FINANCE WITH THE FRIDAYS TREASURER

A Financial Literacy Newsletter

Issue 19, Oct. 2, 2026

NC Cash | NC ABLE

In this issue:

•Bottom Line with Brad
•Demystifying
•The Red Flag Files
•When a Scammer Steals Your Identity
•Digital Disguises
•Tips For Teens
•Golden Guidance
•Financial Literacy in Action
•Recommended Reading
•Test Your Knowledge

Finance Fridays
is a publication of the N.C. Department of State Treasurer. Treasurer Brad Briner is focused on preserving, protecting and sustaining the state's pension and health care plans. Briner was most recently the Co-Chief Investment Officer for Willett Advisors and has held positions at Morgan Creek Capital, the UNC Management Company, ArcLight Capital and Goldman Sachs.



Bottom Line With Brad

FRAUDS AND SCAMS

My late father walked into a Home Depot several years ago intending to buy $500 worth of gift cards. Fortunately, the cashier asked him why he needed so many gift cards?

I never learned exactly what story he had been told, but it was likely some version of an impersonation scam: someone claiming to represent a government agency, a business or perhaps a family member in trouble. The message would have been urgent, the consequences frightening and the solution strangely specific: buy gift cards immediately and provide the numbers on the back.

The cashier recognized the warning signs and persuaded my father to call one of my brothers before completing the purchase. That conversation exposed the fraud, and my father left the store with his $500 — and, I hope, learned an important lesson on modern days scams.



I remain grateful to that attentive cashier. She did more than provide good customer service that day. She protected my father.

My dad was intelligent, responsible and generous. Those qualities did not make him immune to fraud. In fact, scammers often exploit our best instincts: the desire to help someone we love, fulfill an obligation, protect our savings or quickly correct a mistake.

It's October - all of us are preparing for Halloween frights and scares. This month, we want to make sure none of them are coming from financial frauds and scams.

My dad's story is the first lesson about fraud: smart people get scammed.

The second is that scammers manufacture urgency. They do not want you to think. They certainly do not want you to call a family member, your bank or local police department. They want to keep you frightened, isolated and moving quickly.

I have received hundreds of messages over the years from people pretending to be the IRS and warning that agents are on their way to my house to arrest me. Their persistence is impressive. Their understanding of how the IRS collects

My dad's story is the first lesson about fraud: smart people get scammed.

The second is that scammers manufacture urgency.

taxes is less so.

Those messages are easy to laugh at when the language is clumsy, or the threat is obviously ridiculous. But fraud is becoming much more sophisticated. Artificial intelligence can produce convincing emails, realistic photographs and even voices that sound like someone you know. The awkward scam message filled with misspellings may soon become a very polished message that appears to come from your bank, your boss or your own child.

The details change, but most scams include at least one of these warning signs:

- Urgency: “You must act immediately.”
- Secrecy: “Do not tell anyone about this.”
- Fear: “Your account has been compromised,” or “A family member is in trouble.”
- An unusual payment method: Gift cards, cryptocurrency, wire transfers or cash.
- An unexpected windfall: You have won a prize, inherited money or found a guaranteed investment — after paying a fee, of course.

The Federal Trade Commission says imposter scams are now the most commonly reported type of fraud. Technology will make impersonation easier, which means we should place less trust in communications that arrive unexpectedly — even when they look or sound authentic.

Do not call the number provided by the person who contacted you. Do not click the link in the message. And do not assume caller ID proves anything.

The safest verification is either in person or outbound. Speak face-to-face with the person involved or end the incoming communication and initiate a new one yourself. Call your relative using the number already stored in your phone. Contact your bank using the number on the back of your card. Reach a government agency through the telephone number published on its official website.

Do not call the number provided by the person who contacted you. Do not click the link in the message. And do not assume caller ID proves anything.

Remember one particularly useful rule: gift cards are for gifts, not payments. No legitimate government agency, bank or police department will demand that you settle a debt or protect your money with gift cards. The IRS has many ways to collect money. Asking for the numbers from the back of a gift card is not one of them.



