TIP SHEET:

WHAT TO DO WHEN MALWARE STRIKES

LMG SECURITY

You've been hit with a malware infection—now what? Respond quickly and make sure it doesn't happen again with effective prevention and detection measures. Here are the most important things to do next:

FIRST RESPONSE

QUARANTINE AFFECTED SYSTEMS

First, isolate all infected computers. Depending on your environment, you can logically isolate the system, or physically unplug the network cable immediately to stop the spread.

LOCK OUT THE ATTACKER

Get the attacker out of your network quickly to minimize damage and stolen data.

☑ Reset Passwords

Attackers routinely steal passwords, and often share or sell them on the dark web. Quickly reset user passwords and administrator accounts whenever possible. You may also need to reset service accounts, shared device management accounts (router, switch, firewall, and so on) and other accounts, too.

☑ Kill Active Sessions

Password resets can stop new authentications to the account, however currently authenticated users with a valid user session may still be able to access the account until that session expires. Killing active sessions will log out users and require a new authentication with current credentials, effectively locking the bad actor out. Initiating a session reset for active users can be done through the Active Users section of the Office 365 admin center or can be scripted using PowerShell.

☑ Multifactor Authentication

Activate multifactor authentication (MFA) if you have not already, for both cloud accounts and remote access to your network. This will help prevent a wide range of compromises, including malware. LMG can help you deploy MFA if you need assistance.

HUNT FOR THREATS

Make sure the attackers are truly out of your network. All too often, victims clean off the malware, without realizing that the criminals have a secret backdoor into the network. Don't get hit again. LMG's team of experienced professionals can proactively hunt for threats to prevent the same criminals from locking up your files again.

PRESERVE EVIDENCE

Don't stomp on the crime scene—you may need evidence to legally "rule out" a data breach. Avoid running antivirus or reformatting the computer until a trained forensics professional has examined the system. Keep a copy of the malware if you find it, so that forensic analysts can examine it if needed.

PREPARE FOR THE FUTURE

Once the immediate danger is mitigated, take the following steps to help prepare for a future attack.

ASSESS YOUR CYBERSECURITY

Find the flaws in your cybersecurity before hackers do. Conduct regular penetration tests and vulnerability assessments.

BACKUPS

Verify that your backups are complete and immutable, so hackers can't delete them if they gain access. Ensure that you test them on a regular schedule (i.e. monthly).

VULNERABILITY MANAGEMENT

Ensure that all of your systems are kept up-to-date on software patches. Verify by regularly reviewing detailed patch management reports. LMG's team can audit, if needed.

MONITORING AND LOGGING

Catch intruders quickly, before they have a chance to infect your systems. Make sure that your monitoring systems detect suspicious activity and alert immediately if an intruder is inside your network. LMG conducts network monitoring assessments and attack simulation testing that can proactively identify any gaps in your monitoring program.

TRAINING

Make sure your employees are trained to resist cyberattacks such as phishing emails. LMG provides on-demand awareness training, webinars, seminars, tip sheets, and other materials to support a fully-fledged cybersecurity awareness program.

UPDATE YOUR POLICIES & RESPONSE PLANS

Malware infections are always a learning opportunity. Routinely update your cybersecurity policies and response plans to address any issues that came up, so you are better prepared. LMG's experienced professionals can take care of this for you if desired, so you can get it done quickly without adding to your staff's workload.

Malware infections are difficult and stressful situations. We hope these tips help you move forward with even stronger cybersecurity.

If you have questions or need supplemental support, please contact us. We are here to help.

Contact Us

1-855-LMG-8855
E-mail: info@LMGsecurity.com
www.LMGsecurity.com

Referring a Client

To refer a client to LMG Security, please email info@LMGsecurity.com

LMG™
SECURITY