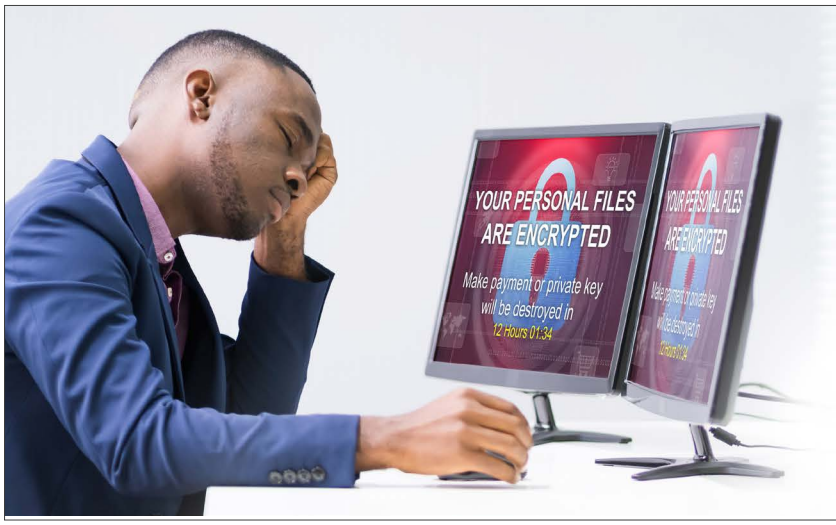
WFG National Title

SAFE Tipsheet

Ransomware - Is It Coming for You?



What do a Major gas pipeline, a Florida city's water supply, one of the world's top meat producers, dozens of government agencies, and a ferry operator in Martha's Vineyard have in common? Ransomware! This is the "digital kidnapping" of valuable data, from personal photos and memories to client information, financial records, and intellectual property.

Microsoft recently issued a warning about attackers using a call center to trick you into downloading ransomware. It starts with a fake Microsoft phishing email, not to click on anything, but to provide a number to call to avoid some upcoming charges but ends the same, getting you to download the hackers' ransomware.

Any individual or organization could be a potential ransomware target, so everyone needs to be vigilant about basic security practices in an increasingly connected world.

So, what can you do?

First, Back It Up!

Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.

Think, Really Think, Before You Act

Links in emails, social media posts, texts, and online advertising are some methods cybercriminals use to deliver ransomware or steal your personal information. Even if you know the source, if something looks suspicious, delete it. Don't click on a link from a stranger! Employ an email scanning software that scans for suspicious emails, and don't click any online ads or anything else that pops up online that you were not expecting.

Restrict Permissions to Install and Run Software Apps on Your Devices

Think about permissions for children and other family members on home devices, not just employees on work devices.

Keep all machines clean

Keep the security software on all Internet-connected devices up to date (think of antivirus, antimalware, and firewalls). All critical software, including computer and mobile operating systems, security software, and other frequently used programs and apps, should be running the most current versions.

Get two steps ahead

Turn on two-step authentication, also known as two-step verification or multi-factor authentication, on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.

Make better passwords

Use a strong password - or better, try using a passphrase, which is a phrase that is at least 12 characters long. The longer, the better, and the harder to crack!

Plug & scan

USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Knowledge, awareness, and some good security practices can go a long way toward protecting your company, your family, and yourself from becoming a victim.

June 2021