Online Security Best Practices

RCB
BANK
That's my bank!

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

Our online services use multiple protections for your security, including unique user IDs and passwords, multi-factor authentication, secure tokens and Secure Socket Layer (SSL) encryption protocol. Despite all of these efforts, we also need your help to ensure your accounts are secure. Here are ways you can help protect against fraud.

The Basics

- **RCB Bank never asks for your online banking credentials, such as your password or security question answers.**
- Be cautious when clicking on links. To safeguard against false links, take time to open the browser and manually type in the URL.
- If you receive any requests when using online banking to verify your account information, social security number, online banking credentials or other personal information, DO NOT respond and contact RCB Bank immediately. The only thing we will verify in online banking is your email address.

Account Monitoring

- **Monitor your bank account often and report unauthorized or suspicious activity to RCB Bank immediately.**
- If a user replies to a fraudulent email or identifies an unauthorized transaction posting to the account, notify us immediately, report it to the local police and inform the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Keep your business information current. This is important if RCB Bank should contact you to confirm any suspicious transaction.
- Use a multi-factor authentication system for all sensitive data or wire transfers.

Anti-Virus, Firewall and Anti-Spyware Protection

- **Install anti-spyware, malware and a firewall. Ensure these are updated and active to protect your network or computer from unauthorized access.**
- Set up website, application and pop-up blocking. Your firewall and anti-spyware/ malware as well as your end-point protection software can each be set up to block websites or applications that may represent a greater risk for malware or fraud.
- Set up programs to automatically update to help ensure protection against the newest and latest threats.

Computer Access

- **Do not use public Wi-Fi or computers at libraries, hotels or other public places for online banking.**
- Never use your online banking password on any other website. Keep it unique and secure. Longer passwords are better.
- Ensure computers are not left unattended and are password protected.
- Do not share user IDs or passwords. Each user should have their own user ID and password that should be secured and not visible or accessible to others.

Get in touch. 855.226.5722 | RCBbank.bank

Member FDIC

Common Scams

Watch out for red flags of malicious activity.

RCB BANK
That's my bank!
MEMBER FDIC

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. • 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**
Uses a fake e-mail, instant message or social media message that appears to come from a legitimate source such as a bank, government agency or online services such as Paypal, Facebook, etc.	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**
A cell phone version of "phishing," scammers use fake company emails to send text messages that appear to be from legitimate or well-known companies.	Anybody with text messaging capability	• 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**
Telephone fraud that uses a technique called ID spoofing, which makes it look like calls are coming from a legitimate or known phone number.	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.***
Invoice Fraud	**Victims**	**Indicators**
When fake invoices are sent to a business in an attempt to extract money from companies through their accounts payable process.	Any size business	• Employees will split payments so they don't have to get manager approval. • Invoices submitted in sequential order. • Unusually high prices for goods and services. ***If in doubt, call the company directly using a known number to verify.***

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