THINK BEFORE YOU CLICK

Small actions. Big protection.



TYPES OF SCAMS TO WATCH FOR

PHISHING EMAILS

An email that appears to come from your financial institution, a retailer, or another trusted company asking you to click a link or verify your account.

Protect Yourself
Don't click links. Visit the company's website directly or call using a trusted phone number.

SMISHING (TEXTING SCAM)

A text claiming there's a problem with a package delivery, bank account, toll payment, or prize you've won.

Protect Yourself
Never click links in unexpected text messages. Verify through the company's official website or app.

VISHING (PHONE SCAM)

Someone calls pretending to be from your credit union, a government agency, tech support, or law enforcement pressuring you to act immediately.

Protect Yourself
Hang up and call the organization back using a trusted phone number.

ONLINE SHOPPING SCAM

Fake online stores advertising unbelievable prices on popular products. Often there are limited payment options and prices far below market value.

Protect Yourself
Shop with trusted retailers and look for secure websites (https://) before entering payment

PRIZE & GIVEAWAY SCAM

"You've won!" messages asking you to pay fees or provide personal information to claim a prize. Often there is a request for payment or financial information.

Protect Yourself
Remember: legitimate prizes don't require you to pay to receive them.

IMPERSONATION SCAM

Scammers use artificial intelligence to create convincing emails, voice recordings, videos, or messages that appear to come from someone you know.

Protect Yourself
Verify requests by contacting the person directly using a trusted phone number, not the one provided.

Brought to you by
Firstmark Credit Union