Wire Transfers Security Best Practices

Safeguarding your account is our #1 priority at RCB Bank.

Our online services use several different methods for your protection, e.g., unique user IDs and passwords, multi-factor authentication, secure tokens and Secure Socket Layer (SSL) encryption protocol. To deliver the highest level of security, we routinely install and upgrade systems for the newest technology available. Despite our best 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 wire transfers, your computer security practices are essential to preventing fraudulent transactions. We encourage you to review your current security measures to safeguard against unauthorized access to the computers used for online banking. We also encourage you to have a dedicated computer that has no email capabilities and limits internet access only to online banking websites.

Email Correspondence

Network users should never open emails or attachments 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 permanently deleted.

Anti-Virus, Firewall and Anti-Spyware Protection

Appropriate software should be installed, updated and active to protect your network, 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 key factor in stopping unauthorized wire 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, notify us immediately, report the incident to the local police and inform the FBI's Internet Crime Complaint Center at http://www.ic3.gov.

STOP. **THINK. DON'T BE FOOLED.**

If you believe you are a victim of fraud, notify RCB Bank immediately so we can help protect your account.

RCBbank.bank/Security
Fraud Dept. 877.361.0814

RCB BANK
MEMBER FDIC

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.

STOP. **THINK. DON'T BE FOOLED.**

If you believe you are a victim of fraud, notify RCB Bank immediately so we can help protect your account.

RCBbank.bank/Security
Fraud Dept. 877.361.0814

*Standard carrier fees for data and text messaging may apply.