Families should talk about scams before an emergency occurs. Consider establishing a family code word that can be used to verify a genuine request for help. Encourage parents and grandparents to call someone they trust before transferring money — and promise that the conversation will begin with help, not embarrassment.

That last part matters. Shame is one of the scammer's greatest allies. If you believe you have been deceived, contact your financial institution immediately and report the fraud. The faster you act, the better the chance of limiting the damage. Every single one of us will be the victim of attempted fraud – the only shame is in not doing something about it once you realize it is fraud.

As artificial intelligence makes fraud harder to recognize, that simple human connection will become even more important. Ask questions when something feels wrong. Check on the people you love. Verify important requests in person or through a call that you initiate.

And when someone demands money immediately, remember that the most profitable financial decision you make that day may simply be to wait.

DEMYSTIFYING

NC Cash and Unclaimed Property





By MaryAnne Fitzpatrick
Deputy Treasurer of the
Unclaimed Property Division
N.C. Department of State Treasurer

We are going to spend a lot of time talking about sophisticated frauds and scams throughout this newsletter - but there is one thing that our team here at the Department of State Treasurer runs - that many people think is a scam - and isn't! Let's demystify unclaimed property in North Carolina.

A message saying the state has money for you can sound suspicious. That is a reasonable reaction, especially when scams often promise prizes or ask for personal information. But North Carolina's NC Cash program is real. It has a simple mission: return unclaimed property to its rightful owners.

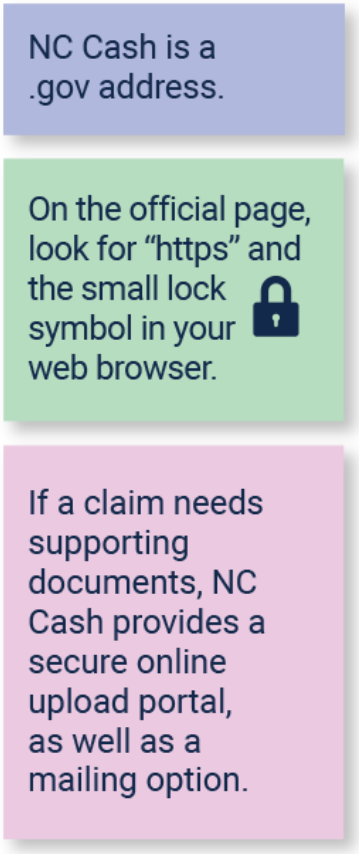
Unclaimed property is money or other financial assets that a business or organization could not deliver to you. It may include anything from an old bank account, an uncashed paycheck, a utility deposit, insurance proceeds or stock. After a period of time, the holder turns the property over to the state for safekeeping. The state keeps it until the owner- or a rightful heir- claims it.

Security Checkpoints:

Sometimes one of the easiest ways to spot a scam, is by the website you are directed to.

- NC Cash is a .gov address. The only way you can get an address that ends in .gov, is if you are a

government agency.
- On the official page, look for “https” and the small lock symbol in your web browser. Those signs show that you are connected to the official state website through a secure connection.
- If a claim needs supporting documents, NC Cash provides a secure online upload portal, as well as a mailing option. The portal uses a secure certificate to protect your information. All details will remain confidential, accessible only by Unclaimed Property Officials and for claims processing purposes only.



An Unexpected Call:

A claim may also require information or documents to confirm that you are the owner. For high-dollar claims, NC Cash staff may contact you as part of the process. That contact can feel unexpected, so it is fine to pause and verify it.

Here is a simple safety rule: if you are unsure who is calling, ask their name and then hang up. Then call NC Cash yourself using the number listed on NCCash.gov: (919) 814-4200 Option 3 and ask to be transferred to the person who called you. Do not rely on a phone number supplied by an unexpected caller or message. A real state representative will understand that you want to check first.

Finding money you had forgotten about can be a welcome surprise. A few careful checks—using the official website, protecting your personal information and calling back through a verified number — can help you explore NC Cash with confidence.

The security, claim document upload, privacy and phone details are reflected in the NC Cash FAQ and claims guidance. NCCASH Make sure to check for your cash today!

