



# PRACTICING “SAFE COMPUTING” AT HOME

WILLIAM (THE GONZ) FLINN

*M.S. INFORMATION SYSTEMS SECURITY MANAGEMENT; COMPTIA SECURITY+, I-NET+, NETWORK+; CERTIFIED PATCHLINK ENGINEER*

ENTERPRISE INFORMATION SYSTEMS SECURITY MANAGER

[HTTP://WWW.GONZOGARAGE.NET](http://www.gonzogarage.net)

[BILL@GONZOGARAGE.NET](mailto:bill@gonzogarage.net)

@COLORADOPREPPER



# INTRODUCTION

- Cyber-Security at home is every bit as important as at work, especially in our era of the “Internet of Things” and high rates of identity theft.
- Many instances of identity theft and computer infections can be prevented by practicing “safe computing.”
- A few simple “computer hygiene” techniques can help keep you safe.
- Being a “safe and smart user” is often the most important step in keeping you safe online.
- The need to keep your home network safe goes beyond computers and smartphones – consider all of your “IoT” devices.

# AGENDA

- Keeping Your System Up to Date
- Antivirus Programs
- Other Security Tools
- Using Secure Passwords
- Using accounts with least privilege
- Avoiding Email Hacks, Scams, and Phishing
- Bogus Tech Support Phone Calls
- Web Browser Safety
- Securing Your Home WiFi Network
- Using an Online Backup Service
- A Word About The Internet of Things (IoT)
- Demonstration



# KEEPING YOUR SYSTEM UP TO DATE

- Regularly install patches and updates.
- Set updates to “Automatic” where possible.
- Update all of your applications, not just the operating system.
- Set your antivirus signature/definition updates to automatic.
- Don’t ignore the “update needed” notifications!

# ANTIVIRUS PROGRAMS

- Make sure that you have one installed.
- Check to make sure that antivirus definitions are up to date.
- Set it to automatically scan regularly.
- Check for warnings and alerts.
- Many AV tools are multi-feature packages that have ability to also address performance, parental controls, and personal firewall settings.

# ANTIVIRUS PROGRAMS AND FEATURES

Windows Defender Security Center

☰

🏠

🛡️






📄

📅

👤

## Your device is being protected.

Last threat scan: 8/15/2018  
Last threat definition update: 8/14/2018  
Last health scan: 8/15/2018

				
<b>Virus &amp; threat protection</b> No action needed.	<b>Device performance &amp; health</b> No action needed.	<b>Firewall &amp; network protection</b> No action needed.	<b>App &amp; browser control</b> You're using recommended settings.	<b>Family options</b> Manage how your family uses their devices.

Windows Defender Security Center

☰

## 👤 Family options

Get what you need to simplify your family's digital life.

### Parental controls

- 🛑 **Help protect your kids online.**  
Choose which websites your kids can visit as they explore the web using Microsoft Edge.
- 🕒 **Set good screen time habits.**  
Choose when and how much time your kids can use their devices.
- 📊 **Keep track of your child's digital life.**  
Get weekly activity reports of your kids' online activity.
- 🛒 **Let your kids buy appropriate apps and games.**  
Choose what they see and purchase for their devices.


[View family settings](#)

### See your family's devices at a glance

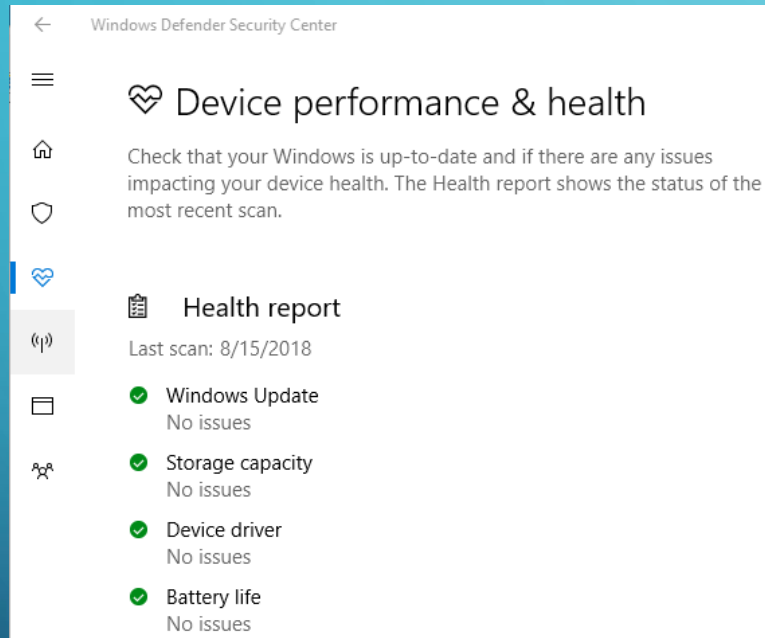
- 📱 **Check the health and safety of your family's devices.**  
Make sure they're up-to-date and see device security and health status.

