EDUCATE

3 WAYS YOUR COMPUTER CAN GET INFECTED

ANTIVIRUS SOFTWARE ALONE IS NOT ENOUGH

BY HEATHER P. REMER, CO-OWNER AND CEO, COMPUTERCARE LLC

We all know that having antivirus software on our computers is important, but people often don't realize that antivirus software alone is simply not good enough to prevent malicious programs (malware) from infecting their systems. There are several ways that malware can be introduced to your company's computer systems and be allowed to wreak havoc on your networks, even when the best antivirus software is installed. Here are a few ways that your systems can become infected, regardless of software protection.

Hackers think differently. They are wired to look for holes in the system and capitalize on them.

SHUTTERSTOCK.COM

"4 TIPS FOR PROTECTING YOURSELF"

1. Ensure you have policies and clear expectations concerning how your remote users access your network and what devices they use to do so. A "bring your own device" policy, along with strong overall security policies, is a good place to start. Consult your IT provider for suggestions on what to include in these policies.
2. Run a virus scanner on devices before attaching them to your computer or network, and consider moving to a cloud-based storage solution rather than transporting files on USB drives.
3. Set a schedule for ensuring that your antivirus solution is being updated regularly. Better yet, get your IT provider to set you up with antivirus monitoring so that those updates are applied automatically for you behind the scenes.
4. Layer your protection. Utilizing not just antivirus protection but firewalls at both the location of the business network and at the location of any remote users can significantly cut down on risks while also preventing spam that often contains dangerous links and files.

SHUTTERSTOCK.COM

1 THROUGH REMOTE EMPLOYEES

While having employees who are able to work at home or in the field can have significant advantages, there are also security risks. It's important to consider all of the devices that interact with your network as doorways through which malware can gain access. This could happen through virtual private networks (VPNs), for example, like those that are often used to allow an employee to remotely access the company's network. This and other unsafe channels, such as unsecure public Wi-Fi at a coffee shop or hotel, make it relatively easy for others to gain access to your computer's data

2 THROUGH EXTERNAL DEVICES

Larger threats come when employees bring infected devices (like USB drives) in from remote locations and then connect them directly into the network. Any device connected to a computer could become a target for malware, so having systems to manage these risks is vital to preventing these very avoidable attacks.

3 THROUGH FAILING ANTIVIRUS SOFTWARE

Antivirus software is not a failsafe, even from website viruses. Antivirus software works primarily through two scanning methods: It looks for key bits of code (or definition files) that are known to be associated with a virus, and it also scans for suspicious activity, like a program that is sending information out frequently from your computer or network. People often don't remember to (or choose not to) update their antivirus software, but it is critical to keep your software as up to date as possible with the newest definition files. And finally, even the best antivirus software programs out there are, by default, one step behind the hackers they are protecting you against. It takes time for developers to address security holes, and that delay is something hackers prey on.

Even the best antivirus software programs out there are one step behind the hackers they are protecting you against.

Ultimately, the more points of entry into your network, the greater the risk; remember that as your company grows, so do the risks of malware. Hackers think differently, and they are wired to look for holes in the system and capitalize on them. Since no system is perfect, completely eliminating the risk of malware infections just isn't possible. Staying proactive, consulting regularly with your IT provider and keeping your antivirus software up to date are truly your best chances for avoiding the costs and hassles associated with malware.

HEATHER REMER is co-owner and CEO of ComputerCare LLC, an IT services company providing a full spectrum of IT solutions and services to small and medium businesses.