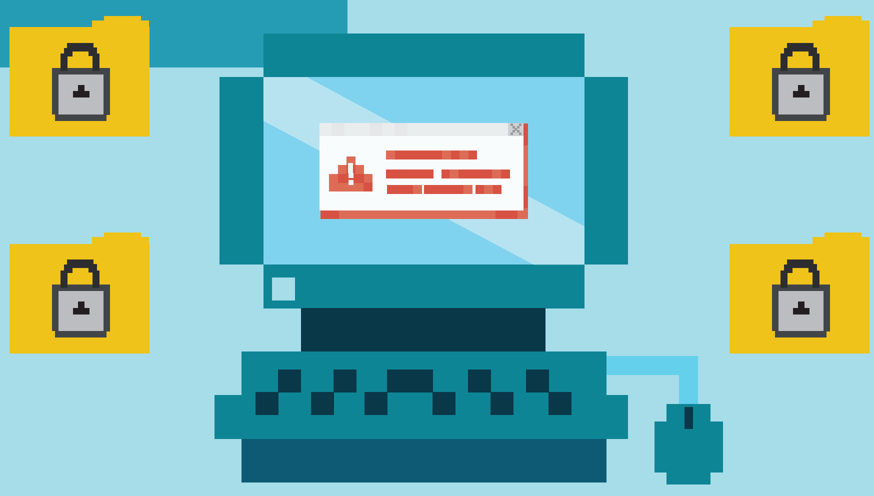
UNDERSTANDING RANSOMWARE

RANSOMWARE Q&A

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software — that is, malware — that blocks access to a device or data until a ransom is paid. Ransomware can affect computers and mobile devices, and both organizations and individuals could be targeted by attackers.



What Does Ransomware Do?

When a device is infected with ransomware, some type of digital lock or encryption is applied, effectively preventing you from accessing your files or your device. If you are infected, you will receive a ransom message from the attacker asking for payment which, allegedly, will grant you access to the digital key needed to unlock your files and/or system.

How Much Are Ransoms?

In the early days of ransomware, payment demands trended relatively low. But as the malware has evolved, average ransoms have escalated sharply. And when an attack is widespread, threatening an organization's ability to operate or serve its customers, attackers can be very aggressive. There have been numerous published accounts of multi-million-dollar ransoms. Ransomware costs organizations billions of dollars every year–though the true cost is difficult to determine, because many incidents go unreported.

How Are Ransoms Collected?

Attackers generally require ransoms to be paid in Bitcoin or another "untraceable" electronic format. These "cryptocurrencies" are fully digital. They are created and held electronically, have no physical form, and are not controlled by any banking entity. In addition, cryptocurrencies are volatile; their monetary value changes frequently, which means the value of a ransom demand (or payment) can fluctuate over time.

RANSOMWARE PREVENTION AND PROTECTION

To Pay or Not to Pay?

Security experts and law enforcement officials — including the FBI — advise against paying a ransom. Paying only encourages these types of attacks.

However, if an organization or individual has not backed up files to a secure location, paying the ransom might be regarded as the only option for recovering data. Though some services claim they can recover files without the decryption key, it can be next to impossible to reverse an infection.

Will Paying a Ransom Restore Access to Data and Devices?

Sometimes. But there have been known instances in which the attackers never delivered the decryption key following payment. In addition, there have been cases of ransomware with critical programming flaws that rendered data unrecoverable, even with the key. In other cases, an organization has paid the ransom only to be hit with a second, larger payment request.

BOTTOM LINE:
Don't count on 'honor among thieves.'

Doesn't My Organization Have Cyber Insurance?

Some organizations may rely on cyber insurance to compensate for ransom payments. But this seems to have bolstered and increased the demands made by cybercriminals. And that is likely to lead to changes in policies related to ransomware coverage.

It's also critical to remember that the fallout of ransomware is often much more than the ransom itself. Organizations also experience losses associated with system downtime, hampered productivity, incident response, remediation, and so on. And cyber insurance typically won't cover loss of business associated with ransomware or other cyberattacks.

Can't I Just Put Everything in the Cloud?

It may seem logical that storing important files in the cloud would protect you from ransomware and make restoring data easy in the event of an infection. But not so fast. Your computers and mobile devices connect to the cloud services you use. And some types of ransomware are specifically designed to seek out and infect cloud files.

If a backup repository — like an external hard drive or cloud storage — is connected to a computer or mobile device at the time of an infection, it could also be compromised. To truly preserve files and data, create an offline backup.

DON'T BECOME A RANSOMWARE VICTIM!

Know how to prevent an infection and be prepared to recover your data if you do get hit.

AVOID
unknown links, ads, and websites.

DON'T
download unverified attachments or apps, and don't access pirated content like illegally copied movies, music and software.

KEEP
software up to date and patch known vulnerabilities.

AUTOMATICALLY BACK UP
data and files to a secure location daily or even hourly (if possible). Create an offline backup for your most important data and files.

REPORT
any ransom message, suspicious emails, or suspected ransomware activity to your security team as soon as possible. Quick action is critical when ransomware strikes.

We deliver security awareness and training about a range of cybersecurity threats, including ransomware.

Our assessment and education tools change behaviors and reduce risk in the workplace and beyond.