Internet, Email and Smartphone Safety

Rob Falk, robfalk@robfalk.net

I. Being Safe Online

1) **Look for a Secure Wi-Fi Hotspot**
   a) Avoid open networks
   b) Secured networks are displayed with a lock (you will need a password to access.)
   c) In order of preference, choose networks secured with:
      i) WPA2-PSK(AES)
      ii) WPA2-PSK (TKIP)
      iii) WPA
      iv) WEP is a little better than nothing.
   d) Secured networks only protect you from outsiders.
   e) Maybe use your LTE/4G/3G connection
2) **Use HTTPS and SSL**
   a) Can protect you against eavesdropping and tampering with the contents of a site or the information you send to the site.
   b) provides some protection against an attacker learning the content of the information flowing in each direction
      i) the text of e-mail messages you send or receive through a webmail site
      ii) the products you browse or purchase on an e-commerce site
      iii) particular articles you read on a reference site.
   c) Look for the lock icon.
   d) Install "HTTPS Everywhere" for Firefox, Chrome & Opera. Not available for Safari.
3) **Use Open DNS**
   a) Replaces your Internet Service Provider's DNS with a free, safer, *faster* alternative.
   b) PhishTank – wisdom of the crowd
   c) DNS Server Addresses
      i) 208.67.222.222
      ii) 208.67.220.220
4) **Lock the Doors**
   a) Put Passwords on All Devices
      i) Consider using a longer password on your phone while crossing borders, and other high risk areas
   b) Turn off un-needed points of access
      i) Turn off File Sharing
      ii) Turn off Bluetooth

Internet, Email and Smartphone Safety

5) **Use a Good Lock!**
   a) Create a long password (12 or more characters)
      i) Use a combination of lower and upper case letters, numbers, symbols, and punctuation marks
      ii) Do NOT use real words!
      iii) NEVER use the same password for more than 1 site
      iv) Change your passwords every 6 months or so
   b) Password Managers
      i) Dashlane ($40/yr.)
      ii) LastPass ($12/yr.)
      iii) Sticky Password ($20/yr.)
      iv) Roboform Everywhere ($20/yr.)
      v) **1Password** ($50 one time)

      Be sure to leave your Password Manager password in your safe deposit box or other secure location where it will be found after your death!
   c) Use 2 Factor Authentication
      i) Standard Login
         (1) Something You Know: Username and Password
      ii) 2 Factor Login
         (1) Something You Know: Username and Password
         (2) Something You Have: phone, tablet, fingerprint
   d) See if your site has 2FA: 2factorauth.org
6) **Use Your Built-in Firewall**
7) **Keep Systems Up to Date**
   a) It's easy to be complacent. Pay attention:
   b) Once a Security Update is released, every hacker knows the vulnerability!
   c) Same for Phone Apps and OS
8) **Use Free Anti-Malware Apps**
   a) Computers
      i) Sophos Home
      ii) Malware Bytes
   b) Phones & Tablets
      i) Lookout
   c) Autodialed & Fraudulent Call Blocking
      i) Landline: nomorobo
      ii) Cell phone: Hiya and/or Truecaller apps
9) **Use a VPN**
   a) Private Internet Access ($40/yr.)
   b) TorGuard ($60/yr.)
   c) IPVanish VPN ($78/yr.)
   d) CyberGhost VPN ($40/yr.)
   e) HotSpot Shield Elite ($50/yr.)
   f) Anchor Free Hotspot Shield (Ad Supported)

Internet, Email and Smartphone Safety

II. Being Secure: If you lose your phone or computer

1) **Tracking and Recovery**
   a) iPhone, iPad & Mac: Find My iPhone
      Track it, Beep it, Lock it, Message, Erase It, Kill It
   a) Android: Device Manager
      i) Track it, Ring it, Lock it, Message, Erase it. A thief can reset your device and you won't be able to track it down
      ii) Avast Anti-Theft
   b) Windows Phone: Find My Phone
      i) Track It, Ring it, Send a Message, Erase. No kill switch
   c) PCs & Surface Tablets: Prey… and pray
2) **Encrypt your Hard Drive**
   a) Different from having a password on the device!
   b) Protects the hard drive, in or out of the computer
      i) Windows 7 & 8: BitLocker
      ii) Mac: FileVault