The Red Flag Files

How to Spot a Scam Before It's Too Late



By Laura Rogers
Director of Cybersecurity Practice in the Secure Computing Institute and Director of NC-PaCE at N.C. State University

What does a scam look like?

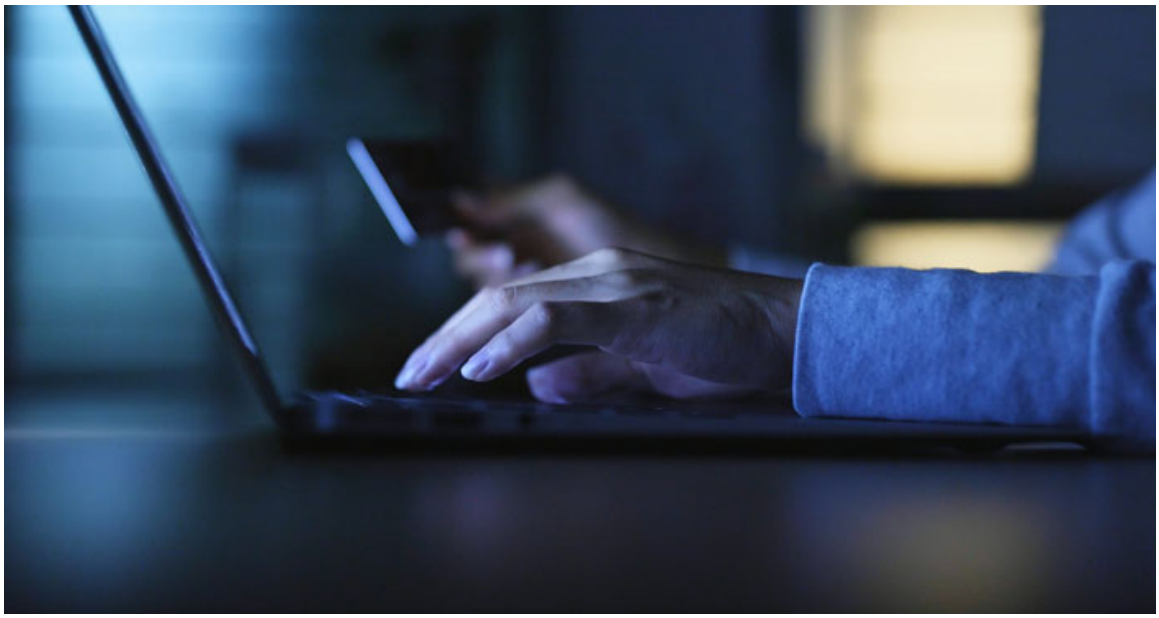
It might be a text saying you owe a toll, a call claiming there is a problem with your bank account or an email promising a prize. The methods vary and stories are different, but most scams follow the same pattern: someone gets your attention, makes you feel you must act immediately and asks for money or personal information. The goal is to get you to act before you think by evoking an emotional response.

Recognizing that pattern doesn't require complicated technology; you just need to change how you react.

What are the biggest red flags?

- **Unexpected contact.** A call, text, email or social media message from someone you don't know asking for personal information or money.
- **A deadline that leaves no time to think.** You are told to pay "right now" or lose access to an account, miss an opportunity or face a penalty.
- **Threats or fear.** The message claims you will be arrested, fined or locked out of an account unless you comply.
- **An offer that sounds too good to be true.** You have supposedly won a prize, qualified for a guaranteed return or found an unusually easy way to make money.
- **An unusual way to pay.** Someone insists on gift cards, cryptocurrency, a wire transfer or a payment app.
- **A request for sensitive information.** They ask for your password, a verification code, bank details or Social Security number.

Any one of these is a reason to stop and think before you act.



Why do scammers try to make everything feel urgent?

