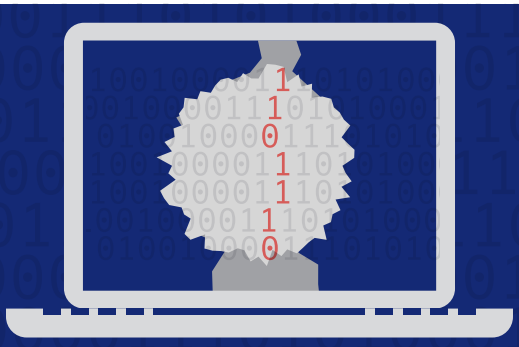
Help Protect Your Business from Zero-Day Vulnerabilities and Attacks

DON'T do business WITHOUT IT™

By welcoming American Express, you have access to information to help you protect your business and customers from new and ever-changing data security threats, including zero-day vulnerabilities and attacks.

What are zero-day vulnerabilities and attacks?

A **zero-day vulnerability** is an unknown security bug or flaw that exists in applications, operating systems and database software. Sophisticated hackers may immediately exploit this flaw and use it to attack your systems with malware in what is known as a **zero-day attack**.



How a zero-day attack could harm your business

As with most cyber threats, a zero-day attack can happen to any business at any time and could present significant risk to:

- Your daily operations and revenue
- Customer data
- Your brand or reputation

Steps to protect your business from zero-day vulnerabilities

1. Make and maintain a systems inventory list.

- Document the type of system/software, manufacturer/creator, model number, version number, serial number and service contact if there's an issue.
- Keep this list up to date to help you understand when a new zero-day vulnerability impacts your business.

2. Conduct vulnerability scans and install security patches.

- Scan all external/Internet-facing components (e.g., ecommerce sites, web servers, email servers) at least quarterly.
- Install critical vendor-supplied security patches within 1 month of release and non-critical patches or updates within 2-3 months of release.
- Subscribe to and monitor vendor communications, so you'll be notified when new patches are released.

3. Deploy a change detection solution.

- Use file and webpage integrity monitors for ecommerce sites to help quickly identify unexpected changes to your business systems.
- When you use these tools, you'll receive an alert when applications, operating systems or databases do not match trusted baselines.

IMPORTANT: Alerts from these systems must be monitored and acted on to be effective.

If you experience a zero-day attack, please contact **American Express® Enterprise Incident Response Program (EIRP).**

An example of how to manage a zero-day vulnerability scenario*

Situation:

Devon uses software ABC to track his inventory and accept payments from his customers. Unbeknownst to him and the software developer, there is a bug in the software, which could allow a sophisticated hacker to install malware on Devon's computer systems, making his business and cardholder data vulnerable.

Devon receives an email from the software company about a needed fix for a zero-day vulnerability.

Steps to protect his business:

Devon checks the information on his inventory list (type of system, manufacturer, version number and service contact) to verify that the email can be trusted.

Devon makes sure his technology partner:

- **Installs the security patch** provided by the software company as soon as possible but within the next 30 days.
- **Closely monitors** the change detection solution until the fix is installed.
- Uses the information provided by the software company to **check whether the vulnerability has been exploited** by a hacker or not.

**Example is for illustrative purposes only.*

Additional resources

What is a zero-day vulnerability?

Document Library for safeguarding cardholder data

PCI Data Security Standard Approved Scanning Vendors

PCI DSS Guide – File Integrity Monitoring

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