STOP | THINK | CONNECT™

RANSOMWARE FACTS & TIPS

As technology evolves, the prevalence of ransomware attacks is growing among businesses and consumers alike. It's important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code. Ransomware is like the "digital kidnapping" of valuable data – from personal photos and memories to client information, financial records and intellectual property. Any individual or organization could be a potential ransomware target.

WHAT CAN YOU DO?

We can all help protect ourselves – and our organizations – against ransomware and other malicious attacks by following these STOP. THINK. CONNECT. tips:

- **Keep all machines clean:** Keep the software on all Internet-connected devices up to date. 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.
- **Back it up:** Protect your valuable work, music, photos and other digital information by regularly making an electronic copy and storing it safely.
- **Make better passwords:** A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.
- **When in doubt, throw it out:** Links in email, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.
- **Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Created by the National Cyber Security Alliance

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT STOPTHINKCONNECT STOPTHINKCONNECT