options

- Review your session information
  - Many sites now allow you to see where you have connected from recently. Unless you travel a lot, the sources should all be similar
- Google Apps – use application passwords
- Selectively accept cookies
- Firefox – use security Plugins
  - NoScript
  - BugMeNot
  - HTTPS Only
- Use a VPN (Virtual Private Network) whenever traveling or at a public hotspot
  - www.strongvpn.com
- Use EMET from Microsoft
  - This is not for the faint of heart

24