THE LATEST TRENDS IN FRAUD

The world of fraud is ever-changing. No matter what we throw at them, fraudsters will adapt and change their tactics. With consumers continuing to take a digital-first approach to everything from shopping to dating to investing, fraudsters are finding new and innovative ways to commit fraud. Make sure you stay diligent in your online security. Here are the trends expected for 2022:

Romance Scams - These scams will continue to be prevalent due to their high success rate. Fraudsters will begin fake relationships in order to swindle money by asking victims for help with fabricated travel costs, medical expenses and more. If it feels too good to be true … it probably is!

Ransomware - Fraudsters will not only ask for hefty ransoms to give back control to computers and mobile devices, but they will also steal and leverage any data they can hack from the sources.

Cryptocurrency Scams - Fake accounts will be created by fraudsters to store and funnel stolen funds.

Digital Elder Abuse - Older consumers and other vulnerable digital newbies will be hit with social engineering and account takeover fraud. Please stay vigilant.

Friendly Scammers - Much like the romance scams, these fraudsters will create fake friendships with people, especially through social media, and then use the same tactics to swindle victims out of money.

Coronavirus Scams - Scammers continue to use the pandemic for a variety of scams. The exact messaging or approach is often updated to align with the latest concern. Watch out for fake at home test kits online that collect personal information.

Government Program Scams - Government relief programs are commonly used by scammers. The government response to the pandemic has been no exception to fraud. Stimulus checks, student loan forgiveness and tax changes can all be woven into scammers' messaging.

Phone and E-mail Scams - Robocalls, texts, impersonators, apps, QR codes, and money transfer sites are all susceptible to fraudsters. Be wary of anyone calling, texting, or e-mailing and asking for personal information.

IF IT DOESN'T FEEL RIGHT … CALL YOUR CREDIT UNION

experian™

Become a credit union volunteer! If you would like to serve as a volunteer, stop by or call the credit union office today!

Office Hours

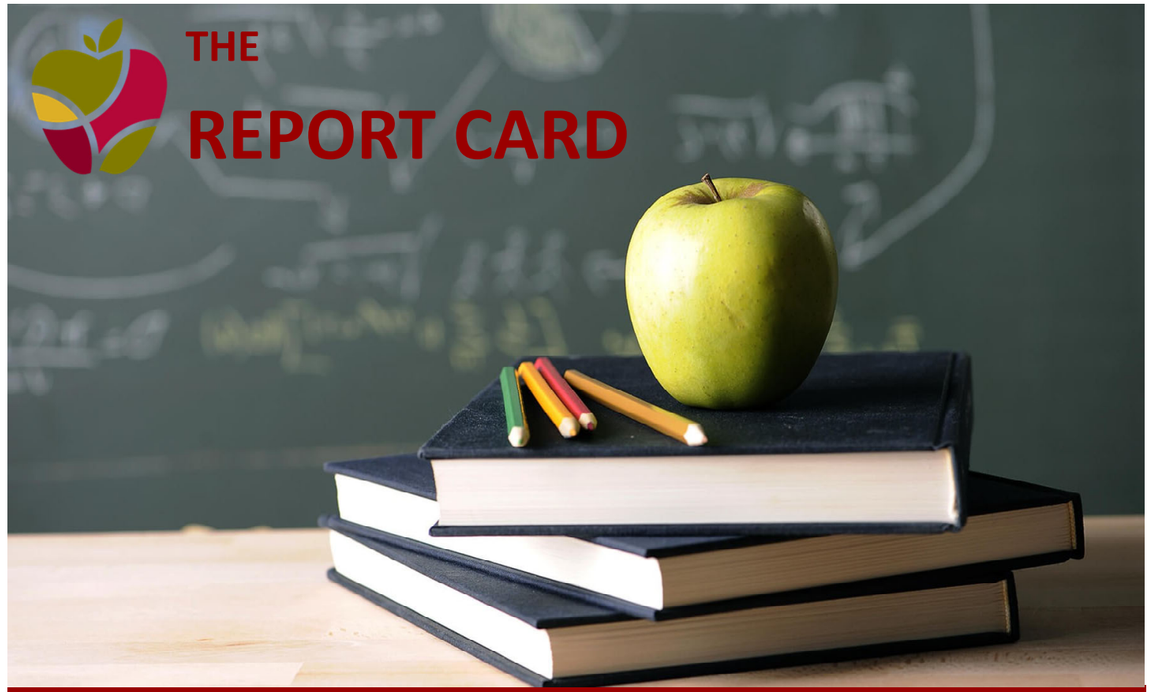
Monday -Friday
9:00 am—5:00 pm

Contact Us

phone: 724-864-7469 fax: 724-864-9230
email: info@norwinteachersfcu.org
wwwnorwinteachersfcu.org

Closed and Holiday Hours

May 31st—CLOSED
June 20th—CLOSED
July 4th—CLOSED



Norwin Teachers Federal Credit Union Spring2022

Notes from Amy

I hope that this note finds you enjoying the spring weather and being able to be outside. Fall is my favorite season; however, spring is a close second due to its promise of warmer weather. Enjoy!

