How to Identify Cyber Threats and Defend Your Company

Today's business culture focuses on speed. During times of change, including remote work locations, many people aren't as focused on security as they should be. Isolation, distractions and uncertainty are factors that can lead to hasty, damaging decisions. Cyber crooks are counting on multi-tasking and will target employees via email.

How to Identify Cybercrime Payment Schemes

The cyber crook targets your most vulnerable asset, your people. Their payment scams all feature one method—they utilize identity deception. Here are the most prominent scams being used today:

BUSINESS EMAIL COMPROMISE

- **CEO/CFO Fraud Scheme:** The fraudster compromises a high-level business executive's email account and uses it to impersonate the executive so they can send fraudulent money-transfer requests—wires or ACH—to internal victims. If you fail to verify the request and send the payment, your money will be lost.
- **Bogus Invoice Scheme:** The fraudster calls or emails a business impersonating a known supplier to trick you into sending funds to a new location. The thief will often provide a new bank account number or mailing address for the payment. If you do not independently verify the instruction before making the payment, your money will go to the crook. You won't recognize the fraud until your vendor calls to request payment on past due invoices.
- **Payroll Diversion Scheme:** The fraudster steals log-in credentials from an executive or employee and sends a request to Human Resources to change their direct deposit information. If you act without verifying the request, the crook gets the funds.

Three Steps to Cybercrime Resilience: Review, Validate, Authorize

Paying an invoice without an in-depth review can lead to real losses. You can avoid many of the traps set for you by a cyber thief by designing and implementing sound internal control procedures. Instill a new awareness with your staff. Instead of thinking "ASAP," train them to think "As Securely As Possible." Simply put—never trust, always verify.

Guidelines to Stop Payments Fraud

Solid internal controls validate all requests before changing. Consider these guidelines for your defense:

1: **Beware of "rush" requests and required confidentiality:** Scammers will insist the transfer take place immediately and/or that the transaction is confidential.

2: **Never authorize a wire or ACH payment by email request alone:** If the communication is email only, always independently verify the payment request is valid.

3: **Verify payment requests if the requestor—CEO or executive—is out of the office:** Always verify before sending any funds, and establish specific internal procedures on how to handle this type of request before it occurs.

4: **Validate all new payment instructions or changes:** All requests (including internal) must be independently confirmed. Always use the contact information you have on file to verify requests. Do not call the number cited in the request; you might call the crook.

5: **Be cautious if the request seems out of the ordinary:** The request or the amount may be unusual. Ask questions and request internal confirmation to proceed before paying.

Each of these situations involves processing and changes outside the norm. We recommend your internal controls address each case and note how your organization is signing off on a specific request. At minimum, if you can't verify the request, require proper manager approvals before making the payment. Be sure to include all executive assistants and accounting/payroll personnel in your fraud prevention training.

Minimize Cybercrime

Guard your computers

- Use firewalls and antivirus software
- Add protection with Trusteer Rapport (It's free for Treasury Services clients)

Use layered security controls

- Segregation of duties
- Protect/encrypt sensitive data
- Use multifactor authentication

Reconcile bank accounts—daily

Make training a priority

Add proactive fraud prevention to commercial checking accounts

Now Is The Time to Review Your Defense

The Minimize Cybercrime list implies a ranking; however, the best method of defense is to employ multiple layers of security and internal controls, not just focusing on one or two areas. Hancock Whitney encourages you to address fraud prevention with prudence.

Contact Treasury Services Client Support at 866-594-2304 with any questions or for information on preparing your fraud defense.

FRAUD DEFENSE
COVER ALL YOUR BASES

- Defend Your Business
- Secure Your Process
- Educate Your Staff
- Protect Your Banking Assets

hancockwhitney.com