[View devices](#)

Not all features are available in all markets.



# ANTIVIRUS PROGRAMS AND FEATURES



Windows Defender Security Center

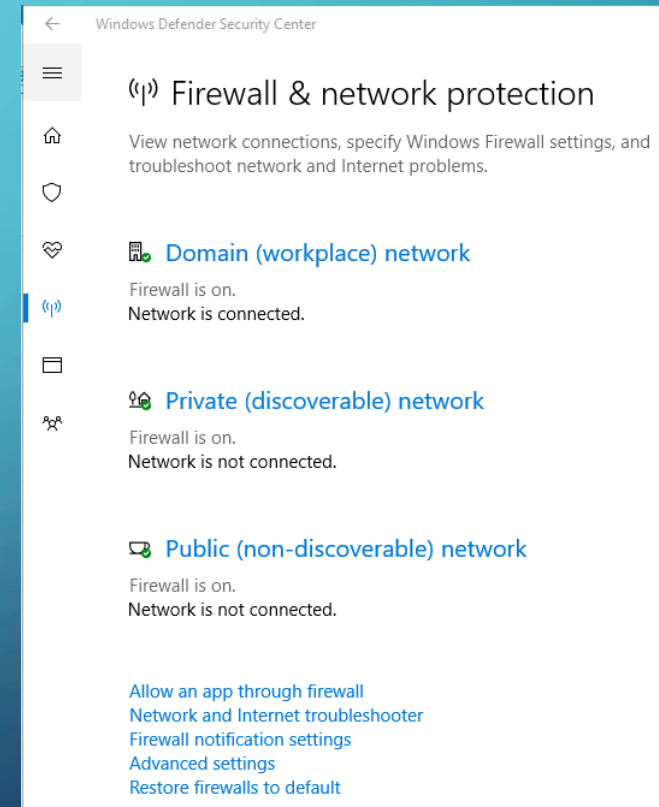
Device performance & health

Check that your Windows is up-to-date and if there are any issues impacting your device health. The Health report shows the status of the most recent scan.

Health report

Last scan: 8/15/2018

- Windows Update  
No issues
- Storage capacity  
No issues
- Device driver  
No issues
- Battery life  
No issues



Windows Defender Security Center

Firewall & network protection

View network connections, specify Windows Firewall settings, and troubleshoot network and Internet problems.

Domain (workplace) network

Firewall is on.  
Network is connected.

Private (discoverable) network

Firewall is on.  
Network is not connected.

Public (non-discoverable) network

Firewall is on.  
Network is not connected.

[Allow an app through firewall](#)  
[Network and Internet troubleshooter](#)  
[Firewall notification settings](#)  
[Advanced settings](#)  
[Restore firewalls to default](#)

# OTHER SECURITY TOOLS

- Personal firewall (Windows Firewall or one provided by your AV suite)
- Periodic scans with other anti-malware tools
  - Stinger
  - Norton Power Eraser
- WiFi router firewall
- Taking advantage of the “free” tools provided by your ISP
- Other maintenance tools such as “DEFRAG” and “Disk Cleanup”



# USING SECURE PASSWORDS

- Passwords should be at least 12 characters
- Passwords should be complex and not made up of common words
  - Bad: dog
  - Good: d0NtTr3admE#!
  - Better: n4xK1&95\$H\*StN#
- Passwords should not be the same on every site that you use (especially financial or healthcare sites)
- Change passwords often
- Using a password manager
  - Dashlane (Ranked #1 by [ConsumerAdvocate.Org](#))
  - Roboform
  - Keeper

# EXTRA USERNAME/PASSWORD SECURITY

- You might want to consider extra security for banking, credit card, PayPal, and healthcare, etc websites.
- Use two-factor security on websites and services that support it.
- Use a strong username as well as a strong password.
  - Make both username AND password complex.
    - Username: M2rtyM00se#!
    - Password: n4xK1&95\$H\*StN#
  - Don't use the same username on every website requiring extra security.
- When entering password “hints” – make the answers obscure, not the real answer (This is how Sarah Palin's email got hacked).

