dti

CyberSecurity Spotlight

Presented by the Division of Technology & Innovation
On Behalf of the Clerk of the Superior Court for Maricopa County

August 8, 2022

What is Ransomware?

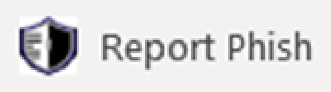
Ransomware is a type of malicious software, or malware, that gathers and threatens to publish a victim's personal data or block access to it unless a ransom is paid. Ransomware enters the network in a variety of ways. The most popular way is a download via a spam email attachment. The download will then launch the ransomware program that attacks your system and attempts to gain access to other systems on the same network. As soon as ransomware gets hold of a “digital hostage”, such as the files on your computer system, it will encrypt them and demand a ransom for their release.

Ransomware infections can occur in various ways, such as downloading software from a fraudulent website or clicking on a link in a spam/phishing email.

Reporting suspicious emails

If something about an email seems suspicious, report it. It is better to report something and find out that it is a safe email than not reporting and finding out it contains malware. It will also help the CyberSecurity team to identify other potential victims that may have also been sent the same email and to block any further emails from being received.

You can use the Outlook or Outlook Web Application phish alert button to report the phishing attempt. This button is located on the right side of menu bar. Highlight/select the inbox message then push the “Report Phish” button to report the message as a phishing attempt.



Or you can forward the email to DTICyberSecurity@maricopa.gov.

Note: If you are unable to report the email with the provided button in Outlook, you can right click on the message and forward it to the email address above without opening the email. But if you have already opened it, you should forward the email without clicking on any links or opening any attachments. In the event you clicked on a link or opened an attachment, you should immediately report the email and mention your activity so the cybersecurity team can determine the appropriate action to take.

Safety measures you can take to reduce the risk of a ransomware attack

Although several of these measures are already in place on Clerk's Office workstations, you should review and understand what you can do to prevent an attack before it happens. These measures would also apply to your personal computer for your own protections.

- **Always Have Antivirus Software Installed:** Ensuring that your antivirus software is automatically updated will prevent infections from known malware. Antivirus programs can detect and delete many types of ransomware programs quickly and easily so long as they are updated regularly. However, new ransomware is always being created and it is possible that the antivirus program is not aware of it yet.

- **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 then 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 you have 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.
- **Never Use Unknown USB Sticks:** 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.
- **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.
- **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.

The five biggest ransomware payouts as of March 2022

Ransomware is big business as you can see by how much some companies have had to pay to have their data restored. Taking time to scrutinize emails and website links as well as taking the security measures outlined above can drastically reduce the risk of you falling victim to a ransomware attack.

- Brenntag - $4.4 million
- Colonial Pipeline - $4.4 million
- CWT Global - $4.5 million
- JBS Foods - $11 million
- CNA Financial - $40 million

For questions or concerns

Please email the DTI CyberSecurity Team for assistance at DTICyberSecurity@maricopa.gov.

Looking for Prior Spotlight Editions?

Prior editions can be found at the DTI CyberSecurity Spotlight page on Clerk Connect.

Clerk of the Superior Court, Maricopa County
620 West Jackson Street
Phoenix, Arizona 85003