Members are the First Line of Defense in Reducing Fraud

The Federal Trade Commission has reported that scam artists continue to social engineer information from unsuspecting individuals. The use of telephone, email, postal mail and the internet are all vehicles that fraudsters use to steal personal information and request you send money.

Below are items that you might consider adding to your web site to help your members reduce the risk of loss.

Be cautious of any company you select to engage in business
When you are contacted by a company or private party through the internet or telephone wanting to do business or sell something, conduct your own independent research. Verify the identity of that company and read over reviews or other information you can find. Make a sound decision on any purchases or dealings with a company who received negative reviews.

Be cautious when asked to wire money
Be extremely cautious if you are asked to wire money to any person or entity you do not know because it's nearly impossible to reverse the transaction or trace the money. Again, do research and make sure of the identity of the person or company you are doing business.

Review your account statements frequently
Fraudsters may have stolen your identity without your knowledge so check your accounts frequently. Dishonest merchants may also take advantage by billing you for "membership fees" each month or other goods or services without your authorization. Contact your credit union or card processor immediately if you see charges you don't recognize or didn't authorize.

Consider giving only to established charities in the event of a disaster
Don't give to an unrecognized charity following a disaster as they could be collecting money for their own purpose or to finance illegal activity. For additional donating tips, check out ftc.gov/charityfraud.

Investments are never a sure thing
Always conduct your own research if someone contacts you with low-risk, high-return investment opportunities. When you are requested to "act now" to reap the benefits from "these guaranteed big profits," be extremely cautious and report them at https://www.ftccomplaintassistant.gov/#&panel1-1.

Be cautious when buying products on line

It's best to do business with online sites you know and trust. If you buy items through an online auction, consider using a payment option that provides protection, such as a credit card. Do not send money or wire funds to someone you don't know.

Don't agree to deposit a check and wire money back.
Members are responsible for checks deposited into their account and if a check turns out to be bogus, the Member is responsible for paying it back. Anyone who overpays with a check and requests that a portion of the funds be returned is almost certainly engaging in fraud.

Don't respond to emails or messages to provide personal or financial information.
Be extremely cautious when opening a link to an email or responding to any question from a telephone call where personal information is requested. Fraudsters are attempting to trick you into revealing sensitive information. If you received such a message and you are concerned about your account status, call your credit union or the number on the reverse side of your credit or debit card.

Report Scams
If you think you may have been scammed:

· Notify your credit union to report the incident.

· File a complaint with the Federal Trade Commission at http://www.econsumer.gov/

· Visit FTC's site on identity theft - http://www.consumer.ftc.gov/features/feature-0014-identity-theft

· File a complaint with the FBI at the Internet Crime Complaint Center at http://www.ic3.gov/default.aspx to report the incident.

· If you get what looks like lottery material from a foreign country through the postal mail, notify your local postmaster.