

# Surf Safe

---

## 1. Use a safe platform

Some computers are inherently safer than others. Perhaps even more important, bad people play the odds and will focus their evil actions on the largest targets. Break-ins today are driven by money. It must be worth the time, resources, and possible punishment to steal stuff. Here is my ranking of platforms.

- a. Linux is safest. It is free and stable, but has the fewest users. It used to be very complicated to install and run. Both issues have been fixed. Printing is still difficult.
- b. Smartphones and tablets are next. The chips are not as powerful as those used by desktop machines, and the operating systems are more modern. Besides pictures, they generally don't have a large number of files that might be economically valuable to others.
- c. Apple desktop platforms run on a form of Linux that is very stable and hard to break into. Additionally, Apple does not allow the user to mess with settings in many respects. It's the Apple way or no way.
- d. Windows desktop platforms are the most dangerous. First, there are more Windows users than any other operating system, so there are lots of opportunities to steal. Also, users can unknowingly change settings, often adding more risk. Windows XP is radioactive and must not be used! Because it is no longer being updated by Microsoft, the bad guys know they can penetrate a WinXP box, using vulnerabilities no longer being fixed.

Regardless of where they rank, all platforms are safe when you follow the advice below.

## 2. Use a router

Routers put an electronic wall between your computer, tablet, or smartphone and the Internet. Any traffic not specifically requested is "routed" into the dumpster. Stand-alone routers cost about \$50-75. Today, most cable and phone companies put a router in with the modem box they give or rent to you. Modern routers provide both wired and wireless output. You can run a cable from the router to your computer, or you can send it over the air by wireless signals. If you have wireless in your home, always protect it by a password. This prevents the neighbor across the street from using your Internet. It also keeps a bad guy from driving through the neighborhood looking for opportunities to break into your home network.

## 3. Never run as administrator

Over 90% of break-ins would never happen if this rule was obeyed! The Administrator has super powers over the computer to change settings and install/remove apps. Unfortunately, the default for a single user is to assign her an admin account. So malicious payloads are allowed to run and wreak havoc. The solution is fairly easy. Add a new user through the control panel. Call that new user Administrator or Superuser and give it admin privileges. A common password for this new

# Surf Safe

---

user is “root”. (It doesn’t need to be strong.) After saving, log out and log back in as the new Superuser. Modify your original user account by changing the privileges to normal. Keep the same password. Save and log out. Now log in as the original user and you are protected.

## 4. Look before clicking

Links in e-mail and web sites can be disguised to look like they come from a friend! Hover over the link and see if the address shows up at the bottom of the screen. Don’t click until after you have studied it. If it looks weird (spelling errors, crazy claims) it probably is. If you haven’t done number 3 above, the link you clicked will download a program to infect your machine. If you are a normal user, not admin, the computer will ask you for a password before running the malicious bundle of code. Exit right away by holding in the power button. Reboot to flush out any remaining bad stuff. Help your friends out by converting documents to pdf before you attach them to your e-mail message. These files cannot run as code.

## 5. Keep anti-virus updated

Stand-alone programs, like McAfee and Norton and Symantec, are generally not worth the price you must pay each year to keep them fresh. All malware has a unique fingerprint, called a signature. When new viruses are found, the AV companies add that signature to the database. The virus can then be blocked. These signatures must be updated at least twice a month. But the AV programs also interfere with normal operation of your computer, slowing things down and causing lock-up. Windows users have a free substitute that works just as well. Under Win7, it is called MS Security Essentials. It must be downloaded from Microsoft.com and installed by you. Win8 and Win10 has it built in and called Windows Defender. The signature files for both Microsoft programs are automatically updated for free once a day. Apple does not provide (or) need AV.

## 6. Practice good password safety

Many on-line sites use a username and password combination to prove the connection is really you. Thieves steal these login databases from banks and stores and sell them on the black market. If you use the same password on many different sites, they not only have your Target credentials, but also those for Fred Meyer, Bank of America and wherever else you conduct financial transactions. Never reuse the same password! Good passwords should be 8-16 characters long. If you write them all down somewhere, they will probably be stolen. The solution is free and easy – use a password manager app to remember everything. You remember one master password to start it going, and the app fills in the username and password fields on all your private sites for you. Last Pass is the best. Because banks are such rich sites for thieves, you should proactively change those passwords every six months. 12-20 character passwords are advised here. Last Pass

# Surf Safe

---

handles this easily. It can also do an “audit” of all your existing accounts to find weak and duplicate passwords. It’s free for desktop machines and \$10/year for mobile devices. Bargain.

