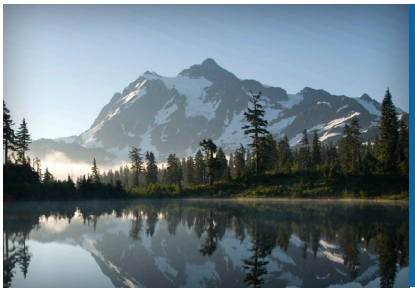

Protect Your Business from Payment Fraud

Targeted scams against businesses are on the rise as criminals leverage various methods to convince businesses that they are working with known partners or vendors.

One increasingly common method is the use of business email compromise (BEC). BEC is used to gain the trust of the business by creating a "spoofed" email address that varies slightly from a known contact. When BEC occurs, it may look like a request from an established business partner or even a manager or executive at your own company. The individual then requests fraudulent payment or transfer orders. Once sent, the payments are often unrecoverable. **It is important to take time to educate staff on how to avoid falling victim to these scams.**

Review Your Process for Authorizing Payments

It is critical for businesses to have strong controls for establishing new vendor payment instructions and changing existing payment instructions. By creating clear and concise procedures, you reduce the likelihood that staff might fall victim to these scams. Considerations include:

- Require a callback to the individual making the request using a pre-established or publicly available contact phone number.
- For internal requests, ensure staff know and are comfortable reaching out to verify the requests with members of management and/or executive leadership.
- If possible, consider segregating duties of who can create payments for those who release them.
- Add steps that include verifying the email contact information, letter by letter. Look for misspellings, additional punctuation, or changes to the email format.
- Be suspicious of spelling and grammatical errors, unexplained urgency, requests for the communication to remain confidential, unexpected, or unsolicited requests.

Develop a Response Plan

In the event fraud does occur, create a plan for staff to follow and respond effectively.

- Create and train a team to coordinate communication and recovery efforts.
- Notify the Bank and any impacted business partners as soon as possible.
- Review your insurance policy and notify the insurance company, if applicable.
- Scan computers and mobile devices with access to email for malware or viruses to identify where the compromise occurred and take action to repair it.
- Report the incident to law enforcement.
- After the recovery efforts have been made, review the events leading up to the transmission of the payment. Adjust the process if needed.

Even you can fall victim to a sophisticated scam

In recent months, several small businesses in our community have fallen victim to BEC payment scams resulting in over $200K in unrecovered losses.

In the event staff is unable to validate the legitimacy of the request, ensure the process includes what is expected from staff. Payment requests that cannot be validated should not be transmitted.

Peoples Bank is here to help. For more information contact your banking officer.

Peoples Bank

100 YEARS OF SERVICE 1921–2021

peoplesbank-wa.com/online-security