How to Protect Your Data from Ransomware Attacks

Ransomware can take on multiple forms. From phishing emails or USB keys containing malicious files to downloaded files from the internet, ransomware takes over your computer and holds your data hostage. Here are some tips on how to protect your data from ransomware attacks.

1

INSPECT WEBSITE EMAIL URLS

Sites or phishing emails that target users with ransomware files come from addresses that contain suspicious elements, like changed or additional characters, or intentional misspellings of common words.

NEVER CLICK ON UNVERIFIED OR SUSPICIOUS LINKS

Avoid clicking on links that come from unknown email senders or ones that lead to unfamiliar websites. Downloads that start after clicking a link is one way your device can become infected.

2

3

DON'T OPEN UNRELIABLE EMAIL ATTACHMENTS

Never open email attachments from untrustworthy senders. Avoid enabling macros in productivity software or running programs that don't originate from a trusted source.

ONLY VISIT OR DOWNLOAD FROM SITES YOU TRUST

Don't visit or download files from unverified or unsecured websites. Only download files and programs from official websites. Also, look for "https" or a shield or lock symbol at the beginning of the address bar to see if the site you're visiting is deemed secure.

4

5

AVOID USING UNFAMILIAR OR UNAUTHORIZED STORAGE DRIVES

Physical storage media, from USB flash drives to backup hard drives, can also infect your device if you don't know where they come from. Cyber criminals may leave storage devices in public places to entice you to use it.

REGULARLY SCAN AND UPDATE YOUR SYSTEM SOFTWARE

Performing regular antivirus scans and keeping your system software updated will help protect your data from ransomware. The latest security patches make it harder for cyber criminals to exploit system vulnerabilities.

6

7

PROTECT YOUR FILES

Store your files in locations that are regularly backed up to ensure recovery in case of infection by ransomware. Never pay the ransom to restore your files and always contact your IT support in case of infection.