# USING ACCOUNTS WITH LEAST-PRIVILEGE

- Never surf the web on your computer when you are logged in with a username that always has full administrative control.
  - Malware often operates in the context of the logged on user.
- Use “User Access Control” (UAC).
- Have a separate username for regular use, and a separate username for administrative functions.

# AVOIDING EMAIL HACKS, SCAMS, AND PHISHING

- Use an email client instead of keeping all emails and your contact list online.
- Use “Preview” mode to see email contents without actually opening the message.
- Hover over links in email messages to see where they go before clicking.
- Do NOT click “unsubscribe” links to get off of email lists from unknown senders.
- If you get a message telling you to log into your account, don’t click on the link.
  - Go to the known web address in your browser and log in that way and see if they have any notifications for you there.

# EMAIL CLIENT – PREVIEW MODE

The screenshot displays an email client window with the following components:

- Menu Bar:** File, Edit, View, Go, Message, Events and Tasks, Tools, Help.
- Toolbar:** Get Messages, Write, Chat, Address Book, Junk, Delete, Reply, Reply All, Reply to List, Tag, Quick Filter, Search <Ctrl+K>, CardBook.
- Left Panel (Folders):** 1 - Comcast, Inbox (15), Drafts, Sent, Junk, Trash (95), 1 - Bills, 2 - From Me, Affiliate Tools, Affiliate Accounts (Gun Digest, LASR, Lucky Gunnar, USCCA), Marketing Tools, Web Development, AMAC, CERT Team, Devotionals, Express Toll, Family, Healthcare (Blue Cross Blue Shield, Tricare, JJ Storage, Job Search, PayPal, Retirement - DFAS, US Law Shield, USAA).
- Message List:** A table with columns for Subject, Date, and Correspondents. The selected message is "Your support fuels our 20,000 Sentinel Activists" from Tim Chapman, dated 4:15 PM.
- Message Header:** From: Tim Chapman, Subject: Your support fuels our 20,000 Sentinel Activists, To: William Flinn.
- Warning Message:** A yellow box with a red border containing the text: "To protect your privacy, Thunderbird has blocked remote content in this message." with an "Options" button.
- Message Body:** William,  
I'm forwarding you a great story of how our Heritage Action Sentinels are holding Congress accountable to conservative principles at the local levels.  
This story below shows how Sentinels are leaders in their communities and in the grassroots fight to advance conservative policy. Sentinels, such as Matt Long and Angela Smith, are critical to our shared mission to hold elected leaders accountable and enact

# HOVERING OVER LINK OF LEGITIMATE EMAIL



**Preview and try out the updates to Wells Fargo Online®**

We're improving the *Wells Fargo Online* experience to help make it easier for you to get your banking done.

The fresh look features easier navigation and quick access to your most frequent activities, such as checking your accounts, paying bills, and more.

Take a look at the new design by clicking the link below:

<http://connect.wellsfargoemail.com/a/hbxs2y4b8ih4bb9ow0cntrvgnqb/bodycta>  
Click or tap to follow link.

1. **Sign on** to your account.
2. From the **Account Summary** tab, select the **Give it a try** link in the blue box.
3. Follow the directions to manage your account information in the new design.
4. Tell us what you think by selecting the **Give Feedback** button at the top of the page.

**Note that your accounts will reflect any transactions and activity that you complete during the preview period.**

# HOVERING OVER LINK OF MALICIOUS EMAIL



## Preview and try out the updates to *Wells Fargo Online*®

We're improving the *Wells Fargo Online* experience to help make it easier for you to get your banking done.

The fresh look features easier navigation and quick access to your most frequent activities, such as checking your accounts, and more.

Take a test <http://www.russianmafia.ru/stealyourmoney/forgodssakedontdick/>

Click or tap to follow link.

1. [Sign on](#) to your account.
2. From the **Account Summary** tab, select the **Give it a try** link in the blue box.
3. Follow the directions to manage your account information in the new design.
4. Tell us what you think by selecting the **Give Feedback** button at the top of the page.

