Rockland FEDERAL CREDIT UNION
Serving generations - our legacy, our future.

July 2023

Member NEWSLETTER

At Rockland Federal Credit Union, we strive to provide our members with quality, affordable financial services in a responsible, efficient, professional and convenient manner.

Volume 30
Issue 3

10 Common Scams to Avoid

With new twists on familiar scams, fraudsters stay current and continue to try to separate us from our cash! The AARP has released these ten common scams:

1. Cryptocurrency-romance scam

Crooks combine crypto scams with old-fashioned romance scams, posing as internet love interests so they can cajole their targets into downloading an app and investing in fake crypto accounts. "They claim that they're even putting some of their own money into your fund," explains former Federal Trade Commission official Steve Baker, who publishes the Baker Fraud Report. While the app displays data that seems to show your wealth growing, criminals are just taking your money.

How to stay safe: Carefully scrutinize any investment opportunity, even if you think you're a sophisticated investor. "People think it's not going to happen to them, but it is happening to many, which is why you have to keep your guard up," Nofziger says.

2. One-time password (OTP) bot scam

Credit reporting company Experian warns that scammers utilize bots — automated programs — to deceive people into sharing the two-factor authentication codes sent to them via text or email from financial institutions (or from companies such as Amazon). The bot will make a robocall or send a text that appears to come from a bank, asking you to authorize a charge, then it asks you to enter the authentication code you've just been sent if the transaction isn't yours. It's actually the bot that's trying to log into your bank account, and it wants the code that the bank sent to you as a precaution, so it can get in.

How to stay safe: Never share authentication codes, or provide other information, in response to an unsolicited phone call or text.

3. Check washing scam

Though other payment modes are replacing them, checks are still used often enough for scammers to exploit. One trick is "check washing," in which crooks steal checks from mailboxes and bathe them in household chemicals to erase the original name and dollar amount, leaving blank spaces they can fill in. It's possible to convert a $25 check to one for thousands of dollars.

How to stay safe: The U.S. Postal Inspection Service recommends depositing your outgoing mail in blue collection boxes before the day's last pickup, so it doesn't sit for as long. At home, avoid leaving mail in your own mailbox overnight, and have your mail held by the post office or picked up by a friend or neighbor if you're going to be away.

4. 'Oops, wrong number!' texts

Seemingly misdirected messages are increasingly the start of a scammer's ploy. A text message addressed to someone else pops up on your phone. It seems urgent — a rescheduled business meeting, or maybe a romantic get-together. You text back, "Sorry, wrong number!" The scammer keeps up the friendly texts, and may eventually invite you to join an adult website to see revealing pictures so you hand over credit card info and money, or try to convince you to make a cryptocurrency investment (and take your money).

How to stay safe: Don't respond to texts from numbers you don't recognize. Don't click on links in them or respond with "STOP" if the messages say you can do this to avoid future messages. Block the phone numbers they come from.

5. Fake barcodes on gift cards

Law enforcement agencies warn that nimble-fingered crooks affix fake barcode stickers over the real ones on the back of

Continued on Page 2

gift cards in stores. When you purchase the card, the cashier scans the fake barcode at checkout — directing your money into the scammer's gift card account.

How to stay safe: With some gift cards, you can make sure the number of the barcode matches the number on the packaging. Or feel or gently scratch the barcode on a gift card before buying. Don't purchase if the barcode is on a sticker, or if the package is ripped, wrinkled, bent or looks tampered with.

6. Crypto refund swindles

Beware if you've lost money in a cryptocurrency scam: Criminals set up fake "get your crypto cash back" websites, including one that looks like it's from the U.S. Department of State. After luring targets, they contact those who respond by phone, email or social media and ask for personal ID information, including account numbers and passwords, plus an advance fee for their services payable by gift card, cryptocurrency or wire transfer. You get nothing, warns the FTC.

How to stay safe: Crypto investments aren't insured by the government the way bank accounts are. For the most part, funds lost to crypto scammers are gone. Don't trust anyone who contacts you saying they can get your money back, says Frank McKenna, chief fraud specialist for the fraud detection company Point Predictive.

