Servis 1st Bank Best Practices

Tips to Protect Against Automated Clearing House (ACH) Email Scams

Criminals may target you by pretending to be your CFO, CEO or a trusted contact. Below are a few best practices to help protect your organization from ACH attacks.

1. Be wary of unexpected changes

Attackers will often use emails and phone calls to impersonate a trusted contact and convince victims to change account information for ACH transactions. Be cautious when receiving unexpected requests for account changes.

2. Use multi-factor authentication

ACH fraudsters often used stolen email credentials to log-in to legitimate email accounts and send emails to a company's clients and customers and ask them to send payments to a new account or bank. Using multi-factor authentication for email reduces the attacker's access to your company's email accounts, even if they have stolen credentials.

3. Read emails carefully

Examine email addresses in the reply field to confirm they match the exact spelling of the originating company's domain and the individual's name. Fraudsters frequently use deceptive lookalike domains to trick victims. They may also use fake phone numbers for fraudulent callback verification.

4. Perform a callback

Always perform a callback to the person making a request using a phone number from your records when setting up a new account, processing a request for payment, changing payment instructions, or changing contact information. Never trust that a phone number provided via email is legitimate.

Elements of a Callback

- Confirm all of the account details, including the new account number.
- Do not confirm payment instructions only via email – always perform a call back using a phone number from your records to the person making the request.
- If a callback is not currently a part of your company's payment control process, try to implement one or escalate the issue to someone who can.

5. Follow up on suspicious transactions

If you receive a call from the bank about a suspicious transaction, pay close attention to the information provided and reconfirm that your organization performed all applicable controls, including a callback. Clients often confirm payments as valid only to later report them as fraudulent.

What to Do If You Suspect Fraud

If you suspect fraud, immediately notify your ServisFirst Bank account officer.
The sooner you contact the bank, the higher the chances of getting your funds returned.

Servis 1st Bank®

For more information on how to protect your organization, please visit www.servisfirstbank.com/fraud-prevention-education/.

Please contact Cash Management with any questions at 866.922.5794 or contact your local banker.