Online Security Handout

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

• Lock your devices, like your tablet and phone: You lock the front door to your house, and you should do the same with your devices. Use strong passwords to lock your tablet and phone. Securing your devices keeps prying eyes out and can help protect your information in case your devices are lost or stolen.

• Think before you act: Ignore emails or communications that create a sense of urgency and require you to respond to a crisis, such as a problem with your bank account or taxes. This type of message is likely a scam.

• When in doubt, throw it out: Clicking on links in emails is often how bad guys get access to personal information. If an email looks weird, even if you know the person who sent it, it's best to delete it.

SHARE WITH CARE

• What you post will last forever: Be aware that when you post a picture or message online, you may also be inadvertently sharing personal details with strangers about yourself and family members – like where you live.

• Post only about others as you would like to have them post about you: The golden rule applies online as well.

• Own your online presence: It's OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite websites.

BROWSE SMART

- Always double-check the URL of your banking site, social networking site, and e-mail site before you log in.
- Type in the URL by hand, and to never follow links from an e-mail.
- Check for HTTPS instead of the less-secure HTTP.
- Most browsers now include a color-change on the left side of the location bar to indicate that the site has been verified as legitimate.

SOCIAL MEDIA SAFETY

- Use caution when you click links!
- Know what you've posted about yourself.
- Don't trust that a message really is from whom it says it's from.
- Type the address of your social networking site directly into your browser.
- Do not allow social networking services to scan your e-mail address book.
- Everything you post to the Internet is permanent.
- Be careful about installing extras.
- Be selective about who you accept as a friend.

PASSWORDS

- Make passwords strong: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- Write it down and keep it safe. Keep a list that's stored in a safe, secure place away from your computer or use a Password manager.

According to the traditional advice—which is still good—a strong password:

- Has 12 Characters, Minimum.
- Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters.
- Isn't a Dictionary Word or Combination of Dictionary Words.
- Doesn't Rely on Obvious Substitutions
- Passphrases are better than passwords.
- Passkeys are stronger than passphrases.

BROWSERS

All Browsers Are Not Created Equal!

Rank	Browser	Security	Privacy
1	**Brave Browser**	5/5	5/5
2	Tor Browser	5/5	4.5/5
3	**Mozilla Firefox**	4.5/5	5/5
4	**Chromium**	4.5/5	5/5
5	Apple Safari	4/5	4.5/5
6	Google Chrome	4/5	1/5
7	Opera	3/5	1/5
8	Microsoft Edge	2.5/5	2/5

RESOURCES

Computer Booters	https://computerbooters.org
GeezerTek	http://geezertekaz.com
GFCLearnFree -	https://edu.gcfglobal.org/en/topics/onlinesafety/
Google Safe Browsing Check -	http://google.com/safebrowsing/diagnostic?site= "site address"
Passphrase Generator -	https://randompassphrasegenerator.com/
Password Strength Test -	https://www.my1login.com/resources/password-strength-test/

Top Online Financial Scams Targeting Seniors (National Council on Aging)

- Medicare/health insurance scams
- Counterfeit prescription drugs
- Funeral & cemetery scams
- Fraudulent anti-aging products
- Telemarketing/phone scams
    - The pigeon drop
    - The fake accident ploy
    - Charity scams
- Internet fraud
    - Email/phishing scams
- Investment schemes
- Homeowner/reverse mortgage scams
- Sweepstakes & lottery scams
- The grandparent Scam

Top VPN Providers – Techradar

(https://www.techradar.com/uk/vpn/best-vpn)

VPN Name	Country Jurisdiction	Total Servers	Countries
ExpressVPN	British Virgin Islands	3000+	94+
NordVPN	Panama	5000+	61+
Surfshark	Netherlands	3200	100
IP Vanish VPN	United States	900	60
Norton Secure VPN	United States	1500	200
PureVPN	Hong Kong	2000	180

Top Internet Security Suites - TechRadar.com

(https://www.techradar.com/news/best-internet-security-suites)

- Bitdefender Total Security
- Kaspersky Total Security
- McAfee LiveSafe
- Symantec Norton Security Premium
- BullGuard Premium Protection
- Trend Micro Maximum Security
- Avast Internet Security
- Panda Dome Advanced
- AVG Ultimate
- F-Secure Total

Top Password Managers – Investopedia.com

(https://www.investopedia.com/best-password-managers-5080381**)**

- **Dashlane –** Best for Extra Security Features https://www.dashlane.com/
- **LogMeOnce –** Best Multi-Device Platform https://www.logmeonce.com/
- **BitWarden –** Best Free Option https://bitwarden.com/
- **RememBear –** Best for New Users https://www.remembear.com/
- **1Password –** Best for Families https://1password.com/
- **Keeper –** Best Enterprise-Level Manager https://www.keepersecurity.com/

YouTube Videos

- Understanding Spam and Phishing https://youtu.be/NI37JI7KnSc
- What is Ransomware? https://youtu.be/LmPRKyKECv8
- What is digital tracking? https://youtu.be/6EHSlhnE6Ck
- How to create a strong password. https://youtu.be/aEmF3Iylvr4
- Password Managers https://youtu.be/hneBN4bgEfo
- How To: Protect yourself online. https://youtu.be/ILHZkxIQK4Q

- Your Browser's Security Features https://youtu.be/2ZZQlgV2Gus
- What is Private Browsing https://youtu.be/4FHPSnMzlRo
- How To Stop Spam Calls, Emails, & Texts https://youtu.be/e8xwUN8TWwY
- What's a VPN & How Does It Work? https://youtu.be/_wQTRMBAvzg
- Secure Search Engines https://youtu.be/GtsPZE5592I
- What are Passphrases https://youtu.be/XIySPpFHJCo
- What is Two-Factor Authentication? (2FA) https://youtu.be/AMOtB7XkTT4

How Can I Avoid a Phishing Scam?

Your best defense against phishing scams is being a well-informed user. Here are some ways you can help avoid a phishing scam.

- **Stay alert for suspicious emails and text messages:** Do you know the sender? Were you expecting an email from this person? Does the email fit in with your job role? Be suspicious if the sender is soliciting personal information.

- **Be suspicious of email attachments and links:** Never open email attachments or click link addresses in emails from parties you don't know, and always double-check email addresses when it appears as if the email is from a known party. Opening email attachments or clicking links can install malware on your computer without your realizing it.

- **Use strong passwords:** Never use the same password for any of your accounts, and make sure to update your passwords on a regular basis. Many attacks happen due to exposed passwords. Use long, secure passwords that include letters, numbers and special characters.

- **Use a password manager:** Use a password manager to create and remember passwords. The primary purpose of every good password manager is to **generate, store, and help you manage passwords**. Password managers also ease your life by allowing **autofill** on trusted devices.

- **Consider using a Virtual Private Network (VPN):** A VPN routes your internet traffic through an encrypted tunnel, keeping all your online activities safe from prying eyes. A VPN also hides your real IP address, ensuring that it is not linked to your real location or your identity.

How to Manage Your Privacy Settings

- Want to view or change your privacy/security settings, but don't know where to find them? National Cybersecurity Alliance provides a list of direct links to update your privacy settings to over 80 popular devices and online services.

https://staysafeonline.org/resources/manage-your-privacy-settings/