**Note that your accounts will reflect any transactions and activity that you complete during the preview period.**

# BOGUS TECH SUPPORT CALLS

*“This is the Windows Department (or “Microsoft” or some other vague service name), my name is “Ralph” (in their best attempt to disguise the foreign accent) and I’m calling about your computer. Your computer is being reported to us (but they can’t tell you by whom) as having malicious software and we need to fix it right away!”*



# BOGUS TECH SUPPORT CALLS

- The call starts by them having you do some simple commands that show you “errors” and “warnings” from your computer’s event viewer.
- They then want to charge you to fix problems that don’t exist.
- They also attempt to steal personal information.
- If you give them your credit card number, then they’ll have that, too.
- They attempt to get you to allow them to connect to your computer and take control:
  - To steal files.
  - To install malicious software.
  - Damage your computer in another way so that you have to pay again to have it fixed.

# BOGUS TECH SUPPORT CALLS

- Microsoft will never call you!
- Do not give them any information over the phone!
- Do not follow their instructions.
- Do not let them take control of your computer.
- Hang up!

# WEB BROWSER SAFETY

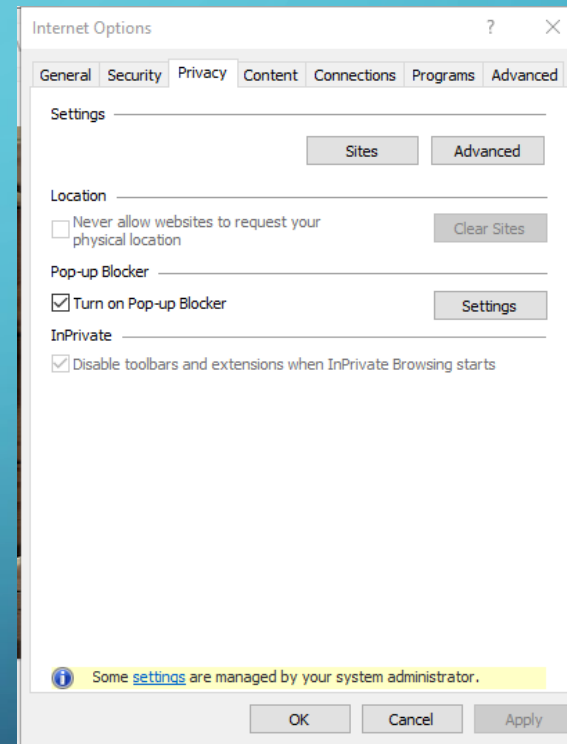
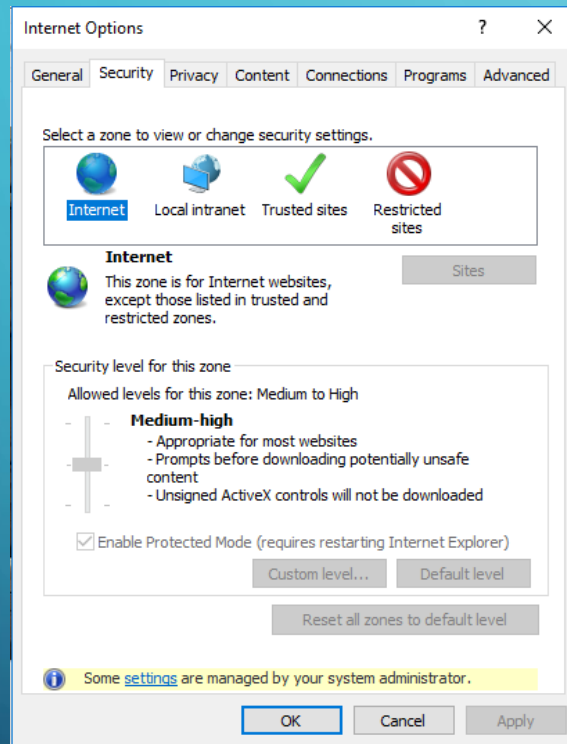
- Use an alternate web browser with good security and privacy rankings.
- Use and configure a pop-up blocker.
- Set security levels for zones (Internet, Trusted Sites, etc).
- Ensure “https” and “secure” (or the padlock) are displayed when accessing websites that collect information

