Security & Privacy for Computer, Internet & Smartphone

RobFalk
Technology Concierge Services
Helping people enjoy and understand technology

www.robfalk.net | (781) 771-9447 | robfalk@robfalk.net

# I. Being Safe Online

**1) Look for a Secure Wi-Fi Hotspot (presently NO Wi-Fi is secure)**

- Avoid open networks
- Secured networks are displayed with a lock (you will need a password to access.)
- Secured networks only protect you from outsiders.
- Maybe use your LTE/4G/3G connection

**2) Use HTTPS and SSL**

- Can protect you against eavesdropping and tampering with the contents of a site or the information you send to the site.
- provides some protection against an attacker learning the content of the information flowing in each direction
- Look for the lock icon.
- Install "HTTPS Everywhere" for Firefox, Chrome & Opera. Not available for Safari.

**3) Use Open DNS**

- Replaces your Internet Service Provider's DNS with a free, safer, faster alternative.
- PhishTank – wisdom of the crowd helps you avoid bad websites
- DNS Server Addresses: 208.67.222.222 and 208.67.220.220

**4) Lock the Doors**

- Put Passwords on All Devices
- Turn off un-needed points of access like File Sharing and Bluetooth

**5) Use a Good Lock!** *

- Create a long password (12 or more characters)
  - Use a combination of lower and upper-case letters, numbers, symbols, and punctuation marks
  - Do NOT use real words!
  - NEVER use the same password for more than 1 site
  - Change your passwords every 6 months or so
- Password Managers

  Dashlane ($40/yr.) LastPass ($24/yr.) Sticky Password ($20/yr.)

  Roboform Everywhere ($20/yr.) 1Password ($36/yr)

*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!

**6) Use 2 Factor Authentication**

- Uses something you know: Username and Password and something you have: phone, tablet, fingerprint
- See if your sites have 2FA: 2factorauth.org

**7) Use Your Built-in Firewall**

**8) Wi-Fi & Network Router Tips**

- Change default network name a/k/a SSID
- Change administrator name & password
- Enable WPA2 Encryption
- Turn Off "Wi-Fi Protected Setup" a/k/a WPS
- Set up a Guest Network
- Visit GRC.com and test your security with "ShieldsUp!"

**9) Keep All Systems Up to Date**

- It's easy to be complacent. Pay attention!
- Once a Security Update is released, every hacker knows the vulnerability!

**10) Use Free Anti-Malware Apps**

- Computers: Sophos Home and Malware Bytes
- Phones & Tablets: Lookout
- Autodialed & Fraudulent Call Blocking:
  - Landline: nomorobo  Cell phone: Hiya and/or Truecaller apps

**11) Use a VPN**

| | | |
|---|---|---|
| Private Internet Access ($40/yr.) | TorGuard ($60/yr.) | IPVanish VPN ($78/yr.) |
| CyberGhost VPN ($40/yr.) | HotSpot Shield Elite ($50/yr.) | Nord VPN ($69/yr.) |
| Cloak ($100/yr.) | Anchor Free Hotspot Shield (Ad Supported) | Opera VPN (free*) |

# II. Being Secure: If you lose your phone/computer

**1) Tracking and Recovery**

- iPhone, iPad & Mac: Find My iPhone
  - Track it, Beep it, Lock it, Message, Erase It, Kill It
- Android: Device Manager
  - 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
  - Avast Anti-Theft
- Windows Phone: Find My Phone
  - Track It, Ring it, Send a Message, Erase. No kill switch
- PCs & Surface Tablets: Prey… and pray

**2) Encrypt your Hard Drive**

- Different from having a password on the device! It protects the hard drive, in or out of the computer.
  - Windows: BitLocker  Mac: FileVault

# III. Being Smart, Part 1

**1) What Not to Do on Social Media Sites**

- Don't share personal information! Passwords, credit cards, e-mail addresses, or when you are or will be away
- Be careful of revealing location data in photos and check-ins.

**2) What is Phishing?**

- Scam Email (or Web Page) intended to trigger a quick reaction from you.
- Common Characteristics

- Upsetting or exciting information
- Demanding an urgent response
- Asking you to "update," "validate," or "confirm" account information or face dire consequences.

**3) Don't Get Phished**

- Suspect any urgent requests for personal or financial information
- Contact the organization by using a phone number from a phone book or a bill.
- Never e-mail personal or financial information.
- Avoid embedded links in e-mails.
- Look for egregious grammar and spelling errors
- Do not open unexpected email attachments
- Look at a website's address line and verify if it displays something different from the address mentioned in the email.
- Spot these favorite Phishing attempts:
  - E-mail Money Transfer Alert: Please verify this payment information...
  - 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...
  - Dear Online Account Holder, Access To Your Account Is Currently Unavailable...
  - Important Service Announcement from..., You have 1 unread Security Message!
  - We regret to inform you that we had to lock your bank account access. Call (telephone number) to restore your bank account.
- Check with a reliable source:

  Google Snopes.com

  Scanurl.net robfalk@robfalk.net
- Install "Web of Trust"

# IV. Being Smart, Part 2: Common & Not So Common Sense

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

# V. Resources

**For a Clickable List of Links, visit https://www.robfalk.net/helpful-links**

**More Secure Web Browsing:**

| | |
|---|---|
| HTTPS-Everywhere | https://www.eff.org/https-Everywhere |
| OpenDNS: | http://www.opendns.com |
| ShieldsUp!: | https://www.grc.com/x/ne.dll?bh0bkyd2 |

**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 |
| Avast Security | https://www.avast.com |
| 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):**

| | |
|---|---|
| Nord VPN | https://go.nordvpn.net/aff_c?offer_id=15&aff_id=9208&url_id=263 |
| IPVanish | https://www.ipvanish.com/why-vpn.php |
| CyberGhost VPN | http://www.cyberghostvpn.com/en_us |
| Private Internet Access | https://www.privateinternetaccess.com |
| TorGuard | https://torguard.net |
| Cloak | https://www.getcloak.com |
| Opera VPN (free*) | http://www.opera.com/computer/features/free-vpn |

**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 |

For questions and more information,
or to sign up for the newsletter mailing list,
please contact **Rob Falk** at:
www.robfalk.net|
(781) 771-9447| robfalk@robfalk.net