



INTERNET SECURITY

Internet Security - Protecting your computer from cyber-attacks includes properly setting up your web browser. Join SeniorNet's Zoom web seminar to learn how to secure your computer from attacks via the Internet such as identity theft and scams. Discussion includes anti-virus software, firewalls, malware, phishing, private browsing, and security settings for MS Edge, Firefox, Google Chrome, and Apple's Safari.

➤ **Modems, Routers and Firewalls**

- The modem is the device that brings the internet into your home by sending and receiving data.
- The router is a separate machine that takes the information from the modem and allows it to be accessed by many different devices.
- Personalize your Router's password >
 - To log into your router > <http://192.168.1.1>, you will need your password!
 - To find your router's IP address > advanced students only!
 - [Find Router IP Address \(19216811ip.host\)](#)
 - To find a default password >
 - [Default Router Passwords \(19216811ip.host\)](#)
- The firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules, therefore prevents untrusted data from ever reaching your computer.
- Neither firewalls, routers, nor anti-virus software can protect against phishing scams; nor clicking on an inappropriate link especially in pop-ups.

➤ **Protect Your Computer & Malware Countermeasures**

- Ensure your Firewall, Anti-Virus, and Browser programs are up to date.

➤ **Update your browser**

- Settings > Automatic updates – varies with browser program
- Double-check your typing when entering web addresses
- HTTPS and the "Green" padlock – encrypted vs. secure



INTERNET SECURITY

➤ **Browser Set-Up**

- Window's Microsoft Edge will automatically update with your Windows updates.
- Firefox Menu (3 bars "hamburger") > Settings > scroll down to "Firefox Updates" > Allow Firefox to: "Automatically install updates (recommended)". Close and relaunch to complete action.
- Google Chrome (3 Dots "ellipsis")
 - Default is to automatically update when closed and restarted
 - If "More" appears in the menu line, then you need to update.
 - 3-dots (ellipsis) > Settings > About Chrome for version and update
- Apple's Safari - When Software Update says that your Mac is up to date, then macOS and all its apps are up to date, including Safari, Messages, Mail, Music, Photos, FaceTime, Calendar, and Books.

➤ **Cookies**

- Block only third-party cookies
 - Firefox – Privacy and Security > "Standard" setting
 - Edge - "Block third-party cookies"
 - Chrome: Privacy and security > Cookies ... "Block third-party cookies"

➤ **Private Browsing**

- Does not store browsing data on your local computer, but your Internet Service Provider (ISP) will have this information.

➤ **Anti-Virus Programs**

- Always ensure your Anti-Virus is enabled and set to automatically update

➤ **Devious Internet Scams**

- Phishing
- Charitable Collections
- Opening Attachments in Emails



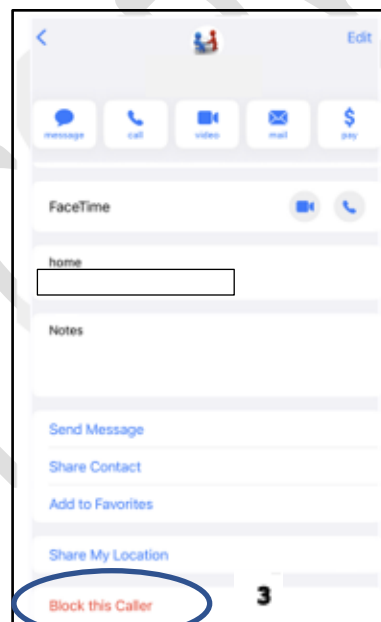
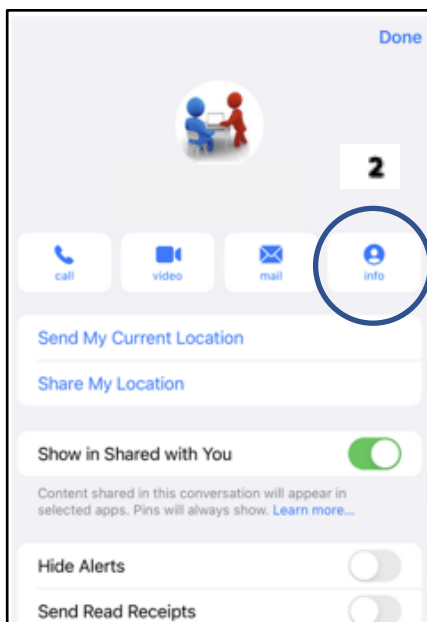
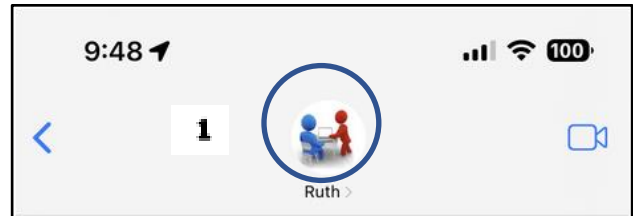
INTERNET SECURITY

➤ Smishing – Phishing via Texts

If you see a link in a suspicious text message, don't click on it.

iPhone – *displayed in screen shot*

- Click on Icon of Sender
- Click on “i” in little circle
- Scroll down to Click “Block this Caller”



Android -

- Tap a message that you want to block.
- Tap the three-dot menu at the top right of the screen.
- In the drop-down menu, choose "Details."
- On the Details page, tap "Block & report spam."

➤ Verify a legitimate email address: Email Verifier in any browser.

<https://verify-email.org/>

SeniorNet – a Program of Family Service League

www.seniornetli.org • www.fsl-li.org • www.facebook.com/seniornetfsl • FSLseniornet@fsl-li.org • 631-470-6757



INTERNET SECURITY

➤ **Virtual Private Networks (VPNs)**

- Deal with responsible vendors
- “Free” doesn’t give you the security you think it does.
- Where is it located? What permissions is it requesting?
- Check reviews.

➤ **Identity Theft**

- Deal with responsible vendors
- Use credit responsibly
- <https://haveibeenpwned.com>
- <https://cybernews.com/personal-data-leak-check/>
- Are you giving out too much “truth”?

➤ **Password Essentials**

- Passwords should be at least 8 characters long.
- Passwords need to contain special characters such as @#\$%^& and do not use the forward or back slash as that is an instruction to the computer “/” or “\”
- Passwords should not have any common words such as “123”, “password”, “your birth date”, “your login name” and any words that can be found in the dictionary.”
- Include a variation of upper- and lower-case letters.
- Security questions – the truth may be your enemy.
- Use Two Factor Authentication (2FA) when possible.
- Do not reuse your passwords, especially for financial accounts.
- Consider a password manager.
- eWallet by iliumsoft.com for local or 1password for cloud based.

To contact the teacher directly: sandie.seniornet@gmail.com



The Computer Help Desk supports students’ classroom Learning, provides guidance with Windows and Computer Operations, and advice on selecting the computer for your needs.

www.seniornethelp@gmail.com

1 (631) 629-5426

SeniorNet – a Program of Family Service League

www.seniornetli.org • www.fsl-li.org • www.facebook.com/seniornetfsl • FSLseniornet@fsl-li.org • 631-470-6757