Protect Yourself Against Fraud

Fraud is on the rise and wreaking havoc on the lives of many Americans. There's no foolproof way to eliminate it, and unfortunately, everyone is at risk. However, learning how to protect yourself against fraud can go a long way in lowering your own personal exposure.

As we continue to rely more heavily on technology, our phones are never far from reach. It's no surprise that "smishing" scams have become more prevalent. Smishing involves fraudulent text messages that appear to be from your financial institution, trying to trick you into revealing account numbers or other personal identifying information.

Some smishing scams may ask you to click a link to access your accounts. The fraudster will pretend to already know your sensitive information, and will ask you to "verify" it. This includes Social Security numbers, account numbers and passwords, and any other personal, confidential information. The sense of urgency and the immediate need for specific financial information should both be red flags. The message may also be spoofed to display a website or phone number from the organization the scammer claims to represent. **We will never contact you via text message, phone call, or email requesting personal identification or account information**.

Smishing is just one example of how fraudsters are taking advantage of consumers. You may visit our Fraud & Scam Awareness page to learn more about the tactics commonly employed by these criminals. In the meantime, here are a few tips to help protect yourself against fraud:

Remain vigilant. Even under the most watchful eye, identity theft and fraud can still happen. Be cautious with your personal and account information, and report anything that doesn't feel right - Early detection is essential.

Monitor your accounts. Take a few moments each day to monitor your accounts with our Digital Branch. This enables you to keep a close eye on balances and account activity, and it helps you detect unauthorized transactions quickly. Contact us immediately if you suspect that you've fallen victim to fraud or unauthorized transactions.

Utilize multi-factor authentication. When available, enable multi-factor authentication for all of your online accounts. This includes credit unions, banks, and other financial service providers, email platforms, retailers, and more. Multi-factor authentication sends a verification code via email or text message upon account login. You must enter this code along with your username and password as an extra step in verifying your login credentials. We use Google Authenticator for this, and you may enable it for your credit union accounts through Digital Branch.

Setup mobile alerts. Mobile Alerts are an additional resource to help you stay on top of your credit union account activities, and are customizable to your needs. For example, you may create a Mobile Alert to notify you of account withdrawals, to help you detect unauthorized transactions. Mobile Alert settings are found in the Self Service tab of Digital Branch.

Shred sensitive documents. Keep financial records such as ATM receipts, deposit slips, and checks that you remotely deposit until you reconcile them with your monthly account statement, and then

shred them. Similarly, save your monthly checking and savings account statements securely until you file your taxes, and then shred them. And better yet, let us store them securely for you by enrolling in eStatements. You may access them via Digital Branch anytime, anywhere.

Again, you can't always prevent fraud from happening, but you can take steps to protect your personal and account information by limiting potential exposure. If you suspect you've become a victim, contact us as soon as possible. The sooner we're made aware, the better the chances your hard-earned deposits may be recovered.