

Online Safety

“Phishing” is one of the most common scams used by internet criminals. When criminals “fish”, they typically create a replica of an existing Web site and send it to you hoping to deceive you into disclosing your Social Security number, credit card, check card, and checking account numbers, passwords, or other sensitive information. They lure you to “take action” such as logging on to online banking, deactivating your card(s) to temporarily guard against fraud, or activating your card(s). When you click on any link in their e-mail, it takes you to a log-in page that looks exactly like the real one but it’s a trick and will re-direct the information to the fraudster instead.



- Kingsport Press Credit Union will never send you an e-mail asking for your account numbers, usernames, passwords, or Social Security number.
- Never click on any links provided in an e-mail. Type in the site address directly yourself or use a link you have previously marked as a favorite instead.
- Do not be intimidated by an e-mail or caller who suggest dire consequences if you do not immediately provide or verify information. If you don't know the source, personally call your financial institution yourself and talk to someone you know.
- Never respond to or click on e-mail requests for personal information.
- Most fraudulent e-mail contains spelling or grammatical errors so if you notice these obvious mistakes, do not respond to the e-mail.
- Be suspicious of any e-mail that's not personalized with your name. It's usually mass produced messages sent to many people in an attempt to obtain personal information for fraudulent purposes.
- Regularly check Credit Union and credit card statements to make sure all transactions are legitimate.
- Use antivirus software and a firewall, and keep them up to date. Download updated security patches.