COMPUTER GURU — *by Don Benjamin*
The Donald and Nancy Light Technology and Literacy Lab Programs
sponsored by: Stark & Stark Attorneys at Law

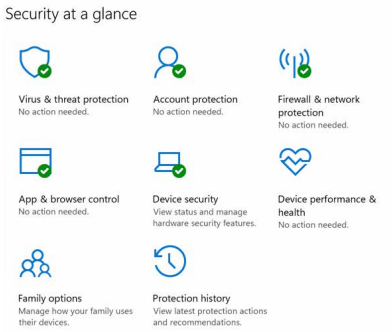
Malware Protection

(To learn more, register for the Tech Workshop on Computer Security, Wednesday, May 4 at 2:00 p.m. on Zoom.)

Hacking, scamming, phishing, and spoofing. What security software do you need to stay safe? And safe from what?

Let's answer that last question first.

Most security breaches fall into two categories: **1. Hackers** who steal data from your online accounts, and **2. Malware** that makes your computer do bad things.



Windows security options.

Hacking

Hackers do not try to break into your computer. Instead, they hack into corporate file servers to steal information, which could include your usernames and passwords. Unfortunately, you cannot prevent hackers from stealing your information from corporate servers. That's why you should assign different passwords to each of your online accounts and use double authentication (via email or text) for your financial accounts. Then, if someone does obtain the password to your online bank account, they won't be able to log in, and you'll know if they tried.

Malware

Malware is software that folks unwittingly download on their computer by 1. Opening an infected email attachment, 2. Downloading infected software from the Internet, or 3. Allowing a scammer to remotely access your computer and install spyware.

Your defenses against malware include 1. Keeping your operating system up to date, 2. Remaining wary of email attachments, and 3. Using anti-malware programs.

Paid-for or Free: Our Recommendations

If you use Microsoft Windows 10 or 11, then **Windows Security**, a.k.a. Microsoft Defender Antivirus, is a good choice. It's built into Windows and costs nothing to use. Microsoft keeps the malware definitions database up to date. The Windows software examines your downloads and the websites you visit and scans your computer periodically to catch software that shouldn't be there.

Malwarebytes (at $40/year) is a good choice if you want more protection. It's unobtrusive and effective.

For Apple users, while MacOS is pretty much "locked down," it's still a good idea to use a malware protection program, and, again, we suggest **Malwarebytes**.

If your security software detects malware, it may display an alert or warn you about a suspect web page, but these programs "quarantine" the offending malware so it can't run.

In no case will Microsoft or Apple call you, text you, e-mail you, or cause a web page pop-up to appear that claims your computer has a virus. If you experience any of these warnings, beware! They're scams. And don't give anyone access to your computer unless you know who they are.

And finally…

1. Don't respond to emails or phone calls demanding money, especially if they want payment in cryptocurrency (e.g., Bitcoin) or gift cards.
2. Don't respond to pop-up banners claiming that your computer is infected. Instead, either close them or exit your browser.
3. Don't call phone numbers or click on links listed in suspicious emails.
4. Don't allow anyone you don't know to remotely control your computer.
5. Request help from our Tech Resources if you suspect a scam or malware infection. Just fill out the tech request form at **princetonsenior.org/psrc-tech-resources/** and we'll be in touch!