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

Member NEWSLETTER

January 2024

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 31
Issue 1

Keep in Touch with Us!

Do we have your most current email address? Beginning in April 2024, the RFCU Newsletter will be delivered by email rather than included in your quarterly statement. We also periodically share important information regarding events, scam alerts, products, and new opportunities via email.

Where to find our newsletter:

- Look for an email this April and quarterly going forward
- Our website at **rfcu.com** in the "About" section
- Within the eStatements portal

How to update your contact information and email address with us:

- Call us at (800) 562-7328
- Log in to RFCU Online Banking or the RFCU Mobile App and select "My Settings"

Common Scams to Avoid

Scammers are constantly finding new ways to separate you from your money. Protect yourself by learning the signs.

The CFPB warns that the following scams are still going strong in the new year.

Money Transfer or Mobile Payment Services Fraud

Con artists use money transfers to steal people's money. If someone you don't know asks you to send money to them, it should be a red flag. Scammers also use mobile payment services to trick people into sending money or merchandise without holding up their end of the deal. For example, a scammer may sell you concert or sports tickets but then never actually give them to you. Or a scammer might purchase an item from you, appear to send a payment, and then cancel it before it reaches your bank account.

Using mobile payment services with family, friends, and only others you know and trust is the safest way to protect your money. But you should also be cautious when people you do know ask you to send them money. Before you send money, verify that they are the ones requesting it.

What to do: Never send money to someone you don't know. If you think you made a money transfer to a scammer, contact your bank or the company you used to send the money immediately and alert them that there may have been a mistake.

Lottery or prize scams

In a lottery or prize scam, the scammers may call or email to tell you that you've won a prize through a lottery or sweepstakes and then ask you to pay an upfront payment for fees and taxes. In some cases, they may claim to be from a federal government agency.

Continued on Page 2

What to do:

- Avoid providing any personal or financial information, including credit cards or Social Security numbers, to anyone you don't know.
- Never make an upfront payment for a promised prize, especially if they demand immediate payment.
- Don't cash a check from someone that asks you to return a portion of the check to them. When the check bounces, you'll have lost the money that you sent.
- Ask yourself why someone is trying so hard to give you a "great deal." If it sounds too good to be true, it probably is.

Imposter scams

Imposter scammers try to convince you to send money by pretending to be someone you know or trust like a sheriff; local, state, or federal government employee; your credit union; or charity organization.

What to do: Remember, caller ID can be faked. You can always call the organization or government agency and ask if the person works for them before giving any money.

If you receive an unsolicited text or phone call from someone claiming to be from RFCU, and you're not sure if it's us, hang up and call us back at (800) 562-7328.

Common Methods Used by Scammers:

Never send money to someone you don't know. Scammers use a variety of ways to collect money from you, including:

- Wire transfers
- Person-to-person payment services and mobile payment apps
- Gift cards

Reporting Fraud and Scams:

If you're a victim of a scam, report it to your financial institution, then the authorities by:

- Submitting a complaint online with the Federal Trade Commission (https://reportfraud.ftc.gov/#/)
- Contacting your local police or sheriff's office
- Reporting it to your state attorney general (https://www.usa.gov/state-attorney-general)

Don't Forget to Make Your IRA Contributions!

2023 IRA Contribution Tax Deadline: APRIL 17, 2024

Traditional and ROTH IRA Contribution Limits		
For Traditional or ROTH IRA	**2023**	**2024**
Under Age 50	$6,500	$7,000
Age 50 or Older	$7,500	$8,000

RFCU in the Community

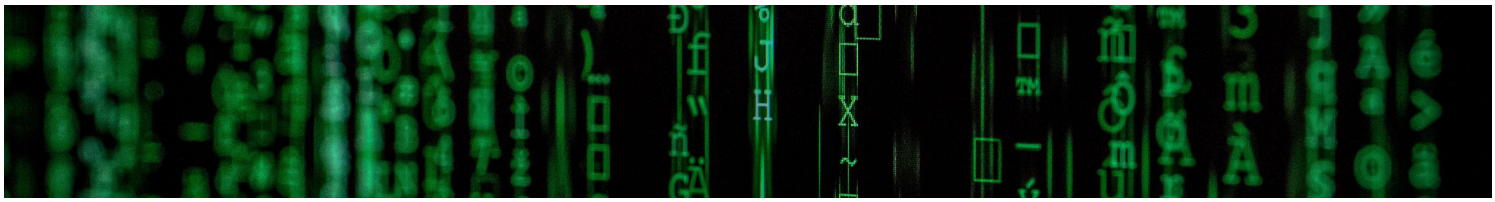
Rockland Federal Credit Union continued our tradition of investing in our communities with charitable contributions in 2023, including:

- **Credit Union Kids at Heart**
- **Marine Toys for Tots**
- **Friends of Attleboro Animal Shelter**

CREDIT UNIONS KIDS@♥

FRIENDS of ATTLEBORO ANIMAL SHELTER

TOYS FOR TOTS



Create and Keep Strong Passwords

Your passwords are like the keys to your life. And when it seems like there's another big security breach every week, you want to be absolutely sure your passwords are strong and safe. After all, with just a few keystrokes, a scammer can have full access to your personal information, financial accounts, social media pages and so much more.

But creating those perfect passwords — and remembering them — can be difficult.

Below, we've outlined 6 steps for creating and keeping super-strong passwords that will keep scammers guessing.