## 7. Install updates for operating system and applications

Not only does this reduce those annoying crashes, it makes your computer safer. Windows, Apple, and Linux all have automatic updating capabilities. Use them. Smartphones and tablets will also auto-update installed apps whenever you are on wireless. (When installing new apps, download them only from the official Apple (iOS) or Google (Android) sites. This assures the apps are safe and not malware in disguise. Avoid programs from Adobe (like Reader) and Oracle (like Java and Flash); they release bad code and make updating difficult.

## 8. Ask for help

Before pressing keys and really messing things up, go online (on a different machine if possible) to do a Google, Yahoo, or Bing search. Chances are, others had the same problem. They shared their solutions. Or contact your friends. Now that I am retired, feel free to contact me by e-mail ([dennisarter@gmail.com](mailto:dennisarter@gmail.com)) or text message (509.783.0377). Sometimes I may even pick up a voice phone call (509.783.0377). I never charge friends for help. Like a medical doctor, it is hard to diagnose a problem over the telephone; I may have to come to your home.

## 9. Thoughts on the new Windows 10

Until recently, Microsoft targeted corporations for their strategic focus. The Windows operating system (the part that actually runs the computer) was stable after XP was released (circa 2000). Windows 7 built on that stability and business interest. But forces all around the world, especially in North America and Asia, were causing Microsoft to question this corporate emphasis. Social networking exploded with the development of the Apple smartphones and tablets. People didn’t need a desktop machine any more. They were always on the Internet and could communicate instantly with friends and associates all around the world through Facebook, Twitter, and other apps. Windows 7 could not compete with this global change in personal relationships.

So Microsoft rolled out Windows 8, their first operating system with touch squares to do things. Since most desktop monitors didn’t have touch control and nobody was buying Microsoft smartphones or tablets, the market rejected Win 8 and Microsoft was forced to release Win 8.1 with a more classic look and feel. (The touch squares were still there for those wishing to click them with a mouse.) Windows 8.1 is really the strong and stable Windows 7 underneath.

But Apple and Android (Google) were cleaning Microsoft’s clock for younger and hi tech corporate users. Everything was networked and sharing was easy. Hard drives are no longer needed when we can store gigabytes of data (files) in the cloud for free. The top dogs at

# Surf Safe

---

Microsoft had to respond to this massive shift among younger users and rich, well-funded businesses. So they came out with Windows 10 for these new needs. Windows 10 assumes you are always connected to the Internet. It assumes you are in a business where most employees have Microsoft phones and Surface tablets. You need to provide resources for your employees with these portable devices. They want to discuss projects and resources wherever they are in the world. They need instant access to your files for updates and revisions. And no Apple or Android sharing allowed.

Unfortunately, folks our age are perfectly happy with a black box, a nice monitor, a keyboard, and a mouse on our desktop. We will use Facebook and other apps on our smartphones to share pictures, but spreadsheets and vacation plans belong in a file on the hard drive (where we can find it). They do not belong on this thing called a cloud someplace in the universe. We don't wish to share our thoughts and plans with the entire world. Some stuff needs to remain under our own control! Many wish to remain with Windows 7 or Windows 8.1, thank you very much.

Here are some suggestions.

- Get rid of that silly reminder to download and install Win 10 until you are ready. Go the Control Panel, then Notification Area Icons. Halfway down the list is GWX (get windows 10). Select hide.
- Windows 10 is very good! It's fast and stable and built to be compatible with all apps running in Win 8.1 and most apps running in Win 7. The upgrade is free but takes about 2 hours to complete. **IMPORTANT:** Do not accept the default settings for Personalization Data (Turn everything off) or Auto-connectivity (Turn this off too). Ask me and I will come to your home and walk you through the install.
- If after installing Windows 10 you decide it is not what you want, you have a month to rewind to your previous operating system. (Caution: Win XP is such a huge security hazard; you **never** want to reinstall it. Stick with Windows 10.) To roll back your machine, go to Control Panel > Recovery (or Settings > Update & security > Recovery). More detailed instructions can be found at <http://windows.microsoft.com/en-us/windows-10/windows-10-recovery-options>
- To make Win 8.1 look more like your old Win 7
  1. Go the Control Panel then click on the **Taskbar and Navigation** icon.
  2. Click on the **Navigation** tab at the top of the window.
  3. Select "*When I sign in or close all apps on the screen, go to the desktop instead of Start.*"
  4. Click **OK**. Easy peasy!