Be Cyber Safe:
Protecting Yourself, Our Philanthropists, and Our Foundations in a World of Cyber Insecurity

John Hotta

Seattle Foundation Trustee

Wednesday, 24 February 2016

First: A Story

This is a time of Cyber Insecurity and Tech Disruption

Many Possibilities for Cyber Crime

- You
- Your Employees
- Your Philanthropists

Travel → Home → Foundation → $

Infected

Public WiFi

Old Home Router

Unmonitored Network

Infected: Downloaded Games and Apps

Why Cyber Insecurity?

- Lawbreaker Goals:
  - Financial Information
  - Identify Theft
  - Threats
- Lawbreaker Perspectives:
  - Individual Criminal
  - Organized Crime
  - Government

Lawbreaker Goal: Financial Information

- Examples:
  - Home Depot hack
  - Credit card skimming
  - ATM theft
- Credit card number
  - Value: approx. $100
- Everyone is a target
  - Our philanthropists are targets
  - You are a target because you have philanthropist information

Lawbreaker Goal: Identity Theft

- Examples:
  - Anthem Blue Cross hack
  - Social media hacks
- Social Security Number, name, and address
  - Open bank accounts
  - File tax returns
- Identity
  - Value: $100s to $100K
- Our philanthropists are targets
  - You are a target because you have philanthropist info
- Grandchildren are targets of identity theft

Lawbreaker Goal: Threats

- Examples:
  - Take over PCs; theft of photos and data
  - Hacking of corporate networks
  - Sony's *The Interview*
- Release of embarrassing or confidential information
  - e.g., emails; medical records, foundation and technology IP
- Threats
  - Value: $100s to $Millions
- Your wealthy and influential philanthropists are likely targets
  - You and Your Foundation are targets
- Your non-technical silver clients may receive threats (e.g., bail for grandchildren, etc.)

Lawbreaker Perspective:

Individual Criminal

Financial Info

- Least sophisticated and most likely
- Skim bank cards; bank card theft
- Send phishing emails

Identity Theft

- Watch social media postings
- Develop phishing sites
- Develop apps and games

Threats

- Unlikely unless personal motivation (e.g., disgruntled employees)

Lawbreaker Perspective:

Organized Crime

Financial Info

- Low-end, but high-volume foundation

Identity Theft

- Social-engineered theft via email, LinkedIn, and other social media
- Increasing number

Threats

- More sophisticated
- Attain healthcare and grandchildren info
- Growing likelihood for wealthy and influential philanthropists

Lawbreaker Perspective:

Government

Financial Info

- Not a focus area

Identity Theft

- By obtaining key identify information, a government can access:
  - Security info
  - Foundation IP
  - Technology IP

Threat

- Likely a target, if your philanthropist has technology IP or national security information

Foundation Response

Foundation Strategy: Improve Productivity

- Strategic goal: Improve productivity
  - Prevent cyber insecurity
  - Be resilient from cyber intrusions and business disruptions, including acquisitions
  - Improve technology adoption
  - …..Focus on clients

Foundation Response: People

- It's mostly about people
- Common-sense prevention for people:
  - Use unique passwords
    - Password method (i.e., Four-letter word; number/symbol combination)
  - Do not click links or open attachments in email
  - Automatic replies to known contacts only
  - Shred financial documents
  - Limit social-media apps
  - Check LinkedIn

Foundation Response: People and their Hardware

- Common-Sense Prevention for Hardware:
  - Update software
    - Plan for second Tuesday
  - Use firewalls
  - Remove viruses periodically
  - Choose your browser and set custom privacy and security settings
  - Do not plug-in portable storage devices
  - Turn off PC when not in use

Foundation Response: People and their Email

- Do not click on attachments
- Verify sender; Email identify theft

- Your email stories….

Foundation Response: IT

- Significantly limit access to IP, employee info, and philanthropist info
  - Separate servers
  - 10 – 20 – 70 guideline
- Monitor disgruntled employees and those who leaving
- Plan for backups
- Reconsider BYOD (bring your own device) hardware policies, including mobile phones
- Conduct penetration “pen” tests frequently
- Consider third-party monitoring of network

Foundation Response: IT and Legal

- Understand contracts with your:
  - IT provider
  - Cloud provider
  - Donation sites
  - Banking platform
  - Third-Party monitoring
- Monitor supply chain
- Hold contractors accountable for cyber-safe practices

Foundation Response: HR

- HR conducts and reinforces cyber training
  - Annual employee agreement?
- Monitor unhappy employees and poor supervision skills

Foundation Response: Board Discussion

- Who is responsible for cyber safety? CEO? COO? IT? HR?
- Is Cyber Security a full-board or committee responsibility?
- Does the full-board review and approve an annual security plan?
- Does management have the technology adoption competency in place?
- Does the board participate in an annual business disruption simulation?

Foundation Response: Practice

- Have the team assembled
  - Outside counsel
    - Outside counsel should have a relationship with regional FBI contact
  - Communications team
    - Communications team should include outside social media firm
  - CEO, CFO, CMO (Marketing), and board
- Practice response annually
  - Practice common scenarios
    - Lawbreakers access philanthropist information
    - Lawbreakers disrupt operations, including denial of service

You and Your Philanthropists

You and Your Philanthropists

- You
- Your Foundation
- Non-Tech Silvers
- Techie Silvers
- Grandchildren

You and Your Philanthropists

	Characteristics
You	• Use many devices and productivity tools
Your Foundation	• Use PCs, mobiles, WiFi, etc. • Slightly more secure and locked down
Non-Technical Silvers	• Use mobile and tablets • Use email • Use landline phones
Techie Silvers	• Very wired • Use many electronics and apps • Expect professional advisors to be cyber safe
Grandchildren	• Use mobile • Use social media, texting apps, and games

Productivity Tools to Manage

- Browsers
- Email
- Social Media
- Mobile Phones
- Bank Cards
- Home Router
- foundation Router
- Personal Hotspot
- Public WiFi
- Tablets
- PCs

Protecting You and Your Philanthropists

	Characteristics
You	• Personal MiFi? Yes. Public WiFi? No. • Password Manager? No. Password Method? Yes.
Your Foundation	• Turn off your computers daily • Update software frequently / monthly • Manage suppliers • Monitor network
Non-Technical Silvers	• Use iPhones and iPads • Local cyber-safe education: FTC's Pass It On
Techie Silvers	• New / updated routers
Grandchildren	• "Nothing is free" • Local cyber-safe education: OnGuardOnline.gov

Resources

Resources

Overview:

- Dept of Homeland Security: Cybersecurity
  - http://www.dhs.gov/topic/cybersecurity
- National Cyber Security Alliance
  - https://www.staysafeonline.org/

From Providers:

- https://www.apple.com/support/security/
- http://www.microsoft.com/security
- https://www.google.com/settings/security

Resources

For Your Foundation:

- US Computer Emergency Readiness Team
  - https://www.us-cert.gov/
- National Institute of Standards and Industry Cybersecurity Framework
  - http://www.nist.gov/cyberframework/index.cfm
- National Cyber Security Alliance
  - https://www.staysafeonline.org/

Resources

For Young Grandchildren and Non-Technical Silvers:

- U.S. Federal Government
  - http://www.OnGuardOnline.gov
- Federal Trade Commission Pass It On:
  - http://www.consumer.ftc.gov/features/feature-0030-pass-it-on

Appendix

Productivity Tools

- Browsers
- Email
- USB Ports
- Social Media
- Mobile Phones
- Bank Cards
- Home Router
- foundation Router
- Personal Hotspot
- Public WiFi
- Tablets
- PCs

Productivity Tool: Browsers

- Choose your browser:
  - Safari for Apple
  - IE for Microsoft
  - Foxfire as backup
  - Trusteer Rapport for banking sites
  - Do not download or use search bars (See Appendix)
- Use a different passwords for each site
  - Do not save passwords in browsers
  - Two- or three- layer authentication is good
- Set Security and Privacy Setting
  - Do not click OK on popups
    - Click on upper right square (See Appendix)
  - Non-technical silvers may need help setting up custom security and privacy settings

Productivity Tool: Email

- Do not click on links or attachments
  - Non-technical silvers may need consistent coaching
- Setup automatic reply to known contacts only
- Report phishing and junk
  - Tell friends when they have been hacked

Productivity Tool: USB Ports

- Do not use unknown USB drives
- When using most USB cords, AC/DC current and data are exchanged
  - Hence use electrical plugs
  - OR use a USB cord that only supplies electricity not data

Productivity Tool: Social Media

- Set custom security and privacy settings
  - Do not use defaults
- Do not accept invitations you don't know
  - Go to site to accept invitations; do not click links
  - Check profile is real
- When possible, setup screen names that are not your real name (e.g., I can be "joho")
- Do not list all information in profile (e.g., year of graduation; birthplace; residence address)
- Grandchildren may need additional, consistent coaching

Productivity Tool: Mobile Phones

- iPhone and Windows Phones are more secure
  - iPhones can be encrypted
  - Fingerprint on iPhone?
  - Move grandchildren to iPhones?
- Viruses can infect phones via games and apps
  - Nothing is free; on many phones, flashlight app takes a copy of your contacts
  - Apps may track keystrokes and location
- Turn off (or limit) location services
- Change settings so photos do not incorporate GPS
- Keep phone locked; if lost, be able to erase content

Productivity Tool: Bank Cards

- Use RFID shields
- Cover the keypad when entering your PIN
  - After transaction, hit multiple keys
- Do not sign your full name on POS terminals
- Use credit cards for online transactions
- Shred financial documents
- Before travelling internationally:
  - Change your PIN
  - Reset your PIN when you return home
- If phone is not infected, mobile payments may be more secure

Productivity Tool:

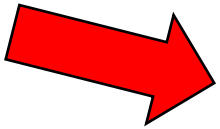
Home and Foundation Routers

- Update home router
  - May be a great gift for techie silvers
- Your foundation router and network may be a source of viruses
  - If your foundation is large, have a third-party monitor your network
- Limit access to:
  - Confidential IP
  - Employee information, and
  - Philanthropist information

Productivity Tool: Personal Hotspot

- Personal Hotspot = MiFi
- MiFi from AT&T, Sprint or Verizon
  - Landline telecoms have a history of following privacy laws
- When travelling internationally, consider bringing your own MiFi
  - Or rent MiFi from a reputable provider
- Do not use default MiFi name and passwords

Productivity Tool: Public WiFi



- Minimize use of public WiFi
  - When using public WiFi, use WiFi from historic landline telecoms
    - Landline telecoms have a history of following privacy laws
- Airport and hotel WiFi are targets for organized crime and governments
- When using “open” network at your foundation, remember information is not private
- Grandchildren may need consistent coaching about public WiFi

Productivity Tool: Tablets

- iPads are less prone to viruses
  - Closed system
    - Apps have been reviewed by Apple
  - Updates are downloaded automatically
- Download reputable games and apps
  - Games and apps may still take contact information
  - Nothing is free
- iPads may be the appropriate choice for non-technical silvers

Productivity Tool: PCs

- Update software frequently
  - Plan for second Tuesday updates
- Free firewall and updates:
  - Windows Defender or Windows Security Essentials
  - Remove viruses using Microsoft Safety Scanner periodically
- Do not plug-in portable storage devices
- Turn off computer when not in use
- When travelling internationally, consider an alternate PC
  - Remember change your passwords before leaving
- Grandchildren and non-technical silvers may need to be reminded consistently about games, browsers, and downloads

Summary Scenarios and Checklists

- Home and foundation
- Your Home
- Your Foundation
- Local (outside of Home or foundation)
- International Travel

Summary Scenario and Checklist:

Home & Foundation

- For your PC:
  - Update software; plan for second Tuesday
  - Use firewalls and update software
  - Remove viruses periodically
  - Choose your browser and set custom privacy and security settings
  - Do not plug-in portable storage devices
  - Turn off your computer when not in use
- Use unique passwords
- Do not click links or open attachments in email
- Automatic replies to known contacts only
- Shred financial documents

Summary Scenario and Checklist:

Your Home

- Update your home router
- For social media:
  - Set custom security and privacy settings
  - Accept invitations only of people you know; check profile is real
  - Do not list all information in your profile
- Move to iPhone or Windows Phone
  - Download only reputable apps & games
  - Turn off (or limit) location services
  - Turn off GPS information in photos
  - Keep phones locked

Summary Scenario and Checklist:

Your Foundation

- Your Philanthropists expect cyber-safe practices
  - Especially techie silvers
  - Significant reputational risk
  - Significant fines for disclosing PII (Personally Identifiable Information)
- Significantly limit access to IP, employee info, and philanthropist info
- Monitor disgruntled employees and those who leaving

Summary Scenario and Checklist:

Local

Outside of Home and foundation:

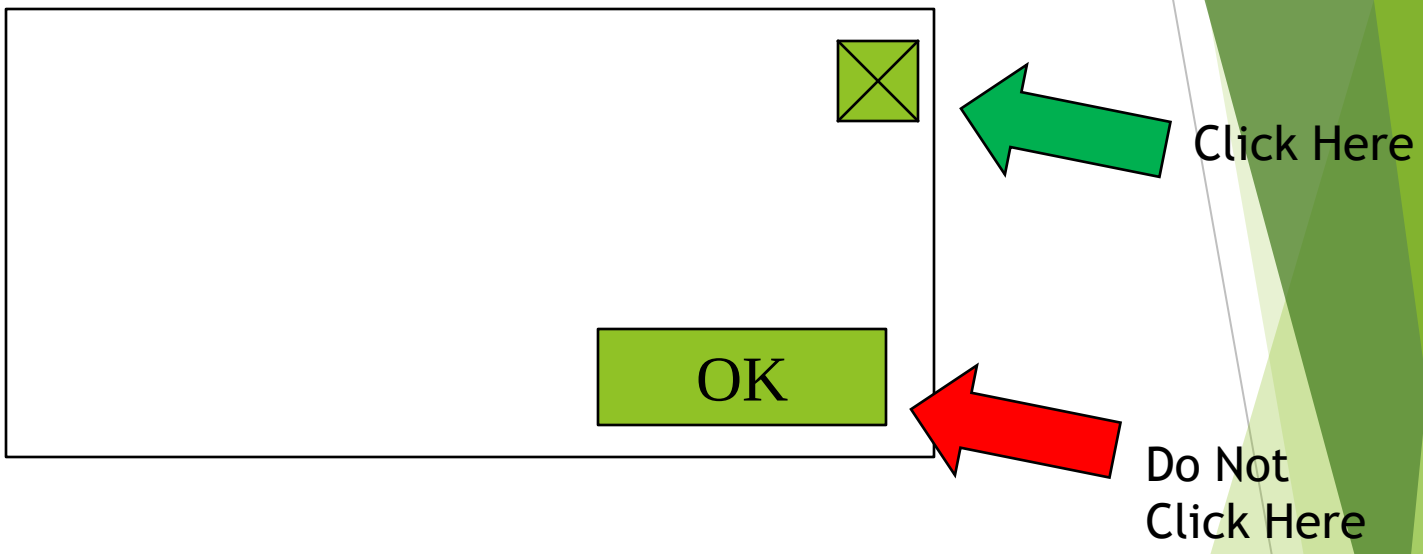
- Minimize use of public WiFi
  - Use MiFi from AT&T, Sprint or Verizon
  - Airport and hotel WiFi are targets for cyber criminals
- Do not charge via USB ports
- RFID shields for bank cards
- Do not sign your full name on POS terminals

Summary Scenario and Checklist:

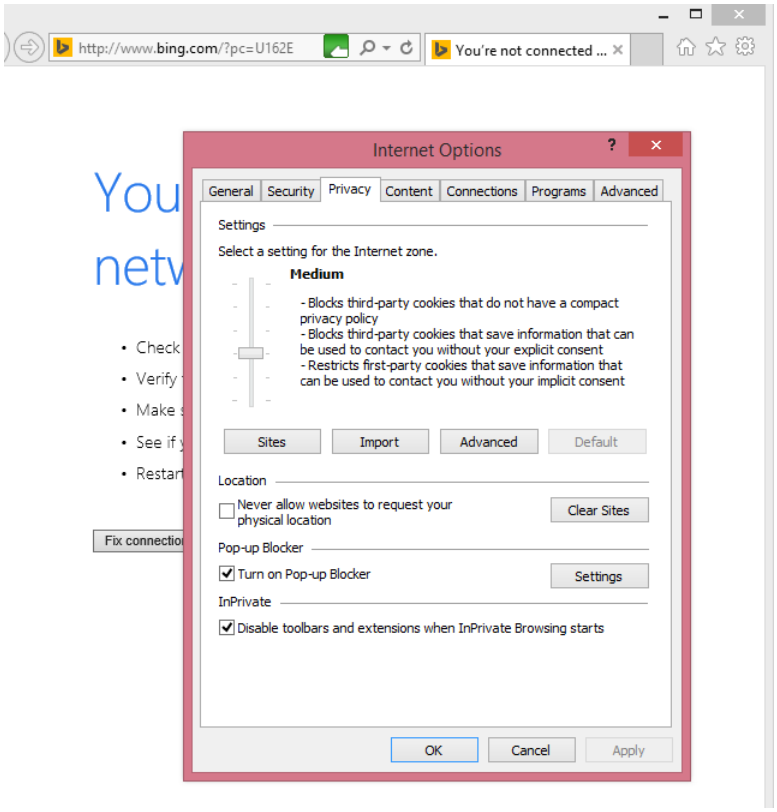
International Travel

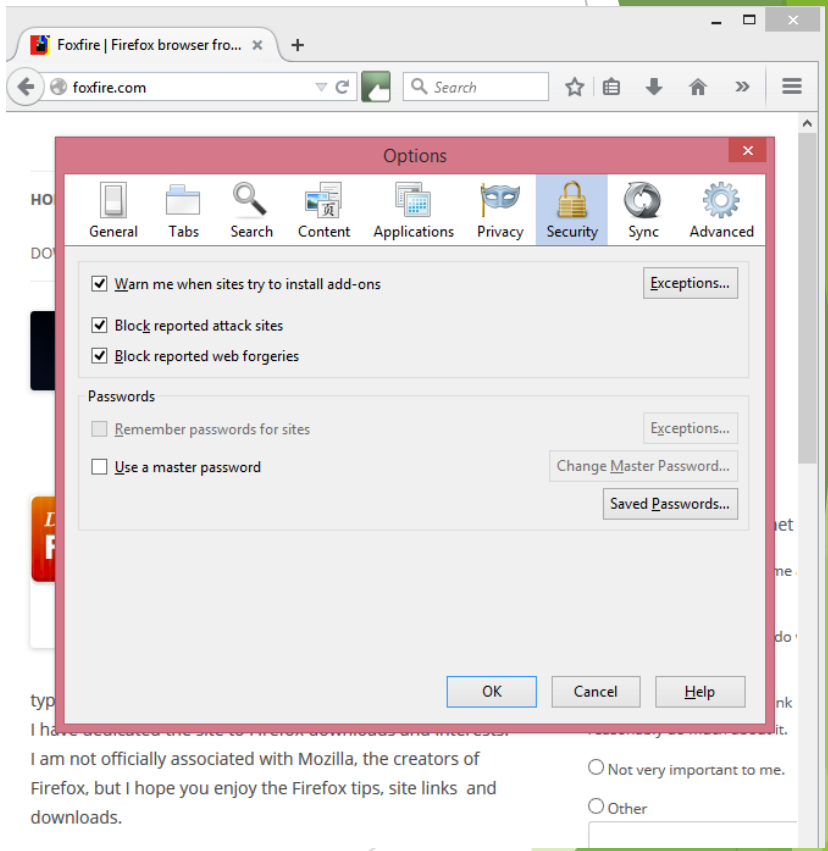
- Minimize use of public WiFi
  - Bring your own MiFi; change name and password
  - Airports and hotels are targets for cyber criminals
- Change your PINs and passwords before travelling
- Consider using alternate phones and laptops

Click on upper right of pop up boxes

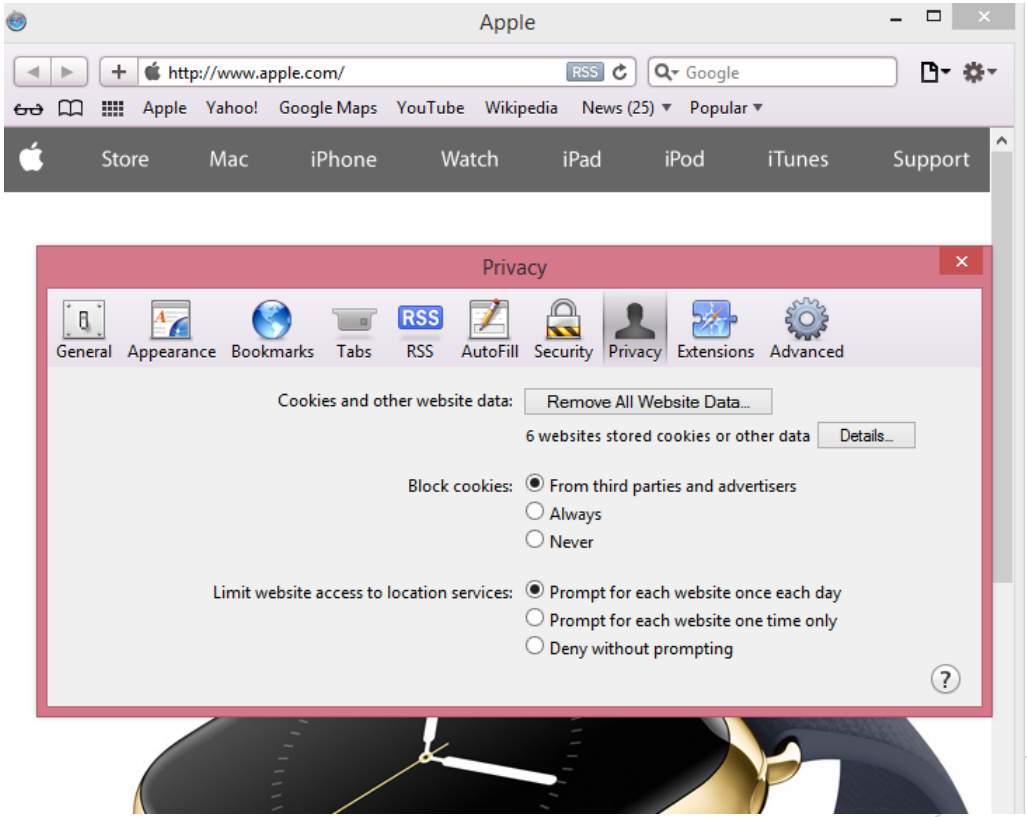


Set custom security and privacy setting





Set custom security and privacy settings



Do not download or use search bars

Contact Information

John Hotta

- johnhotta@hotmail.com's vCard:

Thank you for your time!

- To learn more, watch CSI: Cyber