FORGE

The Arkansas Cyber Defense Center

Credit Card/Bank Account Scam

A credit card/bank account scam involves using fraudulent means to get the information necessary to access your financial accounts and ultimately take your money.

Why be aware of this scam?

These scams can be difficult to detect. Scammers can be very good at pretending to be a representative of your financial institution. They will often manipulate your emotions in order to get you to quickly give them the information they need. Once they have your account information, they can withdraw your money, or even open new accounts in your name.

Common tactics:

- Impersonating representatives of your financial institution
- Threatening physical harm to you or people close to you
- Creating a sense of urgency to manipulate you to give your information quickly

Red flags:

- They ask for your account information or personally identifiable information (These companies already have your information)
- Broken English in phone calls, or poorly written emails or texts
- Pressure to act immediately

Immediate action:

- If your financial institution is calling you and asking for information, hang up, look up their phone number online, and call them back to help ensure they are who they say they are.
- If you have already provided your financial information, contact your financial institution to see about stopping transactions or canceling accounts.
- Keep all documentation related to the scam in case you need to file a police report.
- If you provided personal information, like your Social Security number, you may be at risk for identity theft. Contact your bank or credit card company to make them aware. Then, contact the three major credit reporting agencies – Experian, TransUnion and Equifax – and place a fraud alert on your credit reports. This will make it harder for the scammer to open new accounts in your name.

POWERED BY SBA U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599