First Republic
It's a privilege to serve you®

Best Practices to Keep Your Payment Systems Safe

Businesses face increasing challenges in creating a secure online environment. We've assembled the following best practices to help you work toward minimizing risk.

Reconcile online banking activity frequently. Review all online activity at the beginning and end of the workday.

Implement a strong multifactor authentication process. Ensure that individuals remotely accessing your network, email or payment systems are in fact who they say they are by verifying their identity through at least two factors. For example, an individual would log in using a unique password (something they know) and then enter a code sent to their smartphone (something they have) to create and release payments.

Segregate financial transaction responsibilities (dual control). Require at least two users to initiate, approve and release wires or ACH payments. Ensure that no single user can perform all three steps in the payment process.

Train employees to protect themselves and your company.

- Protect online passwords and do not share them with anyone. Do not use the same username and password for other online accounts (e.g., social media, email, payment systems and online banking).
- Create strong, complex passwords and change them regularly. Choose a password that is over eight characters long and uses both upper- and lowercase letters, numbers and symbols in nonobvious arrangements.
- Be suspicious of unexpected emails. Do not open attachments, click on links, or respond to emails from suspicious or unknown senders. These activities can potentially infect computers with malicious software that allows hackers to steal confidential information or perform fraudulent transactions.
- Report malicious emails ("phishing") and any suspicious or unexpected activity related to online banking.

Install enterprise tools to protect your network.

- Limit the ability of employees to access their personal email and social media accounts and prevent access to websites with inappropriate content, such as gambling, pornography and hate sites.
- Scan and filter inbound emails to detect spam and malicious content.
- Cyberthreats often take aim at your data. Ensure that you have data loss prevention technology in place to detect and prevent the unauthorized movement of data out of your organization.
- It's important to secure and back up files in case of a data breach or malware attack. Have requirements in place about how and where to back up data. Important files can be stored offline, on an external hard drive or in the cloud.
- Have zero-day technology in place to mitigate the risk of unknown vulnerabilities being exploited.

Secure all computer systems and mobile devices.

- Keep your workstation, server operating systems, applications and web browsers up to date.
- Use and update spyware and virus protection software.

- Keep an accurate inventory of physical devices, software platforms and applications, maps of network resources, connections to company networks and logging capabilities.
- Data breaches could begin from within the company. You should monitor all users who have temporary access to your organization's computer network. It's important to restrict third-party access to certain areas and remember to deactivate access when users finish their work.
- Be wary of conducting money movement activities, viewing statements, or downloading documents on public or shared computers.

Dedicate a single computer exclusively for online financial transactions, if permitted by your business processes. Do not allow the computer to be used for email or general web surfing. This will minimize the possibility that the computer could be infected through emails with malicious attachments or links to fraudulent websites.

Regularly perform assessments of the technology, processes and controls used for banking and transactions to identify any weaknesses or vulnerabilities.

Devise a comprehensive incident response plan that integrates with your current IT incident response process.

Prioritize cybersecurity. Make sure management teams understand the importance of adhering to cybersecurity best practices and consider adopting a formal security framework with baseline capabilities.