Quikteks Business Technology Solutions Shares Vital Malware Defense Tips

Tech support experts provide advice on malware prevention and how to deal with attacks on company data.

FAIRFIELD, NEW JERSEY, USA, March 14, 2022 /EINPresswire.com/ -- Quikteks Business Technology Solutions, which provides enterprise-level IT practices to small and medium sized businesses, today announced the release of new information to avert and prevent cyberattacks from malware.

> Malware, whether temporary or permanent, is very dangerous. Ultimately it is up to the end user to be able to identify and avoid whatever it is that looks suspicious."
>
> *Andrew Rich, CEO*

1. Use a reputable antivirus software - Don't install dubious antivirus software after seeing a popup threat warning. Install a reputable and reliable antivirus software, and set it to block threats in real-time and receive updates immediately. One should also use the software to perform regular deep scans.

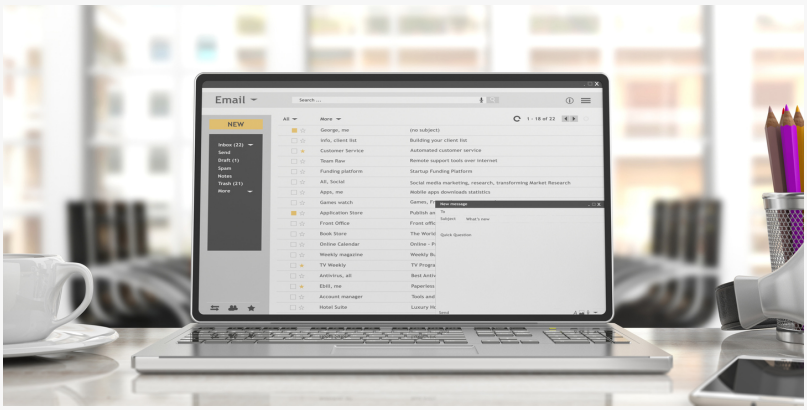
2. Control spam- Many disguised threats arrive in the inbox. These messages may seem to be from a bank with a link for one to sign in and view the latest security alerts, or a .zip file containing a bank statement. Familiar logos and URLs make the message look legit, but if one clicks the link or open the file, one could be activating malware! A good anti-spam solution will catch "phishing" attempts and other spam messages.

3. Keep all of the computer security software current - Make sure that all of the computer security software is current. New malware and variants are released all the time, making it necessary for computer security software developers to update their software frequently. If one doesn't have the latest protection, one's computer is vulnerable.

4. Patch an operating system with the latest security updates - Security holes in one's computer's operating system could make a PC vulnerable to threats. As new hacks are discovered, operating

system developers create “patches” to fix them. If one doesn’t apply the latest updates, one's computer won’t have the latest protection.

5. Backup data regularly - Because ransomware holds data hostage, backing up one's data gives leverage against the hackers. By having a copy or more, one has better leverage over their data and negotiating power in a hostage-ransom situation.



6. Secure the Wi-Fi Network - Wi-Fi networks must also be secured from hackers. Start by switching to either WPA or WPA2 encryption and set up a strong, hard-to-guess password. Make sure to turn off SSID broadcasting as well.

7. Avoid using public Wi-Fi - It’s easy for one to log on and use public Wi-Fi, but the same is true for hackers, and a device will be vulnerable. If one must use a public hotspot, use only those that require a password which is only given to customers and changed daily, and don’t access online banking or transmit other sensitive information.

8. Use strong, hard-to-guess passwords - There are ways to memorize complex passwords. simple equations like 1+1=two would be considered strong and easy to remember.

9. Be mindful what/how you share - If it's out there, it's out there. Be mindful where one's data is, what information one is sharing, how one shares it, etc.

10. Be mindful what you click - Even with security software installed, think before clicking. That invoice.zip file from a shipping company, for example, might not be real. Expecting a message with an attachment? Is this normal behavior for that contact? Check an alternate method before opening anything unexpected. Hover over links with the mouse to view the actual URL.

“Malware, whether temporary or permanent, is very dangerous,” said the CEO of Quikteks, Andrew Rich. “There is hidden, non-overt malware that can turn on at any moment and attack company computer data. Ultimately it is up to the end user to be able to identify and avoid whatever it is that looks suspicious.”

Quikteks is a Managed Service Provider (MSP) supports small- and medium-sized businesses in New Jersey and New York. The IT experts from Quikteks offer technical help desk support and network security. The company keeps data safe so businesses can grow securely.

To schedule a free IT security assessment, please give us a call at (973) 882-4644 or visit us at Quikteks.com

Andrew Rich
Quikteks
+1 973-882-4644
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
