Ransomware: Don’t Let Bad Digital Hygiene Paralyze your Computer

By District Attorney Summer Stephan

When hospitals or gasoline pipelines are paralyzed from operating because hackers installed ransomware that forced a temporary shutdown, it’s a good time to emphasize that everyone is at risk for falling prey to digital threats.

Technology is constantly evolving and our own reliance on that technology is intertwined on nearly every level of life. That’s why it’s vital to have good digital hygiene – which is cleaning up and maintaining your electronic information or assets and regularly updating them. As with most things, bad actors have found ways to exploit technology for their own gain. A day rarely goes by without a headline describing a recent hack or exploit utilizing ransomware.

Ransomware locks out the rightful user of a computer or computer network and holds it hostage until the victim pays a fee. Ransomware hackers also threaten to leak sensitive information to get victims to meet their demands. On a larger scale ransomware could prevent a hospital from providing important medical services. On a smaller scale you could lose access to every family photo stored on your computer.

The most common ways ransomware can infect a computer include:

* Phishing emails that contain a malicious link or attachment.
* Intentionally downloading files from a website, which unknowingly contains the malware.
* “Drive-by” downloading, which can occur when a user visits an infected website, and the malware is installed without the user’s knowledge.
* Through social media and web based instant message applications.
* Through browser security holes, which are used by bad actors when visiting a malicious website.
* Remote access to your system using compromised usernames and passwords.

While Benjamin Franklin couldn’t have foreseen the technology we have today, his famous quote, “an ounce of prevention is worth a pound of cure” is great advice when it comes to cyber security. Often a user’s data can be irretrievable if they fall prey to ransomware. So, preventing these infections in the first place and planning are the best ways to keep your precious data safe. Keep your data safe by following these tips:

* Do not download attachments from unknown senders. Before clicking on an attachment think about whether it could be a malicious attachment.
* Do not click on links in emails from unknown senders. Bad actors often send emails that seem like they are from legitimate sources. Inspect the email closely to look for defects or clues that indicate it is not from a legitimate source.
* Use strong and unique passwords for each device or service you use. It should be 10 to 15 characters with lowercase and uppercase letters and include numbers and symbols.
* Backup your data regularly.
* Keep software updated on all devices – this includes updating the operating system of your computers and smartphones and the applications installed on those devices.
* Use two-factor authentication for online accounts, when applicable.
* Use the built-in anti-virus software on your computer or install trusted anti-virus software. Ensure the anti-virus software is updated and scan your system regularly.
* Turn off the option to automatically download email attachments – to simplify the process of reading email, many applications include a feature to download attachments without user confirmation

If you fall victim to a ransomware attack, law enforcement does not advise paying a ransom, because it does not guarantee you will get your data back and may only serve to encourage the perpetrators. Instead, report the incident to your local law enforcement as quickly as possible.

As your District Attorney, I’m committed to increasing communication and accessibility between the [DA’s Office](https://www.sdcda.org/office/meet-da.html) and the public. I hope these consumer and public safety tips have been helpful.