



Fraud Awareness & Risk Management: Mastering Malware Defense

Criminal perpetrators of malware attacks are displaying unprecedented relentlessness, intensifying their efforts to pilfer data, tarnish reputations, and wreak havoc across businesses of all scales. Understanding malware and knowing how to thwart attacks is the first line of defense for business leaders.

What is Malware?

Malware is an intrusive software cybercriminals use to steal data or destroy computer systems. Often times, the malware can be disseminated via phishing emails, downloads or by accessing unsafe websites.

Types of Malware

Adware

This software displays ads to the user by multiple pop-ups. Adware can track information about you or extract personal information. Adware can be bundled with other software or downloaded from non-reputable sources, like unofficial app stores.

Stalkerware

This runs silently and gives an attacker control over a device. Stalkerware can be installed when the attacker has physical access to your device and installs a stalkerware app, or if you get tricked into downloading the app via a fraudulent email or text message.

Trojan

When downloaded, Trojan software performs like the legitimate application but actually does malicious activity in the background. Trojans can be found in pirated or fake antivirus software.

Ransomware

When downloaded, this malware encrypts a company, organization, or individual's data and holds the electronic key for ransom. Ransomware gained popularity recently and is now a primary objective for attackers globally. It usually attempts to spread itself at high speed through the network, locking every computer and server it can find.

Advanced Persistent Threat (APT) Attack

An APT attack is an attack from an intruder that establishes an undetected presence in a network to steal data over a prolonged period of time. APT attacks are often used simultaneously with fraudsters who will attempt to maintain access to the system.

During 2022, the worldwide number of malware attacks reached \$5.5 billion an increase of 2 percent compared to the preceding year.¹



5 Ways to Avoid Malware

1. Unpatched vulnerabilities

Malware takes advantage of vulnerabilities. Software companies fix these by pushing updates to users. Software updates are critical for security, as they are the most effective way to stay safe.

2. Back up your data

If your company's device is compromised due to malware, theft, or damage, your uncorrupted files may still remain in your backups. Protect them by using a strong password and encryption. Consider backing up offsite or disconnect your backup system from the network each time backup is completed. It is important to note that a lot of ransomware also corrupts backups if maintained on the same network so regularly test your company's backups to make sure they work. Consider backing up your computer data on a removable hard drive or through a cloud backup system.

3. Wait before you click

Link and file sharing is a common practice, but stay aware when interacting with or sharing links. Before clicking, ask: Does this link seem odd? Look out for shortened or cut-off links, typos, copied branding and logos, and fake messages from colleagues. Hover your mouse over the link but don't click on it. Carefully look to see if the link matches the text in the link. If it is something different and is an address you don't recognize, delete the entire email.

4. Be careful whom you give access to

Do not allow sharing of unlocked devices. Your company's devices should use full-disk encryption and strong passwords to protect them from unwanted physical access.

5. Use antivirus and anti-malware software

Not all antivirus software is created equal; some software marketed as antivirus can be disguised malware. You may want to use your device manufacturer's own antivirus software. If you prefer third-party antivirus software, check for independent reviews of the software and see if the antivirus website has an up-to-date list of the type of malware you are concerned about. Consider adding a recognized anti-malware application.

By making sure workflows and processes are secure, you'll rest easier knowing critical steps are in place to keep cybercriminals away, protecting the future of your company.

**Received a
fraudulent or
suspicious email
that appears
to be from
Webster Bank?**

Contact a Webster
Relationship
Manager or call
888-932-2256.



Want more information on protecting your company from cyber threats?
Connect with [Webster Bank](#).

¹ Source: Statista, 2023.

The opinions and views herein are for informational purposes only and are not intended to provide specific advice or recommendations. Please consult professional advisors with regard to your situation.