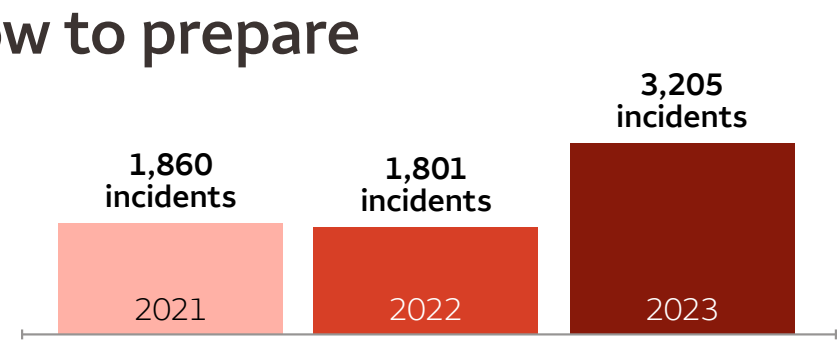
WELLS FARGO

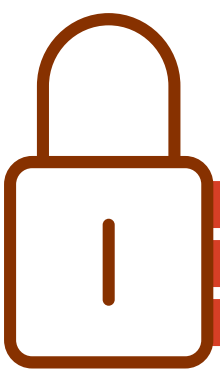
Global Treasury Management

Cybercrime and your company payments

What to know and how to prepare

Cybercrime is a reality for businesses. In fact, 2023 set the record for the most publicly disclosed security compromises at U.S. companies in a single year.[1]





Safeguard your business

- Financial losses
- Reputational damage
- Theft of sensitive data

Businesses face risks every day from threat actors around the world who deploy ransomware, phishing, malware, imposter fraud, and other techniques.

Prevention and early detection help your business avoid these risks.

9 Steps to help protect your payments

Best practices	Actions
Know your risk landscape The more you know about current threat actors and potential vulnerabilities, the better you can help protect your company, your customers, and your payments.	Stay up-to-date on the latest cybersecurity threats and trends Assign responsibility to dedicated resources in your company Leverage publicly available data such as government websites
Protect your data and network Start by identifying the critical systems and devices you need to protect, then create an in-depth defense with a multiple, continuous layers.	Look beyond desktops and servers; include laptops and mobile devices Block as much suspicious activity as possible Set up alerts and respond quickly to any potential issues
Backup critical data Maintain redundant data in a secondary, secure location; backups will help your company continue to operate if an attack occurs.	Review procedures around customer data, employee data, and key transactions Test how quickly you can recover if something goes wrong Make backups a part of your business continuity plan (BCP)
Establish and test your BCP playbook Don't wait for an incident to figure out how to respond; create your processes proactively and train your team on a regular basis.	Identify gaps and test your responses Learn and improve continuously Reach out to your bank for recommendations
Understand your computer network ecosystem Evaluate all the access points to your network and data, then consider how to help prevent an impact outside your organization from potentially cascading to you.	Review and understand your entire network footprint Assess risk factors when connecting with customers and trading partners Set and enforce standards for third parties with network access
Update your software and antivirus Fraudsters will actively exploit businesses that fall behind on their threat protections. Minimize your risk for viruses, malware, and other incursions with up-to-date solutions.	Maintain adequate software and antivirus programs across your organization Install updates and security patches proactively Monitor alerts and reports to prevent and detect malware and viruses
Be wary of business email compromise Thanks to artificial intelligence (AI) and social engineering, cyber criminals can deploy even more sophisticated phishing attempts that target company employees.	Watch for SMS text messages with bogus links Protect against impersonation by limiting what employees can share online Alert customer support about imposters trying to reset passwords and credentials
Consider a managed services provider Outside experts can provide additional resources and help you build peace of mind in your fraud-fighting capabilities.	Supplement your on-staff team with contract network security service providers Set up ongoing monitoring and apply best practices Be prepared to respond swiftly if incidents occur
Remain vigilant Watchful and educated employees remain one of the best defenses against suspicious activity, payments fraud, and security breaches.	Share regular updates on potential threats Conduct frequent training with all employees Make it fast and easy to report emails, calls, or other activity that's out of the norm

1. Identity Theft Resource Center, Q3 2023 Data Breach Report.

TM-3296 RO-3550143 LRC-0524