# WEB BROWSER COMPARISONS

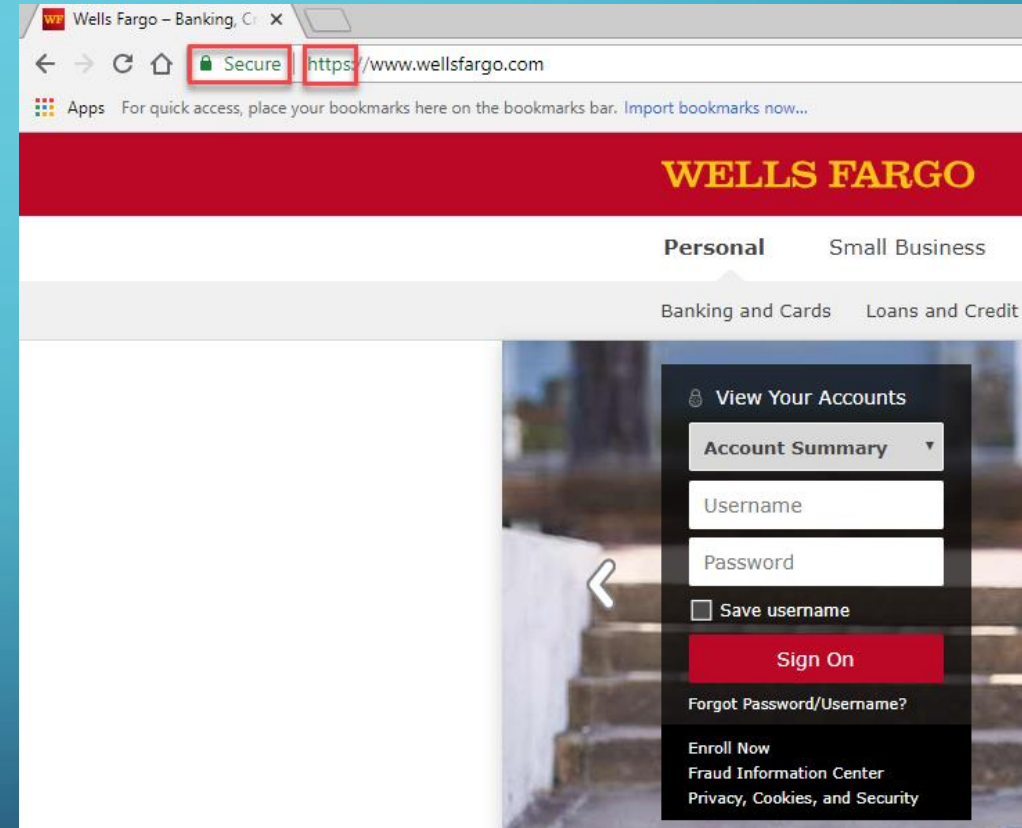
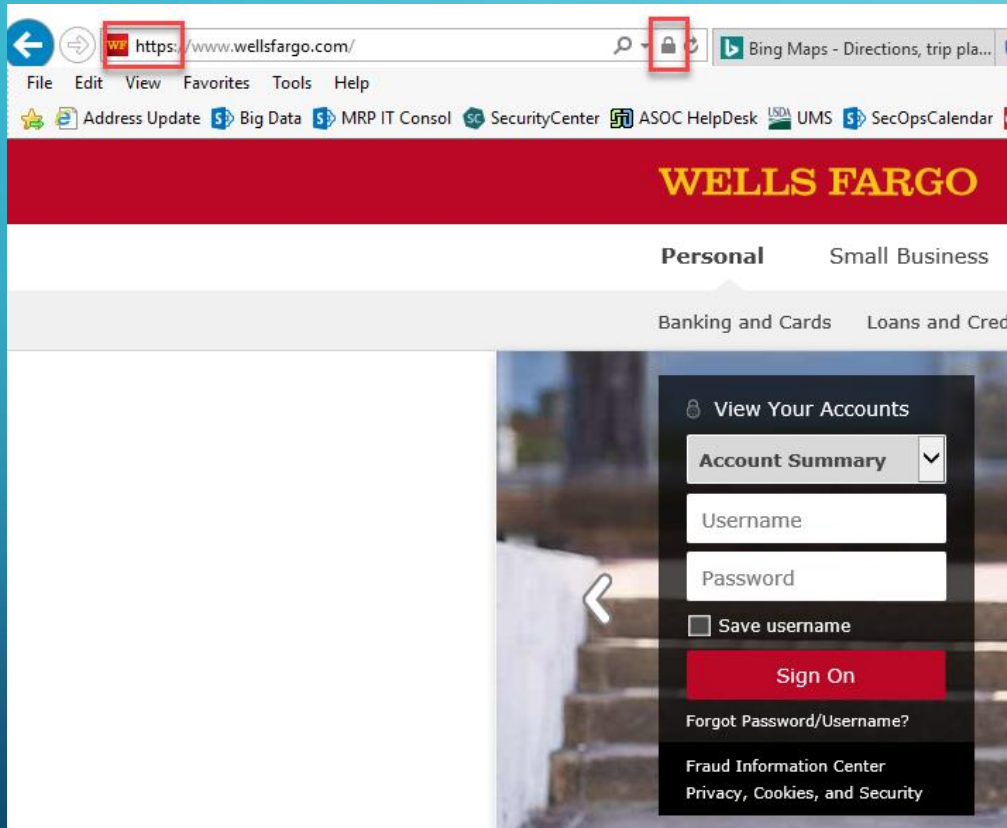
Browser	Version	Security	Privacy	*Browserscope
 Chrome	53	The Best	The Worst	16/17
 Firefox	49	Okay	The Best	15/17
 Opera	40	Very Good	Good	16/17
 Edge	38	Good (Tentative)	Okay	N/A
 Safari	10	Good	Okay	15/17
 IE	11	The Worst	Okay	14/17