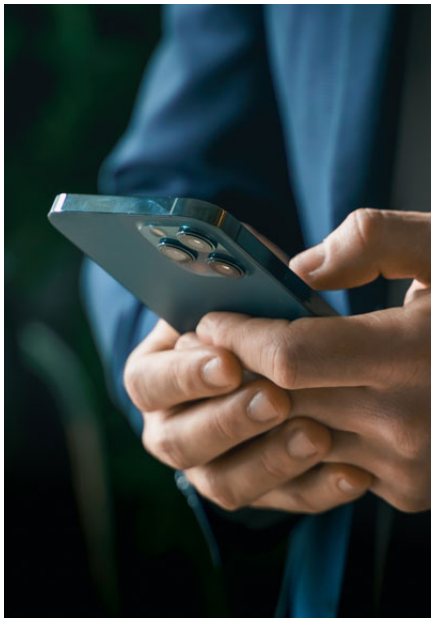
Urgency makes it harder to think clearly. If you believe your money is at risk or a loved one needs help, your first instinct is to act. Scammers use that instinct against you.

Example: You receive a text that says your bank account will be frozen in 30 minutes unless you click a link. You have an immediate emotional response, which is exactly what the scammer wants. Instead of clicking on the link in the text, contact your bank through its official app or a phone number you already trust. If there is a real issue, you can address it with the bank directly.

What if the message appears to come from my bank, a government agency or someone I know?

Verify it using links or phone numbers you know are safe. Scammers can pretend to be organizations and people you trust, so don't use the phone number or link in the message.

This applies even when the message seems personal. A request from a "friend" who suddenly needs money should be verified with a phone call. Taking a few minutes to confirm the story is reasonable, and someone who knows you will understand.

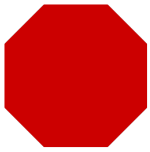


Can a scam happen without asking for money right away?

Yes. Some scammers try to develop a relationship with you over time before they begin asking for personal information or money. By not replying to a text or answering a phone call from someone you don't know, scammers won't have the opportunity to develop a relationship with you.

What does “Stop, Check, Verify” mean?

Keep this simple checklist handy:



STOP. Do not click, reply, pay or share information while someone is pressuring you. If you’re having an emotional reaction to a message or phone call, take a breath. Put your phone down or take your hands off the keyboard. Very few things in life are so urgent they must be taken care of right away.



CHECK. Look at what you are being asked to do. Is the contact unexpected? Is there a threat, a rushed deadline, an unbelievable promise or a demand for an unusual payment method?



VERIFY. Reach the person or organization through a phone number or website you found independently. Ask whether the request is real before taking any action.

What if I already responded or sent money?

Act quickly, and do not be embarrassed. Contact your bank, card issuer or payment service right away and explain what happened. If you shared a password, change it on the affected account and anywhere else you used the same password. Report the scam at **ReportFraud.ftc.gov**. In North Carolina, you can also contact the Attorney General’s Consumer Protection Division at **1-877-5-NO-SCAM**.

If you are the victim of an online crime, report it as soon as possible through the Internet Crime Complaint Center. The sooner you report the crime, the more likely you are to get your money back.

What is the one thing I should remember?

When a message evokes an emotional response, remember: **Stop**, **Check**, **Verify**. Those few minutes can keep you from making an expensive mistake.



When a Scammer Steals Your Identity Your Financial First-Aid Plan



By Hari Ravichandran
CEO of family online safety company, Aura

Identity theft rarely announces itself. The first clue may be a charge you don't recognize, a bank alert you weren't expecting or a notice that your information appeared in a data breach. By then, a scammer may already be using your identity — and your money could be at risk.

In 2025 alone, the FBI's Internet Crime Complaint Center logged nearly 32,000 identity-theft complaints and more than $185 million in reported losses. One recent case shows just how many people can be exposed at once. This September, investigators uncovered more than 153 million stolen driver's licenses from across the U.S. and Canada for sale on the dark web, many packaged as full digital scans and ready to be used.

A stolen license is just one way identity theft can begin. In the wrong hands, personal information — from a license or Social Security number to a bank login — can help a criminal open accounts, apply for credit or pose as you online. And while you can replace a card or change a password, you can't always take back the information that was stolen. That's why knowing how to respond quickly matters.

If you suspect your identity has been stolen, don't panic, but don't wait. Think of the next steps as financial first aid: stop the immediate damage, protect the accounts a criminal could target next and begin repairing your identity.