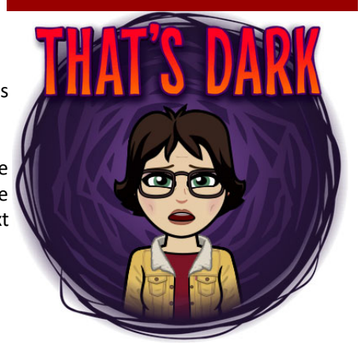
Please BEWARE of scammers. I cannot warn you enough to be wary of those that try to take funds that you work/worked hard to earn. They are VERY, VERY good at disguising their intentions. Please call the credit union whenever you get that feeling that something doesn't sound or feel right. We are happy to talk with you about your concerns. But, you must do this BEFORE you agree to send money. Once you send the money, it is GONE. YOU are in control of who gets the money, not the credit union. Please talk to us if you have any doubts what you are doing is legitimate. Phone calls, emails, texts and social media are just a few of the ways that scammers use to entice you to fund their schemes. Let's work together and keep your money safe. We care about you!

Also, your credit union will be strengthening security on our mobile app and home banking. In the future when you use these online services, you will be prompted into using another layer of identification. Multi-factor authentication will give your accounts another layer of security. It may seem to be an inconvenience; however, it is the best way to protect your information from hackers.

On a lighter note, your credit union sponsored Reality Fairs at Hillcrest Intermediate School and at the High School in April. Students learn about the realities of finances in the real world at this fair. Stay tuned for follow up information about those fairs in our next newsletter.

See you at the credit union,
Amy

Inside This Issue



LOAN RATES

Home Equity up to 60 month	4.25%	4.25%	APR*
Home Equity 61-120 months	4.50%	4.50%	APR*
New Car up to 72 months	**3.24%**	**3.24%**	**APR***
Used Car 4 yrs. old or older up to 48 months	4.24%	4.24%	APR*
Used Car 3 yrs. old or newer up to 60 months	4.24%	4.24%	APR*
"Steal the Deal" Car loan (call for	**2.24%**	**2.24%**	**APR***
details) "More Fantastic than Plastic"	8.50%	8.50%	APR*
Consolidation Share Secured (3% above	3.10%	3.10%	APR*
share rate) Signature up to 60 months	12.00%	12.00%	APR*

*APR - Annual Percentage Rate

SHARE RATES

Share Accounts	0.10%	0.10%	APY*
Christmas Club	0.10%	0.10%	APY*
IRA	0.50%	0.50%	APY*
Share Certificate 6 months	**0.25%**	**0.25%**	**APY***
Share Certificate 12 months	**0.35%**	**0.35%**	**APY***
Share Certificate 24 months	**0.50%**	**0.50%**	**APY***

*APY - Annual Percentage Yield

IRA WITHHOLDING NOTICE

Payments from your IRA are subject to federal income tax withholding, unless you elect no withholding. You may change your withholding election at any time prior to your receipt of a payment. Your withholding election does not effect the amount of income tax you pay. You may incur penalties under the estimated tax rules if your withholding and estimated tax payments are insufficient. You may be required to pay estimated taxes even if you elect withholding.

WHAT IS MULTI-FACTOR AUTHENTICATION?

In today's world, the only constant we can count on is the constant change in data security. As attackers think up new ways to fraud us, we must come up with new ways to protect ourselves. Multi-factor authentication is one of those ways. While this is not a new concept, it has not been widely utilized.

Multi-factor authentication (MFA) adds a layer of validation and security. It ensures an additional method of authentication when a user attempts to verify credentials. It can be something you know (like a password), something you have (such as a mobile phone), or even something you are (think fingerprint and face ID). Organizations have been implementing MFA at varying levels for years.

Keep an eye out for information regarding MFA and your credit union online banking and mobile app.

KEEP YOURSELF PROTECTED FROM FRAUD

Keeping yourself protected is more important than ever. Every 2 seconds at least one person's identity is stolen. Identity theft can occur in an array of forms and new tactics are always being developed. Why not take the proper action to protect yourself by using some of these helpful tips!

1) **Use strong passwords and pins**

Use both letters, numbers and special characters when allowed. Do NOT store your passwords on your computer or mobile device. If you need to write down your password, store it in a secure and private location. You should change your password and pins regularly. Always use different passwords for each account.

2) **Maintain computer security**

Use personal firewalls and security software packages . Make sure your software is up to date regularly.

3) **Use your own computer**

The use of your own personal computer is generally safer when accessing your accounts. Avoid using public computers to access accounts with sensitive information. If you have to use public computers, be sure to delete the temporary internet files, cache, and history before AND after logging into accounts.

4) **Log out completely**

Always click logout to completely terminate your access to sites you have accessed (especially on public computers). Avoid multi-tasking on multiple web pages to avoid "session stealing."

5) **Be prudent when using wireless connections**

Unsecure Wi-Fi connections do not provide as much security as a wired internet connection, encrypted wireless network, or even a mobile carriers' cellular data connection. Many public "hot spots" reduce their security settings so it is easier for individuals to use. This increases the ability and likelihood someone could intercept your information.

6) **Check for secure websites**

When accessing accounts, check to ensure that the log in page indicated that it is a secure site. The address of the secure site should start with http**s** instead of http. A key or closed padlock should also show in the status bar.

7**) Be careful downloading**

Only download software from sites you know. Be wary of free software downloads because it can be accompanied by other software such as spyware.

CunaMutualGroup™ FINRA