- Source: <https://tiptopsecurity.com/what-is-the-most-secure-web-browser/>
- Browserscope Coparison: <http://www.browserscope.org/?category=summary&v=top>

# WEB BROWSER SECURITY – SECURITY SETTINGS



# WEB BROWSER SECURITY – RECOGNIZING A SECURE WEBSITE



# SECURING YOUR HOME WIFI NETWORK ROUTER

- Change administrative username and password from defaults.
- Set SSID and WiFi password to complex values.
- Change WiFi password regularly
- Set firewall security levels, if available.
- Configure security logging on your WiFi router.
- Monitor periodically to see who is connected to your network.
  - Xfinity, for example, has an app to alert you when a new device connects to your WiFi router.

# ADVANCED WIFI ROUTER SECURITY

- Allow router administration **ONLY** with a wired (LAN) connection – no wireless connections.
- Make SSID name complex
- Disable SSID broadcast
  - Users will then have to know **BOTH** the SSID and password to connect.
- Set MAC access lists to only **ALLOW** certain devices to connect.
  - Block all, allow by exception
- Use third-party router firmware to allow more granular configuration and to send router logs to SANS.



# WHY USE AN ONLINE BACKUP SERVICE?

- Google Cloud, OneDrive, Carbonite, Idrive.
- Can be automated to backup constantly or as configured.
- Files are stored off-site on a secure service.
- Files and computer configurations can be easily transferred to a new computer in case of computer failure, disaster, or theft.
- You can access your files through a web browser if you are away and need a file while using another computer or your smartphone/tablet.

# THE INTERNET OF THINGS (IOT)

- Smart TVs
- Nest Thermostats
- Alarm Systems
- Video Cameras
- “Alexa”
- Refrigerators
- Garage Door Openers
- Smart Locks
- These things connect to your home network.
- They all have vulnerabilities.
- They can all be configured securely or incorrectly.
- If compromised, all have the ability to give outsiders information about you.
- Some can even give an intruder the ability to break into your home!
- They all spy on you ;)

# LIVE DEMONSTRATIONS

- Setting Windows Backup
- Antivirus Program Settings
- Using additional AV Scans (Stinger/Power Eraser)
- Using Two-Factor Security
- Hovering Over Links in Emails
- WiFi Router Configurations



# REFERENCES AND ADDITIONAL RESOURCES

- US-CERT: Home and Business
  - <https://www.us-cert.gov/home-and-business>
- Basic Computer Security: How to Protect Yourself from Viruses, Hackers, and Thieves
  - <https://www.howtogeek.com/173478/10-important-computer-security-practices-you-should-follow/>
- US-CERT: Avoiding Social Engineering and Phishing Attacks
  - <https://www.us-cert.gov/ncas/tips/ST04-014>
- US-CERT: Home Network Security
  - <https://www.us-cert.gov/ncas/tips/ST15-002>
- US-CERT: Before You Connect a New Computer to the Internet
  - <https://www.us-cert.gov/ncas/tips/ST15-003>
- Security Tip: Hover Over Links Before You Click
  - <http://www.brucebnews.com/2016/08/security-tip-hover-over-links-before-you-click/>
- Krebs on Security: Password Do's and Don't's
  - <https://krebsonsecurity.com/password-dos-and-donts/>
- Top Ten Tips for Wireless Home Network Security
  - <https://www.lifewire.com/wireless-home-network-security-tips-818355>