Here's where to start:



1. Contact your bank and credit card companies

Call your bank or credit card issuer right away using the number on the back of your card, not one provided in a text, email or unexpected phone call. Ask them to freeze or close

affected accounts and issue new cards if needed. Federal law limits your liability for certain fraudulent charges when they're reported promptly, so don't wait to make the call.

2. Freeze your credit with all three bureaus

A credit freeze can prevent someone from opening new credit accounts in your name until you lift it. You'll need to contact Experian, Equifax and TransUnion separately, since freezing your credit with one bureau doesn't automatically freeze it with the others. Credit freezes are free and don't affect your credit score.





3. Change your passwords, starting with your most important accounts

Start with your email and financial accounts, since access to those can give a criminal a path into other parts of your digital life. Create a unique password for each account and turn on two-factor authentication wherever it's available and, when possible, use an authenticator app rather than text-message codes.

4. Check your accounts and credit reports for anything unfamiliar

Review recent bank and credit card statements carefully for transactions you don't recognize. Check your credit reports for unfamiliar accounts or inquiries and report anything suspicious directly to the creditor. You can also report identity theft and create a recovery plan through IdentityTheft.gov.





5. Create an official record

If your identity has been stolen, filing an identity theft report with the Federal Trade Commission can help document what happened and support you as you dispute fraudulent accounts or charges. Depending on the circumstances, you may also want or need to file a police report.

6. Know what information you should never share

Scammers often piece together bits of personal information to build a fuller picture of your identity. Be especially cautious about sharing sensitive information with anyone who contacts you unexpectedly, even if they claim to represent your bank, the IRS or another government agency.



That includes:

- Your Social Security number
- Bank account or debit or credit card numbers
- Online banking or email passwords

- One-time verification codes sent to your phone
- Your driver's license or passport number
- Your date of birth alongside your full name and address

Be wary of anyone pressuring you to provide sensitive information immediately. If you're unsure whether a request is legitimate, end the conversation and contact the organization directly using a phone number or website you know is authentic, rather than contact information provided by the person who reached out.

Recovering from identity theft can take time, but moving quickly can help limit the damage and make the recovery process easier. For more guidance on what to do after your information is exposed in a breach, Aura offers additional resources on protecting your identity and securing your accounts.

Digital Disguises

Don't Let Phishing Scams Haunt Your Wallet



By Renee Bourget
Information Security Officer,
Information Technology Division
N.C. Department of State Treasurer

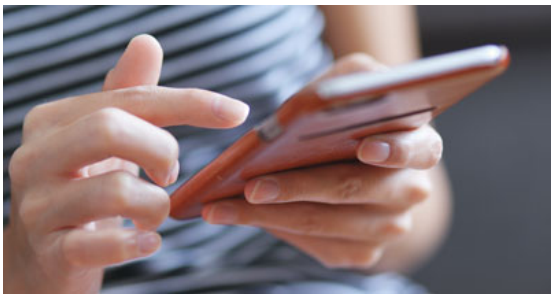
Halloween is the season for masks, costumes and things pretending to be something they are not. Unfortunately, scammers no longer wait until October to put on a convincing disguise.

With artificial intelligence, criminals can create realistic emails, text messages, photographs, videos and even cloned voices. A scammer can appear to be your bank, your employer, a public official or someone you love. Unlike the friendly ghost decorations hanging from the porch, these impostors are interested in something very real: your money and personal information.

Phishing Messages Have Better Grammar Now

Raise your hand if you have ever had to

complete a workplace training on phishing? (I'll just assume most of you raised your hands). Many of us learned to recognize phishing emails by looking for misspellings, unusual wording and poor grammar. That was helpful advice — until scammers discovered AI.



AI can quickly produce polished, professional messages tailored to a particular person or organization. A fraudulent email may include a company logo, familiar names and information collected from social media. It might claim that your bank account has been locked, a payment failed or you are owed a refund.

Sadly, "The punctuation looked trustworthy" is no longer a sound cybersecurity strategy.

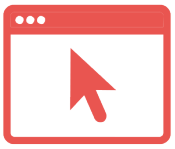
Scammers also use QR codes that lead to fake financial websites. The site may look nearly identical to your bank's actual website, but anything entered there — passwords, account numbers or verification codes — goes directly to the criminal.

