Ransomware worries? Keep up to date.

May 15, 2017
by Nat Wood
Associate Director, Consumer & Business Education, FTC

You've probably heard about the ransomware attack affecting organizations' computer systems around the world. It seems to affect server software on organizations' networked computers. But ransomware can attack anybody's computer, so now is a good time to update your own operating system and other software. And then keep them up-to-date.

The ransomware in the news now is known as WannaCry or WannaCrypt. It locks users out of their systems until they pay the crooks who installed it. This ransomware takes advantage of a security hole in Windows server software that can be closed by an update from Microsoft. Many of the organizations affected by the ransomware had not installed the software update.

Even if you only have one computer, download security updates as soon as they're available – no matter what operating system you use. Hackers are constantly looking for security gaps, and companies try to close those gaps as soon as they are discovered. So it's important to download updates right away. Most operating systems have a setting to download and install security updates automatically. Use it. And install updates for your other software, including apps.

If you use old software that doesn't update automatically, set up a regular schedule to go to the company's website and download and install updates yourself. It's wise to check at least weekly.

In addition to keeping software up to date, here are a couple of other things you can do to prepare for a ransomware attack:

- **Back up your important files.** From tax forms to family photos, make it part of your routine to back up files often on your computers and mobile devices. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt and lock your back-ups, too.
- **Think twice before clicking on links or downloading attachments and apps.** Ransomware often is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.