Hacker Defense: Your SEVEN Point Tuneup

If it seems the online world gets more dangerous every day, you're not wrong. The AV-TEST Institute reports over 450,000 new malware samples are discovered DAILY. (That's up from 350K two years ago.) Thousands of social media accounts are hacked every day; and untold millions of consumer records compromised in data breaches are used by hackers in increasingly clever attacks. Your defense systems must be kept in tip-top shape.

Here are seven things you should keep in mind to "tune up" your computer against malware, hackers and data thieves. Failure to do so is like rolling the dice, and hoping to beat a set of odds that are stacked against you.

1: Update all of your software, from end-user applications to the operating system. Automatic software updates are the easiest, most consistent way to go. Make sure automatic updates in Windows Update are turned on, and in every application software package you have that offers automatic updates. Then install a "universal" software updater, such as **Patch My PC (patchmypc.com)**. It catalogs all software on your system, and finds your stuff in its database of several thousand developer sites that it monitors for new updates. When a new update that you need appears, it downloads and installs it automatically.

2: Activate two-factor authentication (2FA) everywhere you can, on your devices and on all sites that offer 2FA. It may seem to add another layer of complexity that slows you down, but the opposite is true.

Here is a riddle whose answer will seem heretical: When is it safe to use "password" as a password? The answer is, when you have two-factor authentication (2FA) enabled! Even if a hacker guesses your password on the first try, they can't get into your account without the second authentication factor - a code sent only to your phone, or a USB key in your pocket, or your fingerprint, or a scan of your retina, or whatever. Google and Facebook call 2FA "login approval," while Twitter and Microsoft call it "login verification." Your bank may call it something else. Inquire about 2FA and use it wherever you can.

You might wonder if it's safe to use the same, simple password on all sites where you have 2FA enabled, because the second authentication factor will be unavailable to a

hacker. I'd advise against doing that; consider what might happen if you lost your phone.

3: Use Strong Passwords. For other things that need passwords but don't offer 2FA, use a password generator/manager such as Keeper, RoboForm, LastPass, or Dashlane. A password manager not only generates strong passwords for you, it stores them in an encrypted database, and enters them automatically for you on website login pages. All you need to remember is your master password.

Password managers can help avoid weak, easily guessed passwords, and take the pain out of creating and remembering unique passwords for every online service you use.

4: Encrypt your storage devices so that even if your laptop or phone is stolen, its data cannot be read without the encryption key. Windows 7, 8.1, 10 and 11 include Bitlocker encryption. *VeraCrypt* is the free, open-source successor to the popular but now defunct TrueCrypt. Android and iOS have encryption enabled by default.

Just remember that if you don't have a screen-lock pin or password, all the encryption in the world won't help you when your computer or mobile device is lost or stolen.

5: Reduce the "surface area" that exposes you to potential attacks on your privacy and security. Start by uninstalling programs and apps that you really don't need or use. Most software has at least one vulnerability; why leave openings for hackers lying around? Windows 10 and 11 offer finer control of app permissions. Type "privacy" in the Search box and open Privacy Settings from the results. The General tab lets you toggle broad categories of app permissions. On mobile, be careful to check the permissions that apps want (or already have). If you have the Android operating system, you can open Settings > Apps, tap an app's name, then tap App permissions. From there, you can toggle individual permissions on or off. Does that fun word game really need access to your contacts, photos and messages? No.

Don't neglect all the apps that you have given permission to access your Facebook, Google, Twitter, or other "identity" accounts. Go through the "app permissions" sections on each of your social media accounts and disallow apps you no longer use. Make use of the privacy and security checkup tools provided by Microsoft and Google.

6: Defend against ransomware. Millions of ransomware infections were detected last year, costing consumers and businesses billions in losses. Clicking on malicious links is still the primary vector for ransomware attacks. Make regular backups and be very careful where you click. The old advice of "Never click links or open attachments in emails from someone you don't know" is no longer good enough. Remember that malicious links can be unwittingly sent by family, friends, colleagues, or forged to look like it came from someone you know. Malicious emails that mimic the look of your bank, eBay, Paypal, the police, the IRS, UPS or other companies familiar to you are designed to catch you with your guard down, and trick you into clicking right into the ransomware trap.

7: Upgrade your security software. For example, **PC Matic** uses a whitelist approach that allows only known-good programs to run on your computer. This is in contrast to other security tools that rely on blacklists of known malware. There are 450,000 new malware samples are discovered daily. It's nearly impossible for traditional anti-malware tools that rely on blacklists to protect you from all existing and emerging threats. So far, PC Matic has caught several things that slipped past other security software.