CYBERSECURITY HEROES

RANSOMWARE:
YOUR DATA, HELD HOSTAGE

Ransomware is particularly damaging malware that holds data for ransom and it's been on the rise.

Attacks with names like WannaCry, NotPetya, Cerber, Cryptlocker, Locky, and more have increased more than 350% each year, according to recent cybersecurity studies. The motivation isn't always purely financial; sometimes ransomware attacks are meant to disrupt critical services or infrastructure.

This malware prevents or limits a user's access to their system, either by disabling the system screen or locking files unless a ransom is paid. Attackers bluntly inform the user that they must make a time-sensitive payment in a virtual currency (typically Bitcoin) to see their files again. Even if users pay the ransom, there's no guarantee that the files will be unlocked or will be uncorrupted.

Ransomware doesn't discriminate. It targets everyone from executives to emergency services, from health care organizations to city infrastructure like power and water services. It even targets the average computer user. This malware is also device- and network-agnostic: If it can connect to the internet, or if it can connect to another device that has internet capability, it is susceptible to ransomware.

Just as importantly, it targets small businesses just as often as it targets larger organizations. In a study sponsored by Carbonite and performed by the Ponemon Institute, 57% of the respondents thought their business was too small to be targeted. Therefore only 46% thought it was important to take preventative measures. However, more than half of the businesses in the study had been victims of ransomware, sometimes more than once.

The important lesson here?
No company is too small, no device is immune, & taking preventative steps is always a good idea.

MITIGATE THE RISK of Ransomware Attacks

For ransomware, prevention is absolutely the best strategy. You can avoid organizational disruption by following some simple best practices.

1. **Use Robust Antivirus Software.** Check to make sure the cybersecurity software package you use can handle a wide range of threats. Base features should include antivirus and antimalware protection and some level of ransomware protection.

proofpoint.

2. **Don't Fall for Phishing Attacks.** While there are several common methods of delivery, a lot of ransomware is delivered through phishing and spear phishing emails with malicious links and attachments. "Phishing continues to be an efficient and popular method of infecting devices," says Jordan Wright, a R&D engineer at Duo Security.

3. **Be wary of attachments you do not expect.** Maintain an appropriate level of skepticism and contact the sources, even if they seem to be your coworkers, family members, or your bank. Many ransomware attacks start when a user unsuspectingly downloads an attachment which contains the malware.

   In one case, the infected files got in through an email attachment impersonating an invoice laced with macros (shortcuts in tools like Microsoft Word or Excel). If you get an email attachment that asks you to enable macros, or requests access to the internet, report it to your organization's IT or security personnel immediately.

4. **Don't click on links without verifying them.** Don't click on a URL whose domain is a set of numbers or a jumbled string of letters and numbers. Always hover over a link to reveal its true destination. And when it doubt, use a search engine to verify the domain.

Make Sure Everything is Up to Date

- **Browsers, add-ons, plugins, apps, and system software – including operating systems – are especially vulnerable to being exploited by malicious attacks.** WannaCry, the infamous 2017 ransomware attack that crippled large organizations in over 150 countries, took advantage of a Microsoft Windows vulnerability.
- **Keep all software, especially antivirus or antimalware software, up to date.** If your company asks you to apply a software update to a browser or other piece of software, do it immediately.

Protect Your Devices

- **Protect your own device** by using the guidelines above to protect yourself from a phishing attack. In addition, only download apps that are trustworthy.

Whether you are using your own device for company access or one issued by your company, don't allow others to use it. Recent surveys show that nearly 25% of infected employee devices became infected because they allowed an unauthorized person (such as a family member) to use it. It only takes a minute for an unattended child to accidentally click a malicious link.

Back Up Regularly to Safe Locations & Verify Your Backups

Automatic and incremental backups are the fastest way to resurrect your data after a ransomware infection.

- **Off Site:** Pick a trusted service that does automatic, scheduled backups
- **Physical:** Use an extra laptop, a portable hard drive, a USB drive, etc. Make sure to disconnect any external device as soon as the backup is done.

Don't back up just the important files, back up the entire drive. Backups can fail, so you should regularly verify their integrity and practice doing a restore from a backup.

Remember that backups aren't immune to ransomware. Sometimes ransomware can encrypt your backup files if they're attached to your computer via an external hard drive or USB stick. Other times, ransomware can sit dormant and undetected, just waiting for the right time to explode and wreak havoc, including in your backup files.

proofpoint.

Browse Safely

When browsing the web, take these two steps to keep ransomware away:

- **Disable browser pop-ups or use an ad blocker.** Ransomware can sometimes present itself as a fake antivirus installer, an ad on a credible website, or a login window to trick users into clicking on it. Disabling pop-ups and using a reputable ad blocker can reduce this infection vector.
- **Bookmark your trusted websites.** Websites can deliver ransomware to a system without downloading or clicking on anything. Bookmarking trusted sites ensures you won't mistype the web address to a malicious site.

Act Fast if You Suspect Infection

If you think your system or device is infected, immediately disconnect from the network–both wired and wireless. This means that if you are connected to the network via a wired connection (like an Ethernet cable), physically disconnect the network cable from your machine.

Next, alert the appropriate IT or security personnel in your organization to get help.