

SCAM WATCH:

Protect yourself and your \$money\$

Presented by Merrimack Valley Credit Union

April 2021



The Most Common Types of Scams

- **Dating or Romance (online relationships)**
- **Tech Support (Microsoft) (request to Remote into the Computer)**
- **One ring call (to get you to call back)**
- **Income/Work at Home**
- **Family-Friend Emergency**
- **Overpayment of rebate online**
- **Overpayment with counterfeit check**
- **IRS or Government Imposter**
- **Lottery and Sweepstakes**

Four Signs That It's a Scam

SCAMMERS:

1. **PRETEND** to be from an organization you know.
2. Say there is a **PROBLEM** or **PRIZE**.
3. **PRESSURE** you to act immediately.
4. Tell you to **PAY** in a specific way.

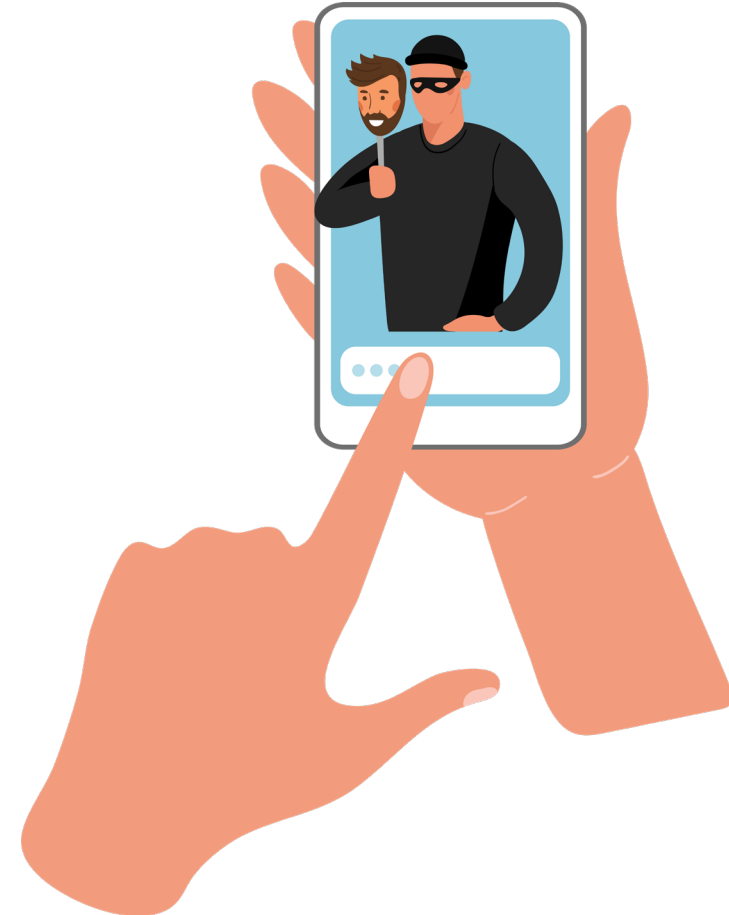


Four Signs That It's a Scam

1. Scammers **PRETEND** to be from an organization you know.

- Social Security Administration
- IRS
- Medicare
- Utility Company
- Tech Company
- Charities

Scammers have been presenting fraudulent Government ID Badges to prove they are legitimate.



Four Signs That It's a Scam

2. Scammers say there's a Problem or a Prize

- You're in trouble with the Government.
- You owe money.
- Someone in your family had an emergency.
- There is a virus on your computer.
- There is a problem with one of your accounts.
- You won the lottery or sweepstakes (but have to pay to get the prize).
- You are owed a refund.



Four Signs That It's a Scam

3. Scammers **PRESSURE** you to act immediately.

- They want you to act before you have time to think.
- They tell you to stay on the phone so you don't have time to verify their story.
- They stay on the phone while you purchase gift cards or go to complete a wire transfer.
- They might threaten to:
 - Arrest you
 - Sue you
 - Take away your driver's or business license
 - Deport you
 - Corrupt your computer

Four Signs That It's a Scam

4. Scammers tell you to **PAY** in a specific way:

- Wire money (Western Union/ MoneyGram)
- Purchase gift cards (Re-load Cards) and give registration numbers.
- Some send you a (FAKE) check, tell you to deposit it, and then mail or ship cash to them. (Through USPS, UPS, FedEx)
- Send Cryptocurrency (i.e. Bitcoin)




Scams That Targeted MVCU Members

Xfinity phone scam

- The scammer pretends to be calling from Xfinity.
- They tell you that you are owed a refund.
- To get the refund, you need to log into online banking.
- The scammer remotes into your computer and transfers money from one of your accounts to another.
- They make the transfer appear to be their rebate when it is actually your own funds.
- The scammer tells you they have processed the refund but gave you too much.
- They ask you to send the excess back to them in gift cards, by wire transfer, or shipping cash.

