Ransomware Prevention Guide

Gillware™ Digital Forensics

1802 Wright Street
Madison, WI 53704
forensics@gillware.com

Ransomware *is malware that denies access to files on your computer, mobile device, or network by encrypting them or making them otherwise inaccessible, and demands that payment be made in order to regain access.*

There are some basic actions you can take which will be helpful preventing a ransomware attack, or easily recovering from one if it occurs.

Back Up Your Files.

The one sure way to defeat a successful ransomware attack without having to pay ransom is to have the ability to recover your files from a recent or real-time back up. Before restoring your backup data, be sure that the computer system or network you are restoring is safe, and that all malware threats have been cleaned up and unauthorized remote access has been blocked.

Backing up files to a reputable cloud-based backup service or creating regular backups to an external drive that is not constantly connected to your computer or network can allow you to easily recover in the event that you fall victim to a ransomware attack.

Backups should be audited frequently to ensure that the backup is a complete set and the data is current. Ideally backups are contained off-site on a different network infrastructure. In the event of a crash or attack, backup restore should be performed targeting different equipment, so if the backups are found to be incomplete or stale the original storage has not been modified.

Be Informed and Aware of the Threats and Risks.

Ransomware infections are usually the result of risky end-user behavior. Phishing emails with malicious attachments or links that are opened by an end user can result in the installation of ransomware and other malware. Educating end users to avoid risky behavior can prevent infection in the first place.

Anti-Virus Software.

Installing and running up to date antivirus software from a reputable company can help to detect and stop malware, including ransomware. However, anti-virus software is not a perfect solution because malware developers are constantly updating and changing their software.

Keep your Systems and Software Up to Date.

Like other malware, ransomware relies upon vulnerabilities in your computer, mobile device or network's operating system and installed software. Enabling automatic updates of your devices, operating system, and software and keeping your systems and software up to date and patched reduces vulnerabilities and can prevent infection.

Limit User Account Access.

Setting up systems where users have limited privileges rather than Administrator or root level access can provide protection by preventing malware from being able to install itself if the account is compromised. Use of strong and unique passwords that are changed regularly can also assist in making computer systems more secure.

Mandate Strong and Unique Passwords & 2-factor Authentication for VPN.

A common Ransomware scenario we see at Gillware Digital Forensics is that a user gets a message from a known business contact from a professional networking site, asking them to view a proposal on a common file sharing site. The site they are directed to asks them to log in and they try. But it wasn't a legitimate site and they just got phished for their username and password. Worse yet, the bad guy who is hosting the fake site also has the victim's IP address.

Perhaps the victim's username is their email address, and they use the same password for their email server or even their LinkedIn account. Now their account can be used to phish other unwitting victims, and the bad guy can dig through all their emails. Perhaps the victim's desktop computer also has the same password and they aren't behind a strong firewall. Next, the bad guy will attempt to remotely access their Windows computer.

If a user has strong and unique passwords everywhere, and the VPN requires a second factor of authentication above and beyond user name and password, you can see how these precautions can mitigate the potential damage.