Scams: Protecting Identity & Preventing Fraud

Jamie Smathers, VP of Fraud Prevention & BSA, MSUFCU

November 10, 2025

msufcu
MSU FEDERAL CREDIT UNION

To provide superior service while assisting members and employees to achieve financial security, their goals, and ultimately, their dreams.

Today's Presenter

Profile

Jamie is the VP of Fraud Prevention & BSA for Michigan State University Federal Credit Union, overseeing the Financial Crimes Unit for the organization. She has been with the Credit Union for ten years. She also serves as the International Association of Financial Crimes Investigators (IAFCI) Michigan Chapter Secretary.

Agenda

- Terms & Definitions
- Fraud & Scam Landscape
- Why This is Important
- Current Fraud and Scam Trends
- Safeguarding Against Fraud and Scams
- Resources

Defining Fraud & Scams

Fraud	• wrongful or criminal deception intended to result in financial or personal gain
Scams	• the use of deception or manipulation intended to achieve financial gain

Social Engineering

Manipulation of people into performing acts or divulging sensitive information

- Rampant through digital channels
- Happens in physical form too
- Familiar to the victim – known entity, person or action (‘click to learn more’)
- Heightens emotions – fear, empathy, excitement
- Creates a sense of urgency to act
- Capitalizes on human behavior

Phishing

Phishing - emails

Vishing – voice calls

Smishing – text messages (SMS)

Quishing – QR codes

Purporting to be a legitimate person or entity to get the consumer to act

Spoofing

Disguising an email, phone number, or website to appear to be a known, trusted entity

Today’s Fraud & Scams

Are prevalent	Move fast	Are tied to everyday behaviors
Impact many, many, many people	Can cause significant financial loss	Most people impacted do not share
Can be challenging to discern if real or fake	Create uncertainty about who to trust and what to do	Can lead to further complications with identity security

Consumer Impact

- Cards compromised
- Accounts compromised
- Loss of reliable device(s) and access
- PII compromised
- Loss of funds
- Emotional, mental, social, physical
- Time spent recovering

Everyone is susceptible to being a victim of fraud.

Basics of Scams

- Can happen in many ways – in person, mail, email, phone calls, text messages, internet, apps, ads
- Technology often plays a significant part
- Old tactics still used while new ones constantly developed and used
- It can develop and happen quickly but also can be gradual
- Create a sense of urgency to respond or act
- Want quick and easy payment – giftcards, cash, wires, P2P

Common Scams

Investment	Relational	“Government”	“Grandparent”
Charity	Sweepstakes, contests, lotteries	Employment	Loan

Fraud Trends

SIM SWAPPING ON MOBILE DEVICES

MAIL THEFT

BURGLARIES, ROBBERIES, MUGGINGS

EXTORTION

Safeguarding

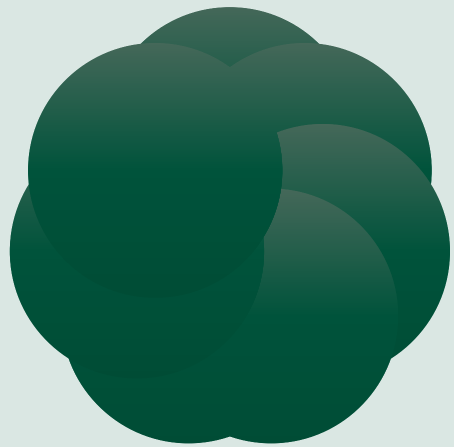
Protect what is important, for yourself and others: identity, finances, physical safety, mental well-being

Don’t engage or participate

- best practice is to not answer or respond at all
- you don’t know what information is exposed already

Be aware of what is exposed and what you share (think social media)

- set your apps to private
- limit what is shared and who can view it



Spread the word – be an ally to others in this fight against fraud

If they get you to do the transaction – it isn’t a fraudulent transaction

Families have a common word or phrase

Pay attention, pause, and verify

Resources

FTC – consumer.ftc.gov/scams

Credit bureaus

- Experian – 888.397.3742
- Equifax – 888.378.4329
- TransUnion – 888.909.8872

Internet Crime Complaint Center – IC3.gov

Local Law Enforcement Agency