Fraud Awareness
Malware & Phishing

WHAT IS MALWARE & PHISHING

Malware is short for malicious software and is made to conduct unwanted actions on your device. It can be computer viruses, or programs that steal passwords, record you secretly, or delete your data

Phishing is a type of malware. A phishing attempt is a message, email, or link that looks okay, but is actually malicious. Phishing usually involves an attacker impersonating someone you know using a platform that you trust. Phishing most frequently comes in the form of an email, a Business Email Compromise (BEC) attack, from individuals outside the organization. Treasury staff discovers the majority of payments fraud.

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, 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 business 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 malware from an attacker that compromises your system from multiple resources. A.P.T. attacks are often used simultaneously with actors who will attempt to maintain access to the system

HOW CAN YOU AVOID MALWARE?

UPDATE YOUR SOFTWARE

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.

BACK UP YOUR DATA

If you lose your device to malware, theft, or damage, your files will 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. There is a lot of Ransomware that also kills backups. Test your backups to make sure they work.

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 and cut-off links, typos, copied branding and logos, and fake messages from friends. 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.

BE CAREFUL WHO YOU GIVE ACCESS TO

Use caution when lending your unlocked device to someone. Your device should use full-disk encryption and a strong password to protect it from unwanted physical access.

Fraud Awareness
Malware & Phishing

HOW CAN YOU AVOID MALWARE? *(continued)*

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 malware on the type of malware you are concerned about. Most anti-virus applications do a good job against virus' but are not very effective against Trojans or malware. Consider adding a recognized anti-malware application.

IMPORTANT FRAUD FACTS*

82% of organizations were victims of attempted or actual fraud in 2018
- 70% Checks
- 45% Wires transfers
- 35% ACH Debits
- 29% Credit Cards
- 20% ACH Credits

80% of organizations have been subject to attempted or actual Business Email Compromise (BEC)
- Up from 64% in 2016
- 54% of companies reported losses as a result of BEC

47% of organizations discovered fraud less than 2 weeks after the incident occurred

65% of payments fraud is committed by individuals outside the organization occurred

QUESTIONS AND ANSWERS

Q. Experienced a malware attack?

A. Do not turn off your device. Immediately disconnect the device from the network and notify your IT group. Do not wait as the damage may already be spreading.

Q. Received a fraudulent or suspicious email which appears to be from Webster Bank?

A. Forward the email to reportfraud@websterbank.com

A. Or, call Webster Bank's Security Hotline at 1.800.966.0256, 7:00 am to 10:00 pm, 7 days a week

*Sources: Security Education Companion, a project of the Electronic Frontier Foundation and 2019 AFP Payments Fraud and Control Survey Report

FN02303 04/2020