Health Information Compliance Alert

Clip And Save: Sidestep "Malvertising" Mayhem With These Expert Tips

Hint: Keep on top of the latest software patches.

Healthcare hackers have a seemingly bottomless bag of tricks that promise to destroy data, disrupt workflow, and hijack your computers. The little known problem of "malvertising" is something your practice should investigate to keep your systems running smoothly.

Nuts and bolts: Malvertising is a malicious variety of online advertisements generally used to spread malware, and it is one of the most common ways of infecting computers with malware," explained **John Roman, Jr., CISSP,** director of IT Firm Operations at Nixon Peabody LLP in the Rochester, New York office in a recent blog posting.

Malvertising involves "malicious ads that attempt to surreptitiously install crypto ransomware (this is the software that encrypts all of your data and holds it ransom until you pay the hacker to send you a key to unlock your files) and other malware on the computers of unsuspecting visitors" to websites, Roman said.

"Hackers take advantage of vulnerabilities found in unpatched versions of Adobe Flash, Microsoft Silverlight, and other widely used internet software," noted Roman. "The malware is 'installed' by hackers through banner ads that are located on compromised ad networks."

Follow These Protective Steps

Websites are hacked every day, and a single click can infect your system. Roman offered the following tips to reduce the risks to your computers and network from receiving malware from malvertising websites:

- If possible, uninstall Adobe Flash, Oracle Java, Microsoft Silverlight, and other third-party browser extensions.
- Keep your plug-ins updated and set them to automatically update.
- Update your web browsers (web browsers should automatically update themselves, but make sure you don't disable automatic updates).
- Install Windows security updates as soon as they become available.
- Install Windows 10.
- Use Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or Malwarebytes Anti-Exploit to monitor your web browser and detect malicious code targeting vulnerabilities in your system.