Red Flags

- They remoted into the member's computer.
 - Asked member to log into online banking.
 - They asked for payment via wire transfer, gift card, or shipping cash.
- 
- Companies you deal with would NEVER need to remote into your computer and have you log into your on line banking in order to provide you with a rebate or refund.

Scams That Targeted MVCU Members

Amazon Refund Scam.

- Member received an e-mail from “Amazon” that his computer had an issue and needed to be updated.
- Member responded and allowed the technician to remote into his computer.
- Member was instructed to log into online banking.
- Member was unaware the scammer conducted multiple transferred funds from the member’s saving to checking and labled the transfers “FedEx refund” and “Amazon refund”.
- Member shipped cash and conducted a foreign wire transfer.
- Member lost over \$30K.

Red flags:

- They remoted into member’s computer
- Asked member to log into online banking
- Asked for payment via wire transfer and shipping cash



Scams That Targeted MVCU Members

Fraudulent Check, Account take over and COVID Unemployment

- One member was approached to process three types of scams:
 - Tried to credit COVID Unemployment payments tied to her account.
 - Tried to post an ACH Credit from another institution in someone else's name to the account.
 - Member presented fraudulent checks.
 - Member stated she was helping her friend she met online.
- Once you are approached, the criminals will keep trying to get you to fall for multiple scams.
- You must remain diligent.

Scams That Targeted MVCU Members

Helping Military Friend

- Member met a friend online who is in the military.
- Friend needed help to process check.
- Asked for member's Remote Deposit username and password.
- Friend remotely deposited the fraudulent check.
- Asked member to send funds back.

Red Flags:

- **Met the person online.**
- **Asked for remote deposit login.**
- **Asked to send funds back.**



Scams That Targeted MVCU Members

Online Loan Scam

- Member was trying to apply for a loan online from “The Lending Company”.
- Company stated she needed to deposit a \$595 check and send back before they could provide the funds for a \$6,000 loan.
- Company required: account number, routing number, online banking username and password.
- Company remotely deposited the \$595 check.
- CU recognized check was fraudulent, no loss to the member.

Red flag

- Company required member to deposit a check from them and send the funds back to get the loan.
- Company requested and received online banking user name and password
- Company remotely deposited the check for member.



Scams That Targeted MVCU Members

Spoofer MVCU Phone Number

- Member receives a phone call. Caller ID states call is from MVCU.
- During the call, the perpetrator states there is an issue with their account.
- Requests the member's debit card number in order to assist.
- Requests the member social security number or other personal information to confirm their identity.

Red Flag:

- **Caller stated there was a problem with their account**
- **Caller requested the member's debit card number.**
- **Caller requests personal identifying information.**



The Credit Union will NEVER ask you for your account or personal information. The Credit Union already has it.

Scams That Targeted MVCU Members

Fraudulent MVCU e-mail:

RED FLAGS:



The "from" e-mail does not match the "from" company name.

- do-not-reply@achs.com should state @mvcu.com

The link did not go to the MVCU website

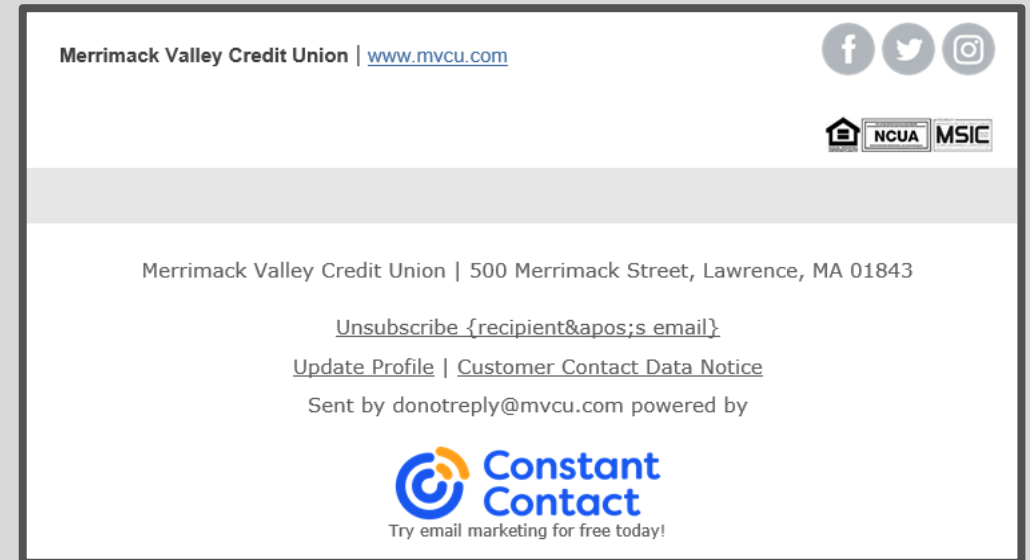
How to Verify an Official MVCU E-mail

If MVCU sends you an official e-mail, do not click on a link unless you verify the e-mail is legitimate.

Verify the e-mail address, it should state, “@mvcu.com” If it does not it is fraud.

- Hover over the link before you click on it.
- To hover, simply hold your mouse point over the link- the website address (URL) will appear. It should state “mvcu.com”

All official MVCU e-mails will include the following at the bottom of the e-mail:



How to Protect Yourself From Scams

- Block unwanted calls and text messages.
- If you did not expect the call, text or e-mail:
 - NEVER give your personal or banking information
 - NEVER CLICK on any links unless you verify it is legitimate.
 - Hover over it to look at the address. If the root of the link is from a business that you know (like mvcu.com) then it is probably safe
 - Always check the destination of links before clicking on them
 - Not sure? Contact the business to find out if it's a legitimate email and links are safe to click!



How to Protect Yourself From Scams

- Resist the pressure to act immediately.
- Never pay someone who insists you pay with a gift card, wire transfer.
- Never deposit a check and send money back to someone.
- Be extremely cautious about any one you meet online.
- Stop and talk to someone you trust.
 - A friend, family member, neighbor or your credit union.



Helpful Hints

- **Don't trust the number on your caller ID.**
 - Scammers can make it look like they are calling from legitimate numbers.
- **The IRS and Social Security will NEVER:**
 - Call, TEXT or send an e-mail to say you owe money.
 - Scammers manipulate caller ID to look like the call is coming from the government.
 - Request payment by gift cards, money transfers or cryptocurrency.
 - Ask you for personal information.
- **NEVER let anyone remote into your computer.**
- **NEVER give anyone your username or passwords.**

Helpful Hints

A Financial Institution will NEVER ask you:

- For your debit or credit card number
- For the security code given for verifying your identity
- To verify your online/mobile banking user ID or password
- To remote into your computer

Legitimate Contests will never require you to:

- Send money
- Provide bank account information
- Provide credit card information
- Wire money, send gift cards or send cryptocurrency



What To Do If You Were Scammed

If You Paid the Scammer:

- Did a scammer make an unauthorized transfer from your bank account?
 - Contact your bank to report the unauthorized transaction or withdrawal.
- Did you pay with a gift card?
 - Contact the company you purchased the gift card from.
- Did you send a Wire Transfer through a company like Western Union or MoneyGram?
 - Contact the Wire transfer Company
- Did you send a wire through your bank?
 - Contact your bank.
- Did you send money through a Money transfer app or a Person to Person (P2P) transfer?
 - Contact the company behind the money transfer app.
 - Once you send funds through these applications it is difficult to recall the transaction

What To Do If You Were Scammed

If You Gave a Scammer your Personal Information:

- Did you give your Social Security Number?
 - Go to [IdentityTheft.gov](https://www.identitytheft.gov) for the steps you should take.
- Did you give your username and password?
 - Create a NEW, STRONG PASSWORD.
 - If you use the same password anywhere else change it there, too.
- Did you give your bank information?
 - Contact your financial institution.

What To Do If You Were Scammed

If the Scammer Has Access to Your Computer or Phone:

- Does the scammer have remote access to your computer?
 - Update your computer's security software
 - Run a scan, delete anything it identifies as a problem
 - Take other steps to protect your personal information
- Did a scammer take control of your cell phone number? Did you lose your phone?
 - Contact your service provider to take back control of your phone number
 - Once you do, change your account password
 - Check your financial accounts for unauthorized charges
 - Go to [IdentityTheft.gov](https://www.identitytheft.gov) to see what steps you should take.

What To Do If You Were Scammed

- **Do not get embarrassed.**
 - Scammers are great at what they do and everyone can become a victim.
- If you are a victim and have lost money, contact:
 - Your local police
 - MA or NH State Attorney General
- Report the Scam to the Federal Trade Commission at:
 - [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov)



Don't Become a Mule

If a scammer asks you to process transactions through your account.....

Don't allow it!

These funds are stolen and you are committing a crime if you help the criminal process the funds.

- are coming from:
 - Accounts that have been taken over through online banking
 - Fraudulent unemployment claims from multiple states
 - Fraudulent checks drawn off legitimate company accounts
 - Fraudulent tax refunds

Eventually you will be responsible for returning the stolen funds!

Recent Scam Involving the USPS

- Text/E-mails are being sent that appear to be sent from the United States Postal Service.
- They tried to deliver a package to you.
- You need to click on the link the link in order to pay a \$3 redelivery fee.
- You are asked provide bank account and personal information.
- **DO NOT CLICK** on any links! These are not being sent by the USPS.
- **The USPS will never charge you to redeliver a package!**

THANK YOU FOR ATTENDING

If you have any questions or concerns, do not hesitate to contact the Credit Union. We are always willing to assist you!



Online at mvcu.com



By phone at 800-356-0067