EH Private Bank®
EH Private Bank is a Tradename of EH National Bank

Preventing Ransomware Attacks

A Client Information Resource from EH Private Bank
May 13, 2021

What do the NBA Houston Rockets, Washington DC Police Department, and Colonial Pipeline all have in common?

Each of these organizations has been victimized by a 'ransomware' attack…and it could also happen to you or your organization. If ransomware or an encryption Trojan gets onto your computer or network, it could encrypt your data, lock your operating systems and hold hostage all of the data that you and your business depends on every day. As soon as ransomware gets hold of a "digital hostage", such as a file, it demands a ransom for its release.

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
YOUR PERSONAL FILES ARE ENCRYPTED

Your online safety and security is always our utmost concern at EH Private Bank. Here are some tips to reduce the likelihood of finding yourself in front of a locked laptop or encrypted file, and paying horrendous sums for its *possible* recovery. It's important to be prepared.

Are you vulnerable to a ransomware attack?

Ransomware infections can occur in various ways, such as through insecure and fraudulent websites, software downloads and by spam email. It's important to know that ransomware targets individuals as well as companies of all sizes.

There are a number of factors that might make you the target of a ransomware attack. These can include:

- ***The device used is no longer state-of-the-art***
- ***The device has outdated software***
- ***Internet browsers and/operating systems are no longer patched (updated with latest security updates)***
- ***No proper backup plan exists***
- ***Insufficient attention has been paid to cybersecurity, and a concrete plan is not in place***

If one or more of these points apply to the device (or devices on your network), you are at risk of falling victim to a ransomware attack. A vulnerability scan, which can be performed by an IT security software specialist, can remedy this. The software scans the device(s) for possible security vulnerabilities in the operating system or in the programs installed on the computer. By detecting these vulnerabilities, which enable malware to infiltrate, it is possible to prevent the computer from becoming infected.

How can you prevent a ransomeware attack?

• Never click on unsafe links: Avoid clicking on links in spam messages or on unknown websites. If you click on malicious links, an automatic download could be started, which could lead to your computer being infected.

• Avoid disclosing personal information: If you receive a call, text message, or email from an untrusted source requesting personal information, do not reply. Cybercriminals who are planning a ransomware attack might try to collect personal information in advance, which is then used to tailor phishing messages specifically to you. If in any doubt as to whether the message is legitimate, contact the sender directly.

• Do not open suspicious email attachments: Ransomware can also find its way to your device through email attachments. Avoid opening any dubious-looking attachments. To make sure the email is trustworthy, pay close attention to the sender and check that the address is correct. Never open attachments that prompt you to run macros to view them. If the attachment is infected, opening it will run a malicious macro that gives malware control of your computer.

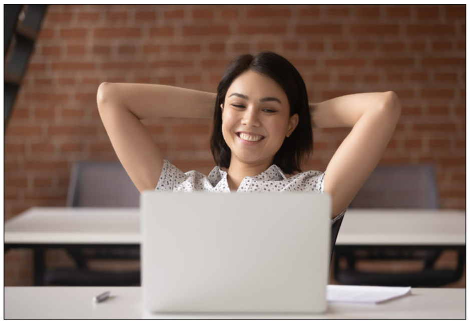
Preventing Ransomware Attacks

A Client Information Resource from EH Private Bank (Continued)

How can you prevent a ransomware infection? (Cont'd.)

- ***Never use unknown USB drives:*** Never connect USB sticks or other storage media to your computer if you do not know where they came from. Cybercriminals may have infected the storage medium and placed it in a public place to entice somebody into using it.

- ***Keep your programs and operating system up-to-date:*** Regularly updating programs and operating systems helps to protect you from malware. When performing updates, make sure you benefit from the latest security patches. This makes it harder for cybercriminals to exploit vulnerabilities in your programs. You or your company may also want to consider augmentation of your current security software to include anti-ransomware if its not already included and properly updated for current threats.



- ***Use only known download sources:*** To minimize the risk of downloading ransomware, never download software or media files from unknown sites. Rely on verified and trustworthy sites for downloads. Websites of this kind can be recognized by the trust seals. Make sure that the browser address bar of the page you are visiting uses "https" instead of "http". A shield or lock symbol in the address bar can also indicate that the page is secure. Also exercise caution when downloading anything to your mobile device. You can trust the Google Play Store or the Apple App Store, depending on your device.

- ***Use VPN services on public Wi-Fi networks:*** Conscientious use of public Wi-Fi networks is a sensible protective measure against ransomware. When using a public Wi-Fi network, your computer is more vulnerable to attacks. To stay protected, avoid using public Wi-Fi for sensitive transactions or use a secure VPN service.

Have questions or need help? We're just a phone call away. Call us at (323) 602-2000 or send us an email at *information@ehprivate.bank*

What should my company pay attention to for preventing a ransomware attack?

Ransomware attacks are by no means only a threat to individuals. In fact, companies are also frequently targeted. Not only large, lucrative companies fall victim to ransomware; small and medium-sized enterprises (SMEs) are targeted too. They often have poor security systems, and are therefore particularly attractive targets for attackers. Below is a list of factors that should be taken into account by companies wanting to avoid ransomware infection.

- ***Stay up-to-date...***with the latest operating software at all times – in the corporate environment too. Past experience shows (for example, WannaCry 2017) that companies that neglect this area are particularly vulnerable to ransomware attacks.

- ***Raise employee awareness:*** This is probably the most effective and important preventative measure of all. A person who knows what to look for will be far more successful at countering attacks and preventing losses and vulnerabilities to your organization. Implement a security protocol that enables employees to assess whether an attachment, link or email is trustworthy.

- ***Be prepared:*** Make sure there is a plan in case of ransomware infection. Give your employees a clear protocol for what to do if they suspect that there is a threat or that their device/network has been infected. If your device or network does become infected, the most important measure is to contain the threat as much as possible and prevent further infection or damage.

- ***Consider cloud technologies, if you haven't done so already:*** The advantage over on-premise systems is that vulnerabilities in cloud-based architectures are more difficult to exploit. In addition, cloud storage solutions allow you to restore older versions of your files. This means that if the files are encrypted by ransomware, you should be able to return to an unencrypted version using cloud storage.

- ***Backups...backups...backups!*** It is critically important to always back up business-critical data to external devices. Responsibility for this essential task should be clearly stated and communicated.