Fraud Prevention Tips - May 2018

Every day, scam artists target people in an attempt to steal money or confidential banking information. We want to help you avoid becoming a victim. Below is a summary of frequent scams and some tips on how to protect yourself.

Phishing Scams

"Phishing" is when someone tries to trick you into giving them confidential banking information, so they can steal your money and identity. Phishing may be done using email, phone calls or voicemail, or text messages. In each case the goal is to lure you into revealing confidential information such as bank account numbers, credit card information, your Social Security Number or your Personal Identification Number ("PIN").

Email Phishing

In email phishing, fraudsters create a fake email that looks like it came from a trustworthy company or person. Emails may be sent to actual account holders whose addresses were obtained illegally, or they may be sent to random email addresses. The email may request you provide them certain information or click on a link. Clicking on the link in these emails may take you to a fraudulent website designed to look like the real website. Once there, you may be asked for confidential information (such as your account number(s) or Social Security Number). The cyber thieves may use the information you enter to steal from you. If an email is suspicious, contact the trustworthy company or person directly.

It's critical to know that Reliable Credit will never ask you to provide sensitive confidential information (e.g., your account number, Social Security number, name, address, password, bank account number, debit card number, etc.) in emails or text messages.

Telephone Phishing

Telephone phishers rely on deception to trick you into providing confidential banking information. The phishers may also warn or threaten that something bad will happen to you (e.g., an arrest) or your account (e.g., it will be frozen or terminated) if you don't follow their instructions. Telephone phishers can spoof caller ID to make it look like a call is actually originating from a trustworthy company or person. They may ask you to call back a number other than the one that shows up on Caller ID. Be suspicious if the caller asks you for information that the trustworthy company or person should already know. If you are suspicious, hang up and contact the trustworthy company or person directly.

So how can you tell whether a caller is really from Reliable Credit? It's simple. *Reliable Credit will never call you to ask for your account number or other confidential information.* The only time we might ask for personal information (such as the last four digits of your Social Security Number) is when you contact us. Reliable Credit will never require that you pay by phone. Furthermore, Reliable Credit does not accept payments via credit card. If you receive a suspicious call or voicemail claiming to be from Reliable Credit, hang up and call us at (888) 462-3003.

Text Message Phishing

Text message phishers send text messages to your phone, instructing you to call a certain number or go to a specified website immediately. As with telephone phishing, text phishers may warn or threaten that something bad will happen to you (e.g., an arrest) or your account (e.g., it will be frozen or terminated) if you don't follow their instructions. Never respond to these texts. Do not call the numbers they provide or click on the links they send to you via text message or email.

Reliable Credit will only send you text messages if you elected to receive Reliable Credit Mobile Alerts or requested them through Reliable's eServices portal. Reliable does not send marketing-related text messages.

How can you protect yourself?

- *Do not fall for scare tactics.* Fraudsters try to make you believe something bad will happen if you don't respond and provide your account number or other confidential information.

- *Do not fall for phone payment demands.*

- *Do not fall for demands that require a specific form of payment.*

- *Protect your confidential information*. As a rule of thumb, never include any information in an email or text that you wouldn't write on a postcard.

- *Trust your instincts.* If an email, text or phone call is suspicious, contact the trustworthy company or person directly so you are certain that you are not being scammed.