Member Fraud Prevention Seminar

Mocse Credit Union
September 24 and 25, 2024

Mocse

Fraud in 2024

- **This could be a day-long seminar**— will focus on top trends.
- Multi-faceted and more sophisticated than ever
- Human intelligence/social engineering bolstered by technology
  Ex. “Brute force attack” for password cracking
- Data for sale on Dark Web
- Credit/debit card fraud still multi-billion-dollar industry
- Account takeover by various means
- Scams

Mocse

How did they get my card number to begin with?

- Brute force attacks
  - *Seeing scripting program use after just one valid card obtained
- Social engineering/phishing (email, text, call, imposter website)
- Hacking/malware
- ATM skimmers
- Stolen mail
- Merchant card compromises, sales on Dark Web
  - *Happens constantly
  - *Insecure Wi-Fi, inadequate cyber controls for online transactions.
  - *Myth is “My credit union was hacked.”

Mocse

What you can do: The basics, first.

- Wiggle ATM components | Use Tap to pay/digital pay
- Monitor online banking activity, especially on weekends.
- Use a locking mailbox.
- Avoid entering card info or passwords when on public Wi-Fi.
- ***Report unusual activity immediately!***
- Watch for “test transactions.”
- Use strong passwords and don’t repeat them for other websites
- Don’t click links/attachments you aren’t expecting.
- Destroy sensitive information
- Monitor your credit report. (Savvy Money, Free annually on annualcreditreport.com.)

Mocse Credit Union

Top fraud trend today: *SPOOFING*

- Bad actors spoof phone number of financial institution (FI) and either call or text victim.
- Ask about “fraudulent transactions.”
- Will instruct victim not to log into online banking for a few days while they “send out a new card and correct the accounts.”
- Accounts are drained while victim is unaware.

Mocse

What you can do: Part Two

- **NEVER give out MFA code.** Your credit union or bank will never ask you for this!!!
- NEVER give out online banking username or passcode.
- Verify your FI is the one contacting you by calling the correct number directly and asking.
- Beware of urgent messages or pushiness on the phone. HANG UP.
- Always report unusual activity immediately.
- Take a breath before responding to an alarming text or call.

Mocse

Romance or “sweetheart” scams

- Commonly starts in social media platforms
- Online love interest
- Considerable time invested to build trust– months to years
- Obituaries leveraged
- Overseas in the military, working on project in foreign country, etc.
- Some type of legal issue with visiting or moving to US, financial or medical emergency, inheritance problems, issues with embassy, need to provide funds to “transaction coordinator”
- Wires, electronic transfers, checks, home equity loans, Bitcoin

Mocse

What you can do: Part Three

- Never give out sensitive information to online love interest, friend, or business partner.
- If someone online asks for help with a financial transaction or emergency, say NO.
- Never pay money to get money.
- Never buy gift cards at the direction of someone else or as form of payment.
- Shut off computer and go to a reputable repair location if you suspect you have a virus or other malware.
- Watch for ID theft red flags: missing mail, withdrawals you can’t explain, medical bills for services you didn’t receive, debt collection calls, IRS notification of more than one tax return in your name.

Mocse
Credit Union

Mocse
Credit Union

BEWARE OF SCAMMERS

Fraudsters have become more sophisticated than ever and are targeting everyone! Here are helpful tips to protect yourself and avoid becoming the target of financial fraud:

- Do not click unsolicited links or attachments via email or texts.
- NEVER give out online banking passcode or verification code (even if they say they are calling from Mocse. We will NEVER ask you for this). Periodically change your username and password.
- VERIFY your financial institution is the one contacting you by calling the number directly.
- Avoid entering card information or passwords when you are on a public Wi-Fi.
- **Report unusual activity immediately!**
- Monitor online banking activity, especially on weekends.
- Beware of urgent messages or pushiness on the phone. **HANG UP.**
- Never pay money to get money or buy gift cards at the direction of someone else or as a form of payment.
- Shut off computer/phone and go to a reputable repair location if you suspect you have a virus or other malware.

Mocse is here to help you. Contact us!