TOKIO MARINE HCC

LHA TRUST FUNDS

Don’t Let Ransomware Destroy Your Business.

Do you...

1. Require two-factor authentication for all remote access to your network?

2. Have a secure data backup solution in the event of a ransomware attack?

3. Use the right email spam filter?

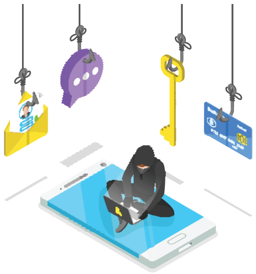
4. Fight malware with behavior-based antivirus software?

You can protect yourself and your organization.

There are 4 key cyber smart strategies:

1. Two-Factor Authentication
2. Offline Backups
3. Spam Filtering & Email Configuration
4. Next Generation Anti-Virus: Behavior-based Protection

RANSOM DEMANDS HAVE INCREASED 40x FROM 2016 TO 2019



You Can Prevent Ransomware Attacks

Just a few easy steps can save your business.

1. Two-Factor Authentication (2FA)

We strongly recommend you implement this simple and cost-effective security measure.

2FA protects your organization because it adds another layer of protection to password-protected remote access to your network. The vast majority of successful hacking/ransomware attacks are a result of the hacker gaining access to a company's network using compromised login credentials. In other words, even if the hacker has stolen an employee's login credentials, dual-factor authentication should prevent them from accessing your network, since they would also need to have the employee's mobile phone which is being used as the 2nd authentication factor.

2FA should also be used on all remote access to your email servers (**Office 365** and **GSuite** have free solutions). Hackers use compromised email accounts to launch ransomware or social engineering attacks against your contacts.

A typical, real-life ransomware attack

Your employee opens an invoice attached to a vendor email. It looked like other emails from the same person. That attachment releases ransomware that immediately spreads to all company machines, including your backup server. As a result, every computer in your organization is rendered **useless** and your business operations shut down immediately because you can't access any critical systems, applications or data.

This attack happened to a mid-size business on the east coast, crippling operations and resulting in at least **$18.2 million** in damages creating a combination of lost revenue and direct costs to restore its systems.

2. Offline Backups

Backups can be another effective strategy to reduce ransomware damages and business disruption. If you get infected with a ransomware virus, you won't need to pay the ransom to get back up and running. You will be able to wipe out the virus, clean your devices and network, and reinstall everything from a recent, clean backup.

Recently hackers have been effectively attacking backups that are not properly protected. All backup solutions that are connected to your network are highly vulnerable to malware/hackers.

You Can Prevent Ransomware Attacks

So consider the cloud. For small and medium sized companies, Veeam, Datto, Backblaze and iDrive provide popular cloud solutions for backups. Just because you are using the cloud does not mean the cloud backups are properly isolated or segregated. Be sure to properly configure any cloud backups to ensure they are isolated from your operating environment.

Create internal procedures for maintaining on-site and off-site backups of your critical systems and data. Best practices include periodically testing your backups by restoring your systems from backup to ensure they work when needed.

3. Spam Filtering & Email Configuration

Your email server can automatically filter out suspicious emails. Activating these filters is an easy way to prevent dangerous phishing emails from landing in your employees' mailboxes. Use email filtering to quarantine suspicious emails and scan documents and files before they are opened.

Because criminals are using a compromised account concurrently with the actual user, they must hide their activity. Check your email for suspicious email forwarding and mailbox rules. These rules are a signature that reliably detect whether criminals have infiltrated your email.

Helpful Tip!

In Office365, administrators can develop alert policies to detect specific behavior. To do so, log into protection.office.com, go to **Security and Compliance center > Alerts > Manage Advanced Alerts. Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both.**

It is also recommended to create a rule for "Set-InboxRule." Details can be found here: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

4. Next Generation Anti-Virus: Behavior-based Protection

Behavior-based security software scans devices for unusual behavior and can decide if the deviation is a threat. These solutions are typically connected to the cloud, so their ability to detect new malware variants is updated in real time. This is sometimes known as Next Generation Anti-Virus.

Anti-virus software on user devices, networks and servers is used to find or block suspicious activity. Traditional anti-virus relies on a vast database of virus signatures to help the software identify malicious applications on your computers. Modern malware can easily be modified to not match existing signatures.

Popular NGAV end point protection tools include Microsoft Defender Advanced Threat Protection, BitDefender Gravity Elite, CarbonBlack and CrowdStrike's Falcon/Protect. Behavior-based endpoint protection is an efficient way to protect against new threats and prevents ransomware from spreading throughout your network.

RANSOMWARE DEMANDS HAVE RISEN FROM $25K TO $1MIL IN 2019

Don't just be insured, be prepared.

For more information, please contact us:

Lindsay Minzey
Business Development Specialist
LHA Trust Funds
225.368.3830
lindsayminzey@lhatrustfunds.com

LHA TRUST FUNDS

TOKIO MARINE HCC