

Defending Against Ransomware

A Resource Guide from the
PCI Security Standards Council

RANSOMWARE IS THE FASTEST GROWING MALWARE THREAT.

Criminals are attacking businesses with a type of malware that holds business-critical systems and data hostage until a sum of money is received.¹

1 Source: [FBI](#)



UNDERSTANDING THE RISK



\$1 BILLION A YEAR

The estimated cost of ransomware crime in 2016²



In 2015, cybercrime victims paid out
\$24 MILLION
to criminals deploying ransomware³



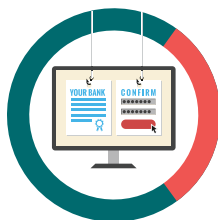
600% GROWTH

in new ransomware families
since December 2015⁴

2, 3: Source: [ZDNet](#)

4: Source: [Proofpoint](#)

THE ATTACK



30%

of users open
phishing emails,
and more than 12
percent click on
their attachments.

PHISHING EMAILS

Phishing emails are a common delivery vehicle for ransomware. These emails look legitimate, such as an invoice or electronic fax, but they include malicious links and/or attachments that can infect your computer and system.⁵



99%

of computers use
software that is
vulnerable to attack
if not updated⁶

WEBSITE AND SOFTWARE VULNERABILITIES

Criminals plant ransomware on websites and take advantage of software vulnerabilities to launch attacks on visitors using outdated software (browser, browser plugin).

5: Source: [2016 Verizon Data Breach Investigations Report](#)

6: Source: [Heimdal Security](#)

PROTECT YOUR BUSINESS

BE AWARE



Train your employees. PCI DSS 12.6

- Develop a plan that educates your employees on the best ways to avoid these types of attacks and how to handle an attack if one does occur.
- Make sure they are aware of the risks and understand that it's okay to delete the email if it looks suspicious.
- Think before you click. Emails can look like they come from anyone in the company. If there are any questions, always contact that person to confirm before clicking on a link or opening a file.

STAY VIGILANT



Test your systems. PCI DSS 11.3

- Have you tested your systems lately to see if it's easy for someone to break in? Criminals are persistent, you should be too.
- A vulnerability provides a "broken" door that criminals can just walk through. It's important that any vulnerabilities found during testing are fixed and that you have other controls in place to prevent a malicious individual from getting into your systems.



Patch. PCI DSS 6.2

- Your vendors send you "patches" to fix problems in your payment systems or other systems.
- When is the last time you checked for new security patches from your payment system and software vendors?
- Patches close doors criminals use to get into your systems. Follow your vendors' instructions and install patches as soon as possible.



Monitor. PCI DSS 11.5

- Are you monitoring your systems for changes? Have suspicious or unauthorized/unapproved changes been investigated?
- Monitoring changes in your systems helps you see when someone makes a change you did not authorize or approve. Investigating the changes as soon as they happen helps you find problems more quickly and improve your chances of shutting down an attack.
- A change management process will help you determine if changes are approved. If the change was not approved or is unknown, you should immediately investigate to determine if your system has been compromised.



Back up your systems. PCI DSS 9.5.1, 12.10.1

- Be careful that your backup does not overwrite previous good backups. This may help prevent backing up the data encrypted by ransomware and overwriting a good backup. Good practice, regardless of the backup method, is to take regular full disk backups and incremental backups (which only back up the data that is new since the last backup).
- To reduce your risk, avoid keeping backup data online (connected to the systems that are being backed up). Instead, store your backup data offsite and offline (storing your backups "in the cloud" is a common method for offline storage; however, see last bullet). This makes it easier to recover your most recent backup if your data files are held for ransom.
- Keep multiple generations of backup and have a retention period consistent with your organization's ability to detect ransomware and its ability to reconstruct using older records.
- Have you tested the integrity of your backups recently? Have you tested the backup and recovery process recently? Making sure you can recover data from your backups is crucial in the event your systems are locked by ransomware.
- When using cloud backups ensure your cloud service provider is being diligent and protecting against malware of all kinds. Cloud storage may also get locked by the attacker if connected to the backup systems doing persistent synchronization.

MAKE A PLAN



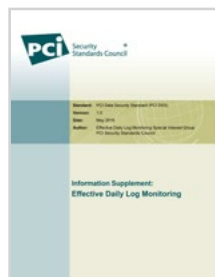
Prepare. PCI DSS 12.10

- You and your employees should know how to respond to an attack and what to do when it happens, including who to contact.
- Make sure you have a plan in place and communicate it to your employees.
- Review this plan regularly and make an ongoing commitment to educating your staff.

PCI IN-DEPTH BACKGROUND MATERIALS



[PCI Data Security Standard Version 3.2](#)



[Information Supplement: Effective Daily Log Monitoring](#)



[Defending Against Phishing & Social Engineering Attacks](#)



[Protecting Your Customer's Payment Card Data from Malware](#)



[Best Practices for Implementing a Security Awareness Program](#)

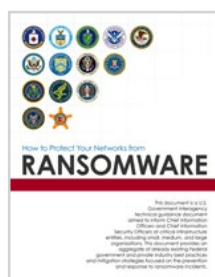


[Payment Protection Resources for Small Merchants: Guide to Safe Payments](#)

RELATED INDUSTRY RESOURCES



[Data ransomware: User and file space error](#)



[Ransomware and Prevention Response for CISOs](#)



[No More Ransom Project](#)



[How to Protect Your Networks from Malware](#)

For expert comment or questions, please contact: press@pcisecuritystandards.org
For more information on PCI Standards and resources, visit: www.pcisecuritystandards.org.