ConnectSafely

QUICK-GUIDE TO

Ransomware

Who is affected by ransomware?

We frequently hear about attacks against big companies, hospitals, cities, or government agencies, but anyone can be a victim. Unfortunately, there are cases of it happening to both adults and children.

How does it happen?

Ransomware attacks are usually a result of some type of intrusion into a computer or a network. Once inside, the criminals have access to all your data and the ability to encrypt your files so that only they have the digital key to unlock them. They can also pilfer through your files to look for confidential or embarrassing information that they can use to extort or blackmail you.

What is Ransomware?

Ransomware is malicious software that criminals use to attack your device and lock up your files unless you pay them a ransom. They sometimes also threaten to reveal confidential or embarrassing information if you don't pay. Sometimes even those who pay don't get their data back.

How can you prevent being a victim?

- Make it harder for a criminal to access your devices. Be sure that your device's operating system and all your software — especially your browsers — are kept up to date with the most recent security patches. Windows and Macs can be configured to update or notify you about a necessary update automatically, but both enable you to check manually, which is a good idea. For instructions on how to update operating systems for Windows, Macs, iOS and Android, visit ConnectSafely.org/updates.

- Don't be a phishing victim. Be very careful before clicking on any links in an email, even if the sender is someone you know. They could be leading you to a malicious site. If you get an email that appears to come from your bank or other trusted source, check with them before clicking on a link or access the company's website directly from your browser rather than clicking.

- Use antivirus software to protect your devices.

- Always have an up-to-date backup of all your data so — even if there is a ransomware attack, you can recover your data without the aid of the criminals. Consider a cloud backup and synchronization service that automatically backs up files as they're created on the service's servers so, even if something happens, the data is safely stored off-premises. Dropbox, Microsoft, Apple and Google offer cloud services which – in some cases — are free or bundled with other software (like Microsoft Office). Also, backup to an external device like a high-capacity thumb drive and consider putting a copy of essential data in a fireproof safe or store it away from your home or office.

What can I do if I'm a victim of ransomware?

- The FBI "does not support paying a ransom" and points out that paying doesn't necessarily mean you'll get your data back, plus it "encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."
- Contact your local FBI field office plus your local police department. It's always important to report crimes, but it's very unlikely that the police or FBI will be able to recover your data.
- If you have a backup, you can recover your files without having to pay the ransom. Don't worry about your software or computer operating system. If you need help, any computer expert can help you recover your operating system and any software you need to reinstall.
- Visit the No More Ransom website for advice on how you might be able to recover your data; the organization says that it is "sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay," but they do advise that, "in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place."

For more info, visit ConnectSafely.org/security

GO

The FBI does not support paying a ransom and points out that paying doesn't necessarily mean you'll get your data back.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

Revised 5/17/21