

Technology

How to Improve Your PC's Security

Nine Ways to Improve Your Computer's Security and Avoid a Cyberattack

BY DANIEL J. SIEGEL

Whenever I discuss a lawyer's ethical obligations and cybersecurity, one question comes up again, and again, and again: What can I do to reduce the risk that my computer will be hacked? After all, if Marriott can be hacked, how can I prevent it? While it is impossible to prevent every possible attack, your goal should be to reduce the risk—in other words, act reasonably. In this column, I will outline nine ways, some of which I have discussed previously, to improve your computer's security and reduce the risk of a cyberattack.

Of course, common sense is key. When something seems wrong, assume it is until you confirm to the contrary.

1. INSTALL WINDOWS 10

Windows 10 was released more than three years ago, while Windows 7 was released in 2009. Windows 10 offers better protection against malware and ransomware and has other enhancements to improve the safety of your web browsing. In addition, because it is the most current version of Windows, Microsoft regularly updates Windows 10 (almost every Tuesday evening) to fix bugs and provide updates that prevent cyberattacks. Plus, Windows 10 is a better, more efficient operating system. How many of you drive a 2009 car?

2. USE ANTIVIRUS SOFTWARE

Windows 10 includes security software, Windows Defender Center,



which works well. There are also other products that are more robust. Many are free, while most security suites are generally low-cost. All of these products update their definitions (the security files) automatically to ensure that you have the most up-to-date protections.

3. USE STRONG PASSWORDS

Hackers prey on simple passwords because once a hacker has your password, the hard part is done. They can then do just about anything they

want. If you have trouble remembering passwords or generating complex passwords, there are many password management programs that will create and store your passwords.

4. CREATE A RESTORE POINT FOR YOUR COMPUTER

A restore point, part of the Windows System Restore utility, is a saved "snapshot" of your computer's operating system and data at a specific time. You should create a restore point when you

Even with secure browsers, some pop-ups manage to slip by, and “closing” the pop-up box may merely be an invitation to download some unknown variant of malware.



know that your computer is working properly and before you make any changes to your computer that could potentially cause problems or make the system unstable. To create a restore point, go to Control Panel and select “Create a restore point” from the System setting. Windows will walk you through the process.

5. MAKE SURE YOUR FIREWALL IS TURNED ON

A firewall prevents malicious information from getting into the ports (doors) to your computer. Windows includes a firewall, and every security suite includes a firewall. You should make sure that your firewall is enabled.

6. BLOCK POP-UPS

Pop-ups are those annoying windows that suddenly appear in front of the browser or other window in your computer. While some pop-ups are

useful and important, most are either advertisements or traps designed to lure or mislead computer users into revealing email IDs or sensitive personal or financial information. Even with secure browsers, some pop-ups manage to slip by, and “closing” the pop-up box may merely be an invitation to download some unknown variant of malware.

There are ways to manage pop-up settings. First, confirm that your browsers have pop-up blocking enabled. Second, enable your antivirus or security software’s anti-pop-up feature. Of course, you also should not click on any pop-ups.

One exception: some legal products, including LexisNexis and Westlaw, may have pop-ups that permit you to download research results. You can configure your browsers to allow an exception for those products. But do so carefully.

Dragon® Legal Group Software

It is possible to save time, cut costs, and, free up staff to create opportunity for more billable hours for your practice or firm with Dragon® Legal Group speech recognition software from Nuance Communications.

Dragon® Legal Group is a suite of speech-to-text software applications that was specifically built for the legal profession and for lawyers. The software enables users to create documents, transcribe audio recordings, and fill out forms and templates using its cutting-edge speech recognition technology.

The software’s “legal specific language model”—its dictionary—uses over 400 million words culled from legal documents as its base and allows the user to customize it further by adding client- or practice-specific terms. With the help of such a robust vocabulary, the user can dictate and format legal documents, insert and format text citations, and edit audio transcriptions—entirely through voice commands.

Additional features include:

Custom command creation – Create automated processes by recording keystrokes and mouse clicks and then save the entire process under a single voice command.

Transcription post-editing – Store audio recordings in the same documents as their transcriptions and include “voice notations” within Word documents for third parties.

Speech recognition training – Upload a 90-second audio clip of a speaker that the software will use to “train” the dictation application for more accurate transcription.

Dragon® Anywhere Group – Opting into this branch of services enables users to do all of the above, but on-the-go via mobile devices and tablets.

To get an idea of what using the software looks like in the real world, check out the YouTube video “Dragon Legal – Streamline Legal Documentation by Voice” at <https://youtu.be/fLH9w7cvi6Y> for a practical demonstration. ■

Change the default password to your WiFi and router hotspot to something complex. In addition, hide the name of your network so that only you can access it. If you do not know how to do this, contact your Internet service provider to help you.

