USALLIANCE FINANCIAL®

Federally Insured by NCUA

4 Types Of Spoofing

Email Spoofing

What it is: An email message sent by a scammer that appears to be from a known and trusted source.

Danger: Will contain links to malicious sites or attachments that will install malware.

Protect yourself: Never click on links or download email attachments from an unverified source.

Caller ID spoofing

What it is: An attacker makes a phone call that appears to be from a known caller.

Danger: The scammer convinces the victim they represent their financial institution and tricks them into sharing account details.

Protect yourself: If you're allegedly contacted by your financial institution, and asked to share account details, hang up and contact your bank or credit union directly.

Website spoofing

What it is: A scammer creates a bogus site that looks just like a reputable website the victim often visits.

Danger: Victims visit the site and unknowingly share their login credentials and/or personal information with scammers.

Protect yourself: Pay attention to URLs of every site you visit. Look out for look-alike URLs of known sites, as well as websites full of typos and spelling errors.

Text-message spoofing

What it is: A victim receives a text message on their personal device that appears to have been sent by a trusted source.

Danger: The text will ask the victim to share personal information.

Protect yourself: Never share personal information with an unverified source.