Popular Scams, and How to Protect Yourself

Examples of how a fraudster may attempt to take over your account through online payment fraud:

Fraudster Strategy	Your Response
Call customers pretending to be a bank representative looking to verify or modify the customer's credentials.	Never hand over your full online credentials over the phone, especially if you received the call. Your bank will not attempt to collect a user ID or password when calling.
Scammers send a text or email message informing the customer that they need to update their credentials with a link to a website.	Do not click on links within text messages or emails. If you need to make a change go to Regions.com or your bank's website and make the appropriate changes.
Fraudsters may setup a fake website linked to a web address that looks like the legitimate website (i.e. bank.com vs banks.com or bank.net.)	Be cautious when you search for your bank via a search engine. Review the results and ensure that the result you select is legitimate. Once you are confident, bookmark the page and access your online tools via that bookmark.
Calls the customer, sends an email, or sends a text message asking the customer to install a remote access application to a phone or computer in an effort to assist the customer in fixing an account issue, setup a new service, or paying a bill	Do not install applications which allow someone to access your phone or computer. Once the fraudster gains access to your device, they could initiate fraudulent transactions, modify credentials, and access private files on your device.