ACH Security Best Practices

Safeguarding your account is a #1 priority at RCB Bank. Our online services use several different methods for your protection. Just to name a few, these methods include unique user IDs and passwords, multi-factor authentication, secure tokens and Secure Socket Layer (SSL) encryption protocol. We routinely install and upgrade systems for the newest technology available to deliver the highest level of security. Despite our efforts, we cannot control the initial point of compromise; that is, the computer used by the customer for their online banking activities.

Computer Access

As an originator of Automated Clearing House (ACH) payments, your computer security practices are essential to preventing fraudulent transactions. We encourage you to assess the measures you have in place to safeguard against unauthorized access to the computers used for online banking activities. We also encourage you to have a dedicated computer that has no email capabilities and limits internet access only to online banking sites.

Email Correspondence

Network users should never open emails from anyone they do not know or have a reason to trust. They should understand the hazards of browsing social media sites on the same computers used for online banking activities. They should also understand the hazards of clicking on any hyperlink in emails from unknown sources, especially in reply to a request for security information, warnings of account suspension, opportunities to make easy money, overseas requests for financial assistance and so forth. Suspicious emails should be forwarded to the Federal Trade Commission at spam@uce.gov and then deleted.

Anti-Virus, Firewall and Anti-Spyware Protection

Appropriate software should be installed, updated and active to protect your network or computer and its contents from unauthorized access. Setting these programs to update automatically will help ensure protection against the newest and latest threats. Please consult your network or computer specialist on the best applications for your environment.

Account Monitoring

Timing is a factor in stopping unauthorized ACH transactions. You and your staff should check accounts daily and report any unusual activity immediately. If a user replies to a fraudulent email or identifies an unauthorized transaction posting to the account, you should notify us immediately, report the incident to the local police and inform the FBI's Internet Crime Complaint Center at http://www.ic3.gov.

Most ACH cybercrimes result from stolen online banking credentials which allows the criminal to masquerade as the legitimate user of account transactions. Having these safeguards in place will help to detect and possibly remove potential threats.

The rules concerning ACH payments are constantly changing. To keep informed of the latest rules and guidelines for ACH processing, please visit www.nacha.org to obtain the current NACHA Operating Rules & Guidelines. They can be found in the NACHA eStore section.

Corporate Account Takeover (CATO)

CATO is a type of identity theft in which a criminal steals a company's online banking credentials and then uses them to initiate funds transfers via ACH (automatic payment), wire or bill payment.

Business Computer Security Tips

- Set up a firewall and actively manage it.
- Purchase and install anti-spyware/malware.
- Setup website, application and pop-up blocking. Your firewall and anti-spyware/malware as well as your end-point protection software can each be setup to block website or applications that may represent a greater risk for malware or fraud.
- Isolate one computer for banking use only. This will reduce the threat of being infected.
- Patch all systems. Enable automatic updates for operating system patches.
- Avoid connecting to public Wi-Fi networks with your business computers.
- Be cautious when clicking on links. Take time to open a browser and manually type in the URL to safeguard against false links.

Online Banking User Security Tips

- Do not share user IDs or passwords. Each user should have their own user ID and password, which should be secured and not visible or accessible to others.
- Use dual control when conducting funds transfers such as wires or ACH and require two users to complete the transaction - one employee to create the wire request and another to approve it before processing transactions.
- Keep your business contact information current. This is important in the event RCB Bank should need to contact you to confirm any suspicious transaction.
- Sign up for transaction and balance alerts through text banking* or online banking.

Common Scams

Business Email Compromise (BEC)	VICTIMS	INDICATORS
Targets a business or commercial client in the attempt to initiate a large funds transfer to an account under the fraudster's control.	CEOs, CFOs, Accountants, Bookkeepers, Accounts Payable	• Large wire or funds transfer to a new recipient. • Transfers initiated near end-of-day or cut-off windows; before weekends or holidays. • Receiving account doesn't have a history of receiving large funds transfers. • Receiving account is a personal account and the company typically only sends wires to other businesses.
Phishing	VICTIMS	INDICATORS
Internet based scam that a person, group or company is pretending to be legitimate but is just trying and compromise your information.	Anybody with access to the internet	• Fake links that want you to take action (i.e. update password). • Threatens to terminate your account if there is no action. • When you hover over link, the URL is not the actual site. *If in doubt, call the company directly using a known number to verify.*
SMiShing	VICTIMS	INDICATORS
Cell phone based scam that a person, group or company is pretending to be legitimate but is just trying and compromise your information.	Anybody with text messaging capibility	• Fake links that want you to take action (i.e. update account info). • The text message will indicate an urgent need to take action. *If in doubt, call the company directly using a known number to verify.*
Vishing	VICTIMS	INDICATORS
Phone based scam that a person or company is pretending to be legitimate but is just trying and compromise your information.	Anybody that has caller ID on their phone	• Caller ID spoofing makes it look like a call is coming in from a legitimate or known phone number. • When you answer, they ask for card numbers or other sensitive info. *If in doubt, call the company directly using a known number to verify.*

*Message, data rates and fees may apply. Member FDIC