The Four Most Critical Cybersecurity Steps – Start this Journey Today

Here are four foundational cybersecurity steps that can make profound improvements to your security!
You don't need to have perfect security. Just make it strong enough that criminals move on to easier targets.
Security is a journey. Start today with small steps and improve over time. Commit to small steps each month!

1) Apply Security Updates/Patches: Keep your Operating System and other software updated/patched for ALL your devices (computers, smartphones, network, etc.) (i.e. install "Windows Updates" or "Security Updates").
- If your device is so old that it can't be patched/updated (i.e. it is out-of-support), then replace it!!
- Set your devices to "auto-update" if possible, otherwise check manually once per month.

2) Install a Password Manager program, which will store and encrypt all your passwords.
- Passwords for all important accounts (email, financial, online shopping, social media, etc.) must be **long**/strong and must be **unique** (either 16+ random characters or 20+ passphrase/words).
- With a Password Manager you only need to remember one long master password to access all your account passwords, which are stored with strong encryption. These programs can (1) create a long, random password for each account, (2) store them, and (3) automatically log you into your website accounts.
- Some recommended Password Manager programs: Proton Pass, NordPass, Dashlane, or KeePassXC.
- Don't reuse passwords on multiple accounts!
- Don't keep passwords in a Word, Excel, or Note file. (A handwritten password list is more secure.)
- Don't let your web browser store your passwords; these are easy for any hacker to steal.
- The only place you should electronically store passwords is in a reputable Password Manager program.
- Password Managers can prevent you from entering credentials in a "look alike" fake web-page.
- Many password managers will monitor the Dark Web and alert you if any of your passwords have been leaked online
- See this link for help choosing and implementing a Password Manager: computersecuritynw.com/password-managers

3) Implement Two-Factor/Multi-Factor Authentication (2FA/MFA) on every important account (including email, financial, shopping, social media, etc.)
- MFA can be done in several different ways: using (1) SMS/Text messages (ok), (2) an Authenticator app (very strong), or (3) YubiKeys (strongest).
- Best for most people: Download an Authenticator App on your smartphone from your App store (such as Google Authenticator or Microsoft Authenticator). If that seems too difficult or you want to do that later, then start by using the SMS/Text message method.
  - **Note**: Make sure to record the "backup" codes given to you when setting up each account with an authenticator; you will need these if you lose your phone. Print them out or store them in your Password Manager.
- At minimum, use your phone number to receive a SMS/text message as your MFA code.
  - **Warning**: Hackers run schemes to steal cell phone numbers (thus intercepting these texts) or trick you into giving them these codes; this could give crooks access to your financial & other accounts. Be aware!

4) Resist Scams/Social Engineering! Your actions can be the most insecure part of strong computer security. Cyber criminals are trying to fool you into giving them access to your accounts or to steal your money. Be on guard! Don't think you are immune from these schemers whose full-time job is to trick you!
- Be suspicious of phone calls you did not initiate. When in Doubt: **Hang Up, Look Up, & Call Back**.
- Be very suspicious of unexpected emails and SMS/Texts; don't respond to random text messages!
- Never open attachments or click on website links in emails or texts messages from people you don't know! And be cautious about unexpected attachments & links from people you do know (who might be hacked).
- Never click a link or call a number sent to you via email/text, even if you believe it is legitimate. Just login to your accounts via your normal method.
- Never give out a Text "verification code" (or PIN) to anyone! (Unless you initiated the call to a known company with a verified phone number). Your bank will not randomly ask you to confirm the numbers they just texted to you! E.g. "Please confirm you're a real person by sending this code." Don't!
- Don't believe a website pop-up that tells you that you have a virus, an outdated program, and urges you to "click here" or "call this number" to clean/update. Do normal updates on your already-installed, trusted antivirus program.
- Some signs of social engineering: Urgent response required, confirm/deny a $ transfer you did not initiate, cancel a subscription (you don't have), respond or your account will be canceled, asking for payment by gift cards, traveling relative needs cash, etc. (See for more details: www.computersecuritynw.com/phishing)