WELLS FARGO

Information and Cyber Security

Is your business doing everything it can to protect against ransomware?

What is ransomware?

Ransomware is a type of malware that blocks access to the victims' computer systems and data. Threat actors employ ransomware and then threaten to publish confidential information or withhold access until a ransom is paid.

Attacks typically spread when a user clicks on a phishing email or visits an infected website. However, a number of malware channels are capable of delivering destructive software to computers, servers, or mobile devices.

Unlocking ransomware

A knowledgeable person may be able to "unlock" some simple forms of ransomware. However, more advanced versions use a technique called cryptoviral extortion. This technique encrypts the victim's files, making them inaccessible. The attacker then demands a ransom payment — usually in the form of digital currencies that are difficult to trace (like Bitcoin) — to decrypt the files. In a well-implemented attack, recovering the files without the decryption key is a complex problem.

During an attack, business operations are hindered or halted because they cannot access the information needed to run the business. Even after files are unlocked, victims must scan networks, clean the environment, and reinstall software. It is a time consuming, complex and expensive issue.

A commitment to cyber hygiene and best practices is critical to protecting your networks.

> "As ransomware has grown in complexity and popularity as a profitable attack type, 'to pay, or not to pay' is a question that more and more organizations have had to realize."
>
> — Wells Fargo Cyber Threat Intelligence, 2020 Cyber trends and predictions

Safeguarding against ransomware

Employing preventative controls, like the ones listed here, may reduce the chances of your business falling victim to a ransomware attack.

Web content filtering

This software filter limits user access to websites based on defined acceptable content and known malicious sites.

Sandbox testing

This tool proactively detects malware by inspecting and executing incoming files in a secure and isolated environment. The technique can be effective at detecting attacks against unknown or unaddressed vulnerabilities (also known as zero-day attacks).

Proxy and email

Filter out categories like uncategorized and no-purpose (placeholders). Block Microsoft Office 97-formatted documents. Look for gaps using Indicators of Compromise (IOC) from other known attacks. Use Antivirus on all attachments. Use phishing reputation scrubbing.

Patch vulnerabilities

Install software and firmware updates with a timed focus on critical and high risk vulnerabilities — especially ones that are tied to common ransomware. Avoid using software that is no longer supported by the vendor and cannot be patched.

Backup, backup, backup

Regularly backup all critical data and system configuration information on a separate device and store the back-ups offline. Verify backup integrity and your test restoration process.

Off-network security filter for laptops

Keep laptops from visiting websites or receiving email when disconnected from the corporate network.

Endpoint security agent

McAfee, Symantec, and Microsoft, to name a few, offer security agent options to prevent malware from launching and running on endpoints (that is, desktops, laptops, mobile devices, workstations, and "Internet of Things" devices).

Prevent installation of unapproved software and remove user access

Use application controls to block the installation of unapproved software on endpoints. Promptly remove end-user access when no longer needed. This control eliminates the ability for a local account to be used to install malicious software or ransomware.

Pre-approve software installation sources

Pre-approval lists explicitly allow only known, company-specific sources to deploy packages and software.

Protect file upload apps

Implement malware detection controls to protect your network perimeter applications that receive files.

An ounce of
prevention is worth
a pound of cure.

How to respond to ransomware

You’re hit with ransomware. Now what?

Ransomware is a scary situation— especially for small municipalities and small businesses who may have no idea what just happened.

Should preventative controls fail and you are affected by ransomware, time is of the essence. Having a plan in place and knowing what to do is critical.

Best practices

The Department of Justice and Department of Homeland Security along with U.S. government partners compiled technical guidance and best practices for government and private industry. They recommend organizations consider taking the following steps upon a ransomware infection:

- Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
- Contact any company that you regularly email or send data to so that they can protect their networks.
- Contact law enforcement immediately. DHS strongly encourages firms to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- If available, collect and secure partial portions of the ransomed data that might exist.
- If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
- Delete registry values and files to stop the program from loading.

The Cybersecurity and Infrastructure Security Agency (CISA) site offers more information on ransomware.

The generalized information contained in this document should be considered best practices and may not address specific security risks of your business. If you have concerns that you have been or may be impacted by ransomware, Wells Fargo strongly suggests you seek the assistance of a cybersecurity professional.

Answer the following questions to help guide development of controls against ransomware.

- Does your company remove executable file attachments (.exe), file archives (.zip or .rar), and JavaScript/Visual Basic scripts from email prior to delivery to organizational users?
- Does your company's email attachment scanning and filtering solution identify files based on their true file type and not via extension?
- Does your company have controls (like an enterprise solution for patch management and deployment) to keep all your IT assets up-to-date with latest security patches?
- Are systems that support auto-run for USB drives and devices and removable media configured to accept only company approved products or solutions?
- Does your organization's information security training program contain specific guidance on how to identify and report spam and ransomware?