Help Protect Your Business from Ransomware

DON'T do business WITHOUT IT™

We have your back when it comes to helping protect your business from data security threats, including ransomware. With ransomware, attackers threaten to publish or block access to your company's data or computer systems until you pay a sum of money or "ransom."

Costly to your bottom line — and your reputation

A ransomware attack can happen to *any* business — regardless of size — limiting your ability to access critical data and resulting in significant recovery costs, including reputational damage, technology restoration and legal and communication costs.

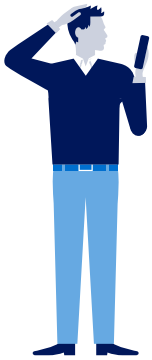
How a ransomware attack can happen

Though ransomware attacks can vary, they often occur when malware is downloaded on your computer or when your login credentials are stolen. This commonly happens with applications that allow you to share your screen, as well as emails, and web/ecommerce programs.

See next page for an example of a ransomware attack.

Tips for preventing a ransomware attack BEFORE it happens

1. Validate your data security using the Payment Card Industry Data Security Standards (PCI DSS). These guidelines provide a baseline of technical and operational requirements that can help you build a strong data security foundation.
2. Install system updates and patches to address vulnerabilities.
3. Educate all your employees on how to avoid phishing.



What to do if you're a victim of a ransomware attack

1. Contact appropriate law enforcement agencies for guidance.
2. Notify the American Express Enterprise Incident Response Program (EIRP).

Learn more about ways to protect your business at **americanexpress.com/datasecurity**

An example of a ransomware attack*

Joy clicks on an email from a shipping company inviting her to check the status of a delivery. She is directed to a fake website, which installs malicious software on her computer (a cyber threat known as phishing).

The software then gives an attacker access to her computer. Joy becomes aware when she attempts to access her browser and is greeted with a ransom note that says:

> **"The files on your computer have been attacked by a virus. You must pay $100 within 24 hours to regain access to your data."**

Joy could pay the ransom, but knows the attacker may not grant access to her data. Instead, she contacts her local FBI office and reports the crime. She also contacts American Express EIRP to report the incident.

**Example is for illustrative purposes only.*

Additional resources

PCI SSC Guide to Safe Payments

PCI SSC Ransomware Resource Guide

CISA MS-ISAC Ransomware Guide

PCI DSS Responding to a Data Breach

Learn more about ways to protect your business at **americanexpress.com/datasecurity**

Sources:

https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Ransomware_Resource_Guide.pdf?agreement=true&time=1632353461140

2021 Verizon Data Breach Investigation Report (see pages 25, 26, 55, 56)