III. Being Smart, Part 1

1) **What Not to Do on Social Media Sites**
   a) Don't share personal information!
      i) Passwords
      ii) Credit Cards
      iii) Email Addresses
      iv) When you are or will be away
         (1) Be careful of revealing location data in photos and check-ins.
2) **What is Phishing?**
   a) Scam Email (or Web Page) intended to trigger a quick reaction from you.
   b) Common Characteristics
      i) Upsetting or exciting information
      ii) Demanding an urgent response
      iii) Asking you to "update," "validate," or "confirm" account information or face dire consequences.
3) **Don't Get Phished**
   a) Suspect any urgent requests for personal or financial information
   b) Contact the organization by using a phone number from a phone book or a bill.
   c) Never e-mail personal or financial information.
   d) Avoid embedded links in e-mails.
   e) Look for egregious grammar and spelling errors
   f) Do not open unexpected email attachments
   g) Look at a website's address line and verify if it displays something different from the address mentioned in the email.

h) Spot these favorite Phishing attempts:
   i) E-mail Money Transfer Alert: Please verify this payment information...
   ii) It has come to our attention that your online banking profile needs to be updated as part of our continuous efforts to protect your account and reduce instances of fraud...
      (1) Dear Online Account Holder, Access To Your Account Is Currently Unavailable...
   iii) Important Service Announcement from..., You have 1 unread Security Message!
   iv) We regret to inform you that we had to lock your bank account access. Call (telephone number) to restore your bank account.

i) Check with a reliable source:
   i) Google
   ii) Snopes.com
   iii) Scanurl.net
   iv) rob@whitecollarhandyman.com
   v) Install "Web of Trust"

IV. Being Smart, Part 2 – Common and Not So Common Sense

1) Be aware of your surroundings
2) Make sure no one is peering over your shoulder when you log into your computer, email, IM, or other accounts.
3) Avoid doing serious tasks like bill paying, accessing your bank account, or using credit cards when connected to public Wi-Fi.
4) Don't let your browser or sites you visit save your username or passwords.
5) Remove sensitive data before you leave home.
6) Never leave your laptop or handheld device unattended
7) Use the room safe if you're not taking it with you.
8) Don't automatically join the nearest network. Check with your host to confirm the network name and connection process
9) Put your name and local contact info on all devices when travelling
10) Don't use hotel or airport docking stations. Plug into the wall, with your own charger only.
11) Never connect an unknown USB flash drive to your tablet or laptop
12) Beware of Conference freebies
13) Don't leave your phone charging in a public conference room while you go for lunch.
14) Don't lend your phone to a stranger who needs to make a call.
15) Back up everything before you leave home.

Clickable list of links ☞ https://www.robfalk.net/helpful-links☜

More Secure Web Browsing:

HTTPS-Everywhere	https://www.eff.org/https-Everywhere
OpenDNS:	http://www.opendns.com

Password Managers:

Dashlane	https://www.dashlane.com
LastPass	https://lastpass.com
Sticky Password	https://www.stickypassword.com/free-vs-premium
RoboForm	http://www.roboform.com
1Password	https://agilebits.com/onepassword

2 Factor Authorization Information:

Two Factor Auth List	https://twofactorauth.org

Free Anti-Malware Apps

Malwarebytes	https://www.malwarebytes.com/antimalware/
Sophos Home	https://www.sophos.com/en-us/lp/sophos-home.aspx
Lookout	https://www.lookout.com/products/personal

Stop Autodialed & Fraudulent Calls

Nomorobo (landlines)	nomorobo.com
Hiya (cell phones)	Apple & Google App Stores, search “Hiya”
Truecaller	Apple & Google App Stores, search “Truecaller”

Virtual Private Networks (VPN):

IPVanish	https://www.ipvanish.com/why-vpn.php
CyberGhost VPN	http://www.cyberghostvpn.com/en_us
Hotspot Shield VPN	http://www.hotspotshield.com
Private Internet Access	https://www.privateinternetaccess.com

Find Lost Devices:

iCloud	https://www.icloud.com/#find
Avast Anti-Theft	https://www.avast.com/en-us/anti-theft
Prey Anti Theft	https://preyproject.com

Sniff Out Phishing and Scams:

Web of Trust	https://www.mywot.com
Snopes.com	http://snopes.com
Scanurl.net	http://scanurl.net

Tips, Tricks and Updates

Rob Falk
http://robfalk.net
✉ robfalk@robfalk.net
☏ (781) 989-2373
☏ (860) 595-2376

Newsletter Signup: https://www.robfalk.net/contact