Look Behind the Mask

You do not need special equipment, a cybersecurity degree or a supply of garlic to protect yourself. A few simple habits can help keep these digital creatures away from your finances.



Pause before responding. Scammers create fear, excitement or urgency because hurried people are less likely to ask questions. If someone demands immediate payment or personal information, stop and take a breath. The pause button is much less expensive than the panic button.



Inspect email and website addresses. Look beyond the sender's displayed name. Scammers may substitute a letter, add an extra word or use an address that resembles the legitimate one. Be cautious with unexpected QR codes because they can conceal the destination website.



Never share verification codes. A scammer who already has your password may ask for the security code sent to your telephone. Do not provide it. Also, never approve a multifactor authentication request you did not initiate.



Enable multifactor authentication. MFA requires another form of verification in addition to a password, such as an authentication-app code, fingerprint or facial recognition. It is not a magical force field, but it can prevent a stolen password from becoming a stolen account.

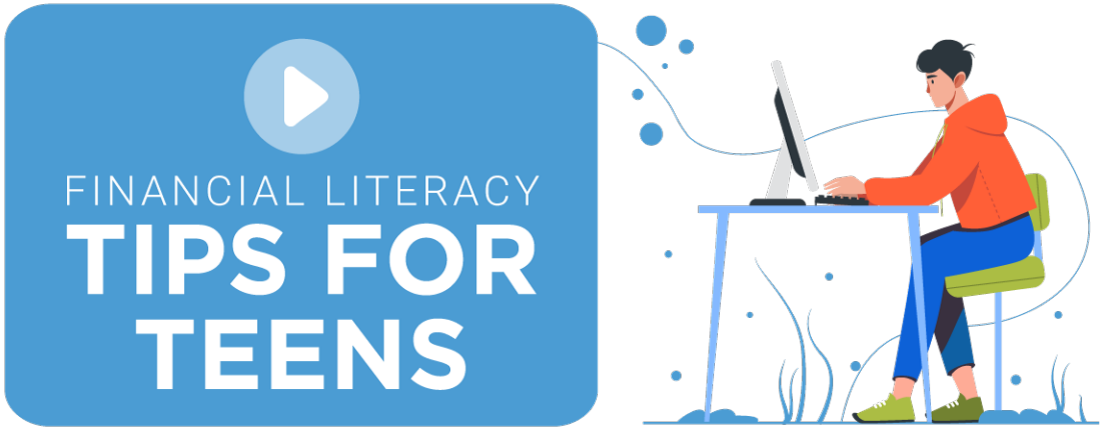
If a Scam Slips Through the Door

If you shared information or sent money, act quickly. Contact your bank or credit-card company, change affected passwords from a trusted device and review your accounts for unfamiliar transactions.

AI can make a scammer look and sound frighteningly convincing. Still, no digital disguise can stop you from pausing, verifying the request and contacting the real person or organization.

This Halloween, enjoy the pretend ghosts and monsters — but do not let an AI-powered impostor haunt your bank account.







Think You Can Spot a Scam?
Think Again.



By John Maron
Director, Investor Protection
& Education Services Program
N.C. Department of the Secretary of State

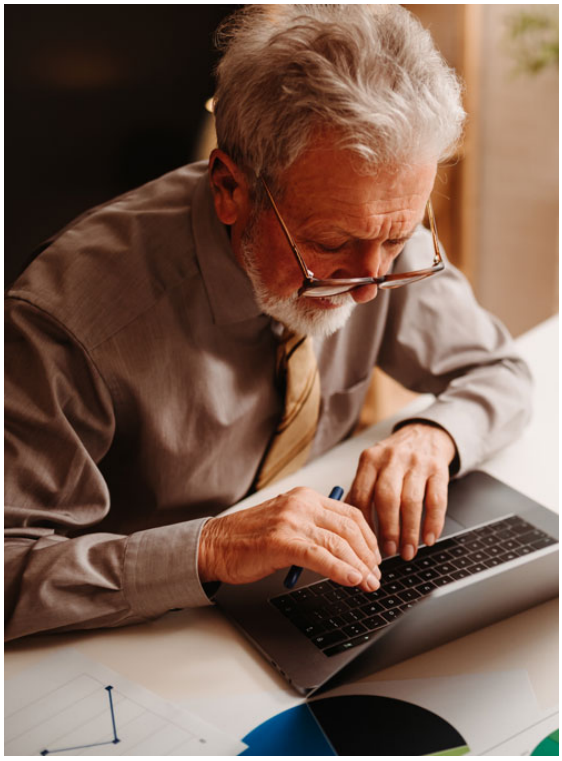
Scammers have gotten very good at looking legitimate.