7. Bank impersonator racket

Let's say you've set up your bank or credit card online accounts so you can access them only with a live code sent from the institution. And let's say a criminal has your bank or credit card username and password login and wants to steal from you. What would he or she do? In this increasingly common fraud, they call you, claiming to be from your bank and warning about a problem with your account. The caller tells you they're emailing or texting you a "one-time passcode" for logging in and asks you to read it back to them for verification. In reality, the scammer's login attempt triggered your bank to send you the passcode. Handing it over gives criminals full access to your account.

How to stay safe: Never give your one-time passcode to anyone who calls you. Hang up, find your institution's phone number on a bank statement or on your credit card, and call. Ask if there really is a problem and report the con to the bank's fraud department, McKenna recommends.

Remember that RFCU will never ask you to confirm your PIN, username, password or one-time verification code you receive by text. If you receive a call like this, do not give them any information.

8. LinkedIn relationship fakes

A criminal might send you a message on LinkedIn, claiming to be just starting out in the same industry you're in, seeking advice from a more experienced colleague. It's flattering and fun to be a mentor, so you agree. You get to know each other, and eventually they ask to move your conversation onto a personal device, then lure you into a scam.

How to stay safe: A request to continue your chat on a more private channel is a warning. So is talking up crypto. LinkedIn may flag requests to go off-platform as it tries to remove fake accounts. But you should end the conversation and block the scammer.

9. Out-of-stock item scam

Scammers often place fake ads on social media sites for products at too-good-to-be-true prices, take your order and payment info, then tell you the item's not available right now. Your refund is on the way, they promise, but it never arrives. And you can't reach anyone at the company about it.

How to stay safe: Research businesses online before you buy, and only shop on secure websites with a lock symbol in the browser bar and an internet address that begins with "https." And pay by credit card, the FTC recommends. That way, you can withhold payment pending an investigation.

10. Student loan forgiveness scam

The Biden administration's plan to forgive student loans faces an uncertain future after being tied up in the courts, but that hasn't stopped scammers from trying to take advantage of people who may not have heard it's on hold. They've built phony application sites aimed at stealing applicants' Social Security numbers and bank information, and sometimes they contact targets by phone, pressuring them into applying and charging a fee for their help. The scam still has legs, "because there's so much debt that people are carrying and they're looking for a way to get rid of it," explains Michael Bruemmer, vice president of the data breach group and consumer protection at Experian.

How to stay safe: Go to the Department of Education's student aid website to keep track of the proposed forgiveness program's status.

Keep in Touch!

Moving? Changed your Phone number or email address? Let us know so that we can keep in touch with you!

Traveling? Please let us know your travel plans 48 hours in advance of departure to avoid disruption in service. With increasing fraud, we continually monitor fraud patterns and transactions to protect your accounts. For your convenience you can let us know by visiting rfcu.com and selecting "Travel Notification" from the Members menu in the homepage footer, or in the "More" section of the RFCU Mobile App.

10 Tips for ATM Safety

1. Keep your PIN private. Don't share this number with anyone and don't write it down anywhere or keep it stored in your phone.
2. Check the ATM for a card skimmer. Scammers are experts at hiding their tracks and often do so by attaching a card skimmer to the payment terminal of an ATM.
3. Bring a buddy. A lone target is always more vulnerable, especially late at night.
4. Be aware of your surroundings.
5. Use your body as a shield. Never let an ATM you are using be in easy view of a criminal.
6. Have your debit card ready to be used. Make sure you can remove your card in just a few seconds when you reach the ATM.
7. Put away all cash as soon as you complete your transaction. Count cash once you're safely in your car.
8. Lock all doors and roll up passenger windows when using a drive-thru ATM.
9. If you suspect foul play, leave immediately.
10. Be sure to take your receipt.

If you think you've been the victim of ATM fraud, report it immediately.

Free Credit Score and Report

You already know that tracking your credit score is important.
Our Credit Monitoring Tool makes it easy!

You have instant access to your credit score, credit report, personalized money-saving offers, and financial education tips on how to improve your score or maintain an already great score.

This tool is built right into our easy-to-use online and mobile platforms, so you don't need a new login.

Get started today:

STEP 1

Log into the RFCU Mobile App or Online Banking

STEP 2

Mobile:
Go to the "More" menu and select "Credit Score"

Online Banking:
Select "Credit Score" from the menu bar at the top

STEP 3

Button: See my Credit Score Now

CHECK US OUT

Did you know that Rockland Federal Credit Union is on Facebook? Like and follow our page to keep up with what we're doing in your community, hear about exciting products and get great tips on the financial matters that matter to you! Visit Facebook.com/RockFedCU today.

2023 Board of Directors Elections

All Credit Union members are invited to attend the 101st Annual Meeting of the members of Rockland Federal Credit Union. The meeting will be held on Wednesday, November 15, 2023 at 241 Union Street, Rockland, MA. The nominating committee has re-nominated current Board Members William J. Shaman, Jr., Chairman and Stephen T. Gorman, Secretary for the existing three-year vacancies, and is nominating Sonia Giandomenico for the open Board position.

William J. Shamon, Jr., Chairman

Bill is CFO of W.J. Connell, Co. of Norwood, MA a Select Employee Group served by RFCU. He received a Bachelor of Science in Accounting from Bentley College in 1975. Bill has been a member of the Board of Directors since 1995.

Stephen T. Gorman, Secretary

Steve is the President and sole owner of Gorman Financial Management, a Registered Investment Advisory firm that he founded in 1992. He has been a member of the Board of Directors since 1995 and has often served as Chairman of the Board. Steve received a Bachelor of Science in Business Administration from Georgetown University in 1981 and earned the Certified Financial Planner designation in 1986. Steve resides in Norwell Massachusetts with his wife Andrea.

Sonia S. Giandomenico, Director

After a career in Commercial Banking, Sonia joined the Supervisory Committee of RFCU in 1999, and has Chaired that Committee since 2002. She received a Bachelor of Arts degree from Yale University in 1978 and a Master of Business Administration degree from Boston University in 1983. She now serves as an adviser to a Walpole-based international satellite communications company. Sonia resides in Walpole with her husband.

Nominations by petition

Any Rockland Federal Credit Union member wishing to add his or her name to the ballot may do so by petition. Candidate petitions will be available beginning July 1, 2023. Petition candidates must obtain 500 valid Rockland Federal Credit Union member signatures by September 8, 2023. To appear on the ballot, petitions must be delivered to the Credit Union's main office by 4:00 p.m. on September 8, 2023. For further information on filing a nomination by petition, please contact Heidi Chandler at Rockland Federal Credit Union, 241 Union St., Rockland, MA 02370.

Voting Procedure at the Annual Meeting

Nominations will be taken from the floor only under the following conditions:

1. When sufficient nominations have not been made by nomination committee, or
2. by petition to provide one nominee for each position to be filled, or
3. When circumstances prevent the candidacy of the one nominee for a position to be filled.

The election will be conducted by ballot and will be by plurality vote, except when there is only one nominee for each position to be filled, in which case the chair may take a voice vote or declare each nominee elected by general consent or acclamation.

Rockland FEDERAL CREDIT UNION
Serving generations - our legacy, our future.

Forbes 2022
BEST-IN-STATE CREDIT UNIONS
POWERED BY STATISTA

Rockland Federal Credit Union is honored to have been named on the Forbes list of America's Best-In-State Credit Unions 2022!

ATTENTION:

Annual Privacy Notice

Rockland Federal Credit Union's Privacy Notice is available for viewing at:
https://www.rfcu.com/privacy/

To request a paper copy of the privacy policy notice, please call (800) 562-7328. A copy will be mailed to you within 10 business days.

Holiday Hours

Tuesday, July 4th – Independence Day
All offices are closed.

Monday, September 4th – Labor Day
All offices are closed.

Monday, October 9th – Columbus Day
Plymouth Branch, open 10am – 2pm
All other offices are closed.

Member Service Center

(781) 878-0232 (800) 562-7328
Website: rfcu.com

NCUA
Federally Insured by NCUA
EQUAL HOUSING LENDER
MEMBER MASSACHUSETTS CREDIT UNION
MSIC SHARE INSURANCE CORPORATION

MN 07/23