STEP 1: Choose a password manager

With so much of our lives accessible online, it's more important than ever to keep passwords secure. The best way to do this is to use a password manager. These services will generate strong passwords for all of your financial accounts, favorite websites and social media platforms and then keep them safely encrypted. You will only need to create and memorize one master password, which you will use when logging into all of your accounts.

There are lots of password managers on the market, but the ones that come most highly recommended are 1password, LastPass and KeePass. 1Password and LastPass are both cloud-based services, and can be vulnerable to remote attacks. However, both services heavily encrypt your data and don't store your one master password in the cloud. As long as that password is strong, you'll be safe even if these services get hacked.

STEP 2: Create an unbreakable master password

Once you've chosen your password manager, create a strong master password. This code can open up every password of yours to potential scammers, so be extra careful about choosing one that is super-secure and virtually unbreakable.

Follow the rules below and you'll have a strong password.

- **Make it long.** Many sites require a password that is a minimum of 8 characters long, but a 12-character password is even stronger.
- **Be creative.** Avoid using names, places and recognizable words because these are easily cracked.
- **Mix it up.** The best way to keep your password unbreakable is to mix up your capitalization and the kinds of characters you use, switching back and forth from letters to numbers to symbols.
- **Don't** use any of variation of these commonly used — and commonly hacked — passwords:
    - 123456123456789
    - Passwordadmin
    - 12345678qwerty
    - 1234567111111
    - 123123123456789000000
    - Abc1231234
    - Iloveyouaaaaaa

Bonus tip: Worried about creating and remembering a long, unbreakable password? Turn a sentence into a password by using mnemonics, misspelled words and symbols that only you will understand. Here are a few to get you started:

- **WOO!TAwonTWS** = Woohoo! The Astros won the World Series!
- **D:'(OspldMlk.JdreenqOJ** = Don't cry over spilled milk. Just drink orange juice

STEP 3: Update all your passwords

Next, you're going to sync all the websites and accounts you use with your password manager. Follow the guidelines on your password manager for this step, as they differ with each service.

When you're through, you'll only be able to log into these sites by using your master password.

Some sites you use might employ outdated systems that won't work with a password manager. For these sites, you will need to use different passwords. You can slightly amend your master password for these sites or create new ones using the guidelines above. Never double passwords; use a different one for every site you use.

STEP 4: Use two-factor authentication

Add another layer of protection by choosing two-factor authentication whenever you have that option.

STEP 5: Be careful with security questions

Ironically, security questions are extremely insecure. Anyone can Google your dog's name or your mother's hometown. And, if all a scammer has to do to retrieve your password with the "I forgot my password" tab is answer a security question, the strongest passwords in the world won't do you any good.

Protect yourself by treating security questions like passwords. Never answer them truthfully. Instead, make up mnemonics or nonsensical answers that are hard to crack but easy for you to remember.

STEP 6: Don't let your browser or phone "remember" your passwords

Don't be lazy; keep your passwords in your head and not on your devices. Otherwise, you'll be in deep trouble if your computer or phone is swiped.

Avoid being an easy target — Keep your passwords strong and safe!

Don't Let the Weather Get In the Way of Your Deposit.

Sign up for Mobile Check Deposit with RFCU and make deposits securely from the comfort of home. It's as easy as taking a picture of the check with your smartphone in our RFCU app!

DeposZip software integrates completely with RFCU's highly secure online banking system. The password and authentication technology used for Online Banking also protects your mobile deposits.

Eligibility:

- You must be 18 years of age.
- You must have a RFCU checking or savings account open for a minimum of 30 days; business accounts must be open a minimum of 6 months.
- You must have a valid email address
- You must be enrolled in Online Banking

Getting started is easy!

Mobile: Log into your RFCU Mobile App and select "Check Deposit" at the bottom of the screen. Read and accept the user agreement and allow 2 business days for your registration to be reviewed and approved. You will receive an email notification regarding the status of your registration request.

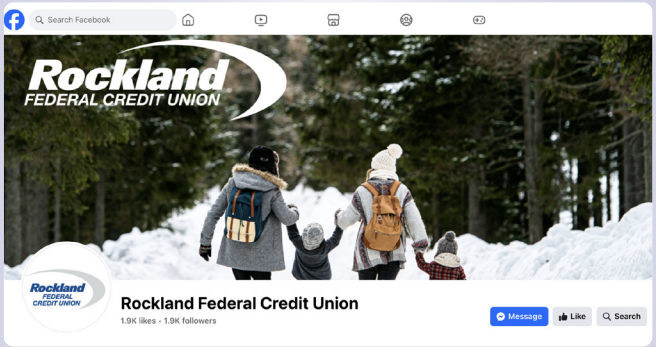
Online: Log into RFCU Online Banking and select the "Remote Deposit" option from the Additional Services Menu. Read and accept the user agreement and allow 2 business days for your registration to be reviewed and approved. You will receive an email notification regarding the status of your registration request.

Enroll today and be ready for whatever this New England winter has in store!

CHECK US OUT

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.



Holiday Hours

Monday, January 1st – New Year's Day
All offices are closed.

Monday, January 15th
Birthday of Martin Luther King, Jr.
Plymouth Branch, open 10am – 2pm
All other offices are closed.

Monday, February 19th – Presidents' Day
Plymouth Branch, open 10 am – 2pm
All other offices are closed.

Sunday, March 31st – Easter Sunday
All 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 01/24