7. SECURE YOUR HOME NETWORK

Enable WPA2 encryption on your wireless router. Change the default password to your WiFi and router hotspot to something complex. In addition, hide the name of your network so that only you can access it. If you do not know how to do this, contact your Internet service provider to help you.

8. USE SOCIAL MEDIA SAFELY

Social media is often a security trap. First, do not use or enable the feature found on many websites that allows

a user to use a social media site's password on the other site. When you do so, a hacker who obtains your social media password will also be able to access any other sites where you have enabled the use of that login, leaving you particularly vulnerable. In addition, check for updates to your social media sites' privacy and security settings, which are always changing.

9. USE COMMON SENSE

When it comes to technology, many users make excuses about why they

cannot learn how it works. Regardless, do not leave your common sense at the door. As we tell clients, and even our children, if something does not seem right, do not do it. Better safe than sorry. ■

Daniel J. Siegel, (dan@danieljsiegel.com), a member of the Board of The Philadelphia Lawyer, is the president of Integrated Technology Services LLC, a consulting firm that helps law offices improve their workflow through the use of technology.

For special needs clients, the settlement is only the beginning.



Our team offers effective and creative options for the administration of special needs trusts and guardianships as families cope with complex and challenging situations. We provide hands-on help and access to a wealth of resources that minimize burdens on your clients and their families before, during, and after resolution of litigation.

Above, left to right:
Susan L. Bartels
Senior Vice President
Peter J. Johnson, Esq.
Senior Vice President
Felicia D. Butler
Account Administrator

PLEASE CONTACT:
PETER J. JOHNSON, Esq.
SENIOR VICE PRESIDENT
DIRECTOR, SPECIAL NEEDS TRUSTS
AND GUARDIANSHIPS
610.975.4308
johnson@penitrust.com
PENINTRUST.COM
RADNOR, PA



**CONSISTENTLY ADDING
VALUE**
for over 30 years



Ecovacs Deebot N79S



Neato Robotics D4 Connected



iRobot Roomba i7+

WHAT IS THE BEST WAY TO MAKE SPRING CLEANING MORE EFFICIENT, EASY, AND AUTOMATIC? One very good answer: a robotic vacuum. Since the original Roomba emerged in 2002 to become a huge consumer hit, the number of robovacs on the market has inundated consumers with a multitude of choices for all types of cleaning needs. Robovacs are becoming so commonplace that a quality purchase can be made for under \$200, although certain high-end versions are built with features well worth their \$1,000 price point.

In a range of prices and features, today's models not only vacuum, they scrub floors, map floor layouts, can be scheduled for cleaning via app or remote, return to their docking stations when finished, and more.

So, a \$200 model versus a mid-range \$500 model versus a near-\$1,000 model, how do they compare?

FEATURES	ECOVACS DEEBOT N79S	NEATO ROBOTICS D4 CONNECTED	IROBOT ROOMBA I7+
SIZE (DIAMETER X HEIGHT)	13.9 X 3.3 IN.	13.2 X 12.6 (D-SHAPED) X 3.9 IN.	• 13.34 X 3.63 IN. • CLEAN BASE: 19 IN. X 12.2 X 15.1 IN. (HWD)
BATTERY LIFE	95 MINUTES	75 MINUTES	60 MINUTES
CONTROLS: A - APP V - VOICE COMMANDS R - REMOTE	A-ANDROID; IOS V-ALEXA; GOOGLE ASSISTANT R-START/PAUSE CLEANING; SCHEDULING; TIME AND DATE; SPOT CLEANING; ROOM CLEANING; WI-FI SETUP; EDGE CLEANING	A-ANDROID; IOS; APPLE WATCH V-ALEXA; GOOGLE ASSISTANT	A-ANDROID; IOS V-ALEXA; GOOGLE ASSISTANT
ACCESSORIES	• CHARGING DOCK • REMOTE	• CHARGING DOCK	• CHARGING DOCK/CLEAN BASE
STAND-OUT FEATURE	POWERFUL SUCTION, ESPECIALLY FOR THE PRICE	PERSONALIZED CLEANING MAPS; VIRTUAL BOUNDARY LINES	CLEAN BASE (SELF-EMPTYING DUSTBIN); PERSONALIZED CLEANING MAPS
PRICE	\$229.00 ON AMAZON + FREE SHIPPING FOR \$199.99	\$499.99 ON AMAZON + FREE SHIPPING FOR \$505.65	\$949.99