The pitch might arrive as a great work-from-home job. A hot investment tip. A message from someone who seems to care about you. Or even a video of a celebrity recommending an investment.

Different stories, same goal: **get you to trust them — and then get your money.**

For many seniors, it is even more difficult to spot scams. You did not grow up with the modern technologies that are becoming more and more sophisticated every day. It might not be in your second nature to suspect someone is trying to use these conveniences to try to trick you.

Here are a few scams seniors need to watch out for and where you can find more information.



"Easy Money" Could Make You a Money Mule

Even as we enter retirement, many folks are still looking for a part-time job- to help with the bills or take up some of your new free time.

It will be tempting to take a job being shopped to you through the internet. Have you ever seen a job ad promising flexible hours, little experience and surprisingly good pay for "processing payments"?

Take a pass. You could be getting recruited as a **money mule** — someone who moves money for criminals, often without realizing where it came from.

The pitch can sound perfectly ordinary: process payments, transfer business funds, reship products or help with an investment. In return, you get a commission. The problem? That money may be stolen.

And even if you didn't know it was dirty money, moving it can leave you facing financial losses and potentially serious legal consequences.

Your best defense: Never agree to move money through your bank account for someone you don't know or trust. Click here for more information.

Your "AI Adviser" Might Not Be an Adviser at All

We all lived through the dawn of the digital age- and that was a lot for us to learn and process. It's even harder now. Artificial intelligence is on the rise- and making scams look more convincing than ever.

Today's fraudsters can create slick websites, realistic videos, cloned voices, fake investment platforms and convincing social-media profiles — often in minutes. The

reality is, folks who are trained in AI can even have a hard time picking out the fake creation sometimes.

You might see a celebrity supposedly promoting an investment. You could receive a call that sounds exactly like your financial adviser or a family member. Or you might be directed to a trading platform showing impressive profits that aren't real.

Crypto and AI-themed investment scams are particularly common. Victims may be promised extraordinary or guaranteed returns and then pressured to send money — often in cryptocurrency.

Your best defense: Before investing, verify the person and firm independently. Check registration. Research the investment. And don't assume information generated by AI is accurate. Click here for more information.



When Online Romance Becomes a Money Pitch

We are all looking for that special connection at any age. But, as with many other things, this can now come with dangerous strings attached.

Romance scammers don't usually start by asking for money. They start by building trust. They may spend weeks or months chatting with you, learning about your life and creating what feels like a genuine relationship. Then comes the investment opportunity.

Maybe they're supposedly making a fortune in crypto. Maybe they know a “special” trading platform. Maybe they need a loan. Whatever the story, the destination is the same: **your wallet.**

Watch for someone who:

- Always has an excuse for why they can't meet in person or by video.

- Talks frequently about wealth or investment success.
- Promises unusually high or “risk-free” returns.
- Encourages you to use a particular investment app or website.
- Asks for access to your bank, investment or crypto accounts.

Your best defense: Don't mix a new online romance with your finances. Verify everything independently. Click here for more information.

One Simple Safety Net: A Trusted Contact



Here's an easy step many people overlook: adding a **trusted contact person** to your brokerage or bank account.

Think of a trusted contact as an emergency contact for your money. Under limited circumstances, your bank or brokerage firm can contact that person if it can't reach you or suspects possible financial exploitation.

And don't worry, they don't get control of your account. A trusted contact **cannot make trades, withdraw money or make investment decisions** simply because you've named them.

Your trusted contact could be a family member, close friend, attorney, