Last Update: 8/2017 Expires: 8/2018

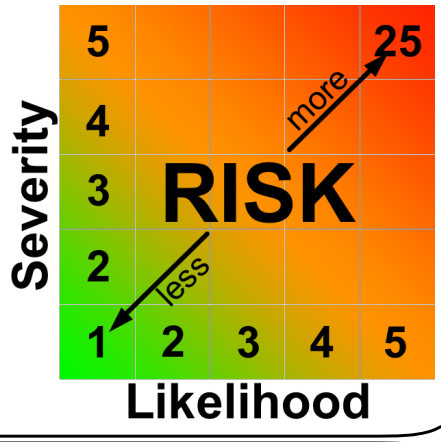
Electronic Frontiers Georgia
Protecting and Promoting Online Civil Liberties

web: https://ef-georgia.org
email: info@ef-georgia.org

Risk Assessment

1) Assets: What do I need to protect?
2) Adversaries: Who do I need to protect assets from?
3) Likelihood: How likely will I need to protect the assets?
4) Severity: How bad are the consequences if they get the assets?
5) Trade-offs: How far will I go to prevent the adversaries? (ex: time, money, convenience)

RISK = SEVERITY x LIKELIHOOD



Strategies

1) Contain - Isolate Inside / Outside
   - ex: Accounts, Networks
2) Harden - Only what you NEED for as long as NECESSARY
   - ex: minimize apps, browser plugins, users, accounts, features (WiFi, Bluetooth), sharing
   - Keep software current (enable auto-updates)
   - Install from reputable sources, ask:
     - Authentic?
     - Business Model? Free/Paid? “Free” services aren’t free, sometimes it pays to pay
     - Commitment? How specialized?
     - Is security a priority? How frequent are updates?
   - Sharing (location, photo, contacts), ask: why does THIS app need THIS info?

Key Takeaways

- Email: Prevent Phishing (Avoid links/attachments)
- Home WiFi: Configure strong password, disable WPS, update regularly
- Traveling: Public systems untrustworthy: Avoid public WiFi or use a VPN, avoid public computers
- Devices: Don’t leave unattended, set lock screens+passwords, only install what you NEED from reputable sources, update regularly
- Browsing: Use a password manager for unique, strong passwords across websites + multi-factor authentication
- Social Media: Beware what you share!

Last Update: 8/2017 Expires: 8/2018

@ Home

- Perimeter => Inward (Gateway => Devices)
- WiFi Contain + Harden
  - Use strong encryption
  - Configure strong unique passwords for internal & guests networks
  - Disable WPS, unused services (remote management, etc.)
  - Update frequently

Traveling

- DON'T leave devices UNATTENDED
- Treat public systems as untrustworthy
  - DON'T use open WiFi without a VPN
  - DON'T use public computers (ex: hotel lobbies)
- Travel with only the data you need
- DON'T have items in printers/fax

Devices

- Enable full disk encryption
- Enable lock screen + password
- DON'T JAILBREAK! Only install what you NEED & keep updated
- Separate Admin from User accounts
- Cover laptop camera/microphone
- User your own (trusted) peripherals/ accessories

Security Online

- Email
  - Avoid Phishing (Avoid links/attachments)
  - Avoid public away messages, Reply-All
- Browsing
  - Ensure sites use ENCRYPTION (https), plugin: HTTPS Everywhere
  - Disable: stored passwords, form auto-fill
  - Enable: prompts for: installs, enabling plugins

Data Security / Privacy

- Audit privacy settings with "privacy checkups", plugin: Privacy Badger
- Don't store credit card info on sites
- Don't sign-in to Chrome, Google or YouTube when browsing
- Use anonymous search engine (ex: DuckDuckGo)
- Use encrypted messaging (ex: Signal)
- Create secure, encrypted backups - protection from Ransomware

Social Media

- THINK before you SHARE: once online it's FOREVER
- Remove sensitive information or make private (birthday, maiden name, etc.)
- Avoid posting, tagging photos or location when away
- Avoid posting photos of valuables
- Separate accounts (family, work, interests)

Resources

Was my data exposed in a breech?
- https://haveibeenpwned.com

Keep current on security
- Krebs on Security Blog (https://krebsonsecurity.com)
- Electronic Frontiers Foundation (https://ssd.eff.org)
- SANS Institute OUCH! Newsletter (https://securingthehuman.sans.org/ouch)

Browser plugins
- HTTPS Everywhere
- Privacy Badger

Tools

- KeePassX - Password Manager
- Signal - Encrypted Messaging & Voice calls
- VPN (don't use a free one)

Reviews
- **https://thatoneprivacysite.net**
- **https://www.privacytools.io**

Privacy/Tracking "Checkups"
- **https://myactivity.google.com**
- **https://panopticlick.eff.org**

World Privacy Forum's Top Ten Opt Outs