BUSINESS SECURITY CHECKLIST

Strong security is something we build together. This practical checklist can help your business stay ahead of fraud, strengthen your defenses, and enhance payment security.

CHECKS, ACH AND WIRE

☐ Regularly review the authorized personnel who have access to your bank accounts, especially those with check issuance, ACH initiation, wire initiation and approval access.

☐ Always verify changes to payment instructions:

- Be mindful of any email requests to change payment accounts or institutions.
- Confirm updates with a known contact at the recipient.
- Never call or click on details presented in a change request email without verifying independently.

☐ For consistency and transparency of errors and fraud, use:

- Mitigation tools like Check Positive Pay, Teller Positive Pay and Payee Positive Pay.
- Wire-transfer templates or Wire Block solutions.

☐ Adopt dual-authorization protocols and callback procedures:

- For all electronic funds transfers.
- To decision exception items.

☐ Introduce stale-date and maximum dollar threshold protocols for check items to help ensure only intended payments are processed.

☐ Establish transfer limits for all wire transactions.

☐ Diligently monitor your account for all non-standard check, ACH and wire transaction activity.

☐ Regularly check your account to make sure transactions are posting correctly.

CARD ACCEPTANCE

☐ Implement tokenization and encryption security for terminal and web-based transactions.

☐ Adopt and utilize EMV card capabilities.

☐ Establish Payment Card Industry Data Security Standard (PCI DSS) compliance and complete self-assessments annually to identify gaps.

CONDUCTING ONLINE BUSINESS

☐ Strengthen your network by:

- Ensuring all systems have up-to-date and patched software.
- Implementing backup procedures.
- Using a secure firewall, monitoring VPN connectivity and maintaining anti-malware solutions.

☐ Restrict or block access to:

- Removable media devices, such as CDs, DVDs and USB devices.
- Email attachment formats commonly used to spread malicious programs, such as VBS, .BA and .EXE.
- Social networking sites.

☐ Educate employees on security best practices, password management, fraud and phishing awareness.

☐ Consider a cyber liability insurance policy to provide first- and third-party coverage for damages when private, personal or financial information is compromised due to a data breach or network intrusion.

Connect with your Treasury Management team to explore more security solutions and best practices.

Huntington Bank

Member FDIC. Huntington Bank is a service mark of Huntington Bancshares Incorporated.
©2026 Huntington Bancshares Incorporated. 2713563 | 02/26