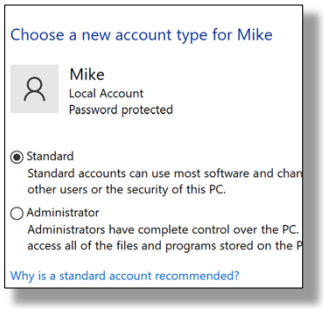
Prioritized Cyber Security Steps for Family Computers

🟢 Less effort and still provides substantial value

🟡 More advanced and adds even more value

🔴 More work and more effective

1. 🟢 **Passwords: Enable two-step verification** on PayPal, LinkedIn, Dropbox, Facebook, and every other web service you use. Look for variations of Settings > Security on the websites.
2. 🟢 **Aggressively apply critical security updates to the Operating System, Browsers, Java, and your PDF Reader.** For family computers, configure Microsoft's and Apple's products to apply security updates automatically. You might need to apply updates to browsers, Java, and your PDF reader manually. Always perform a new backup before installing updates. Patch your hardware devices too.
3. 🔴 **Be sure to change your user account type to "standard"** on your local computer to help block attackers from taking over your computer. The settings are in Control Panel. Steps: 1) Create a new user as a local account. Name it something like "Superhero" 2) Change that user's account type to be a local administrator 3) Change your account type to standard. Now use your account. Mac users can create standard users too.



4. 🟡 **Clone your computer's hard drive.** In addition to the file backups you already make, create frequent clones from the computer's hard drive to external USB hard drives. If your computer misbehaves or seems infected, you can use the clone to restore your computer's hard drive to effectively reset the computer to how it was when you most recently cloned it. Disk cloning tools for Windows include Microsoft's System Image Creation feature, ShadowProtect Desktop from StorageCraft, and Acronis True Image. For Macs, options include Carbon Copy Cloner from Bombich Software, Acronis True Image, or SuperDuper! Check version compatibility. Time Machine is always compatible, and it is possible to boot into recovery mode, but it's not a clone.
5. 🟢 **Reconsider using Public Wi-Fi.** Public Networks are terrible for your security. Connect your laptop to your phone or personal hotspot instead.

If you have any questions, please call: Michael Foster
CISA Certified IS Auditor, CISSP Certified IS Security Professional, CEH Certified Ethical Hacker
805-637-7039
mike@fosterinstitute.com

6. 🔴 **Use excellent web content filtering.** Some people use OpenDNS, CloudFlare for Families, or Quad9.net to help automatically stop some attacks. If you have Internet family protection services, they might already have a feature to block malicious websites, and you won't need these. These services are free for home users, there is nothing to install on your computer, and the sites have tutorial videos.
7. 🟢 **Uninstall Java.** Attackers can exploit Java to hack computers, so it is best to remove Java unless an essential website you need requires Java. You can download a fresh version from java.com
8. 🟡 **Uninstall every program & application that is not essential to you.** Every application on your computer creates a potential toe-hold for an attacker to use to get into your system.
9. 🟢 **Use anti-virus** suites that include a software firewall. Microsoft Defender is an option. Find reviews at www.av-test.org. Always install the anti-virus and firewall before connecting a new computer to the Internet. Enable Apple's Firewall.
10. 🟢 **Passwords: Use a password manager to remember your passwords.** Avoid using the same password on more than one website. Password managers help remember passwords and might be a safer place to store passwords than in your browser.
11. 🟢 **Physical Security:** Keep doors closed and locks locked. Secure your computer and phone, as well as all memory sticks and backup drives. It is best if your computer is not visible through a window.
12. 🟢 **Encrypt your data.** In case a bad actor steals your computer or a USB storage device, encrypt drives with Microsoft's BitLocker, VeraCypt, or Apple's FileVault2.

Dashlane
LastPass
1Password
Keeper
RoboForm
Many more…

These recommendations are for <u>family computers.</u> Protecting an organization's IT security is far more involved. Please tell your IT Professionals that you appreciate them even more than ever. They often don't get noticed until something terrible happens.

- **The Foster Institute performs cybersecurity reviews and audits.**
- **Streamlining and saving money in IT too.**
- **So executives can sleep better at night.**

If you have any questions, please call: Michael Foster
CISA Certified IS Auditor, CISSP Certified IS Security Professional, CEH Certified Ethical Hacker
805-637-7039
mike@fosterinstitute.com