Popular Scams and How to Protect Yourself

Examples of how a fraudster may attempt to obtain your online banking credentials:

Fraudster Strategy	Your Response
Calls pretending to be a bank representative looking to verify or modify your online banking credentials.	Never hand over your online banking credentials over the phone, especially if you received the call. Your bank will not attempt to collect both a user ID or password.
Sends a text or email message informing you that you need to update your credentials using a link to the website provided in the email or text.	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.
Sets up a fake website linked to a web address that looks like the legitimate website (i.e. bank.com vs bank**s**.com or bank.**net**.)	Be cautious when you search for your bank via a search engine. Review the results and ensure that the result your select is legitimate. Once you are confident, bookmark the page and access your online tools via that bookmark.
Calls, sends an email or sends a text message asking you to install a remote access application to a phone or computer in an effort to assist you 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.