first financial bank

2024 fraud awareness best practices

Payments fraud continues to be a significant business challenge. According to the 2023 AFP® Payments Fraud and Control Survey, in 2022 65% of organizations were victims of payments fraud attacks/attempts and 71% of organizations were targeted by a Business Email Compromise scam. If that sounds alarming to you, you're not alone. But we can help your business be more efficient in identifying potentially fraudulent transactions and equipping you with a proactive approach to protecting your accounts from unauthorized activity.

PAYMENTS

- [ ] Segregate vendor selection and billing.
- [ ] Flag duplicate invoices.
- [ ] Utilize all available fraud prevention tools (Check Positive Pay, ACH debit filters, control account structure).
- [ ] Use a company credit card to pay vendors when possible.
- [ ] Confirm payment instruction changes via a trusted manual call.
- [ ] Implement user limits for electronic payment originations.

PROCESS

- [ ] Prepare response and recovery tactics to understand how to react to current cyber-attack scenarios.
- [ ] Review account signers and online banking administrators annually, or more. When an administrator or online account user leaves the company, be sure to discontinue access immediately.
- [ ] Regularly reconcile all bank accounts - in some instances daily. Some company ACH charges only provide a 24-hour notice to Bank of fraud. If outside that 24-hour window, the company unfortunately is responsible.
- [ ] When possible, take all mailed payments into a post office to avoid thieves taking advantage of standalone mailboxes.
- [ ] Back up all operating systems regularly and consistently. Keep backed-up data stored off site and test regularly.
- [ ] Conduct routine employee training and testing so your staff is aware of what to look for.
- [ ] Practice dual authorization for all payment practices; for example, assign one associate to creating the ACH/Wire or paper check detail, and another associate approves.
- [ ] Establish 2-factor authentication wherever possible. While SMS is a common 2FA method, it's susceptible to SIM swapping attacks. Consider implementing additional 2FA options like mobile app authentication, hardware tokens, or security keys to fortify your defenses.
- [ ] If payment instructions change, organize dual control while making the change. Assign one associate to contact the vendor and validate the payment changes, while another associate to enter the changes.
- [ ] Consider the use of a dedicated treasury workstation. Limit access to only necessary bank and financial applications to eliminate the opportunity for surfing or clicking on malicious links.

SYSTEMS

- [ ] Hire a comprehensive cybersecurity risk management company to ensure your systems are secure and protected.
- [ ] Understand what is covered in your cyber-attack insurance.
- [ ] Disable unnecessary peripherals (CD/DVD/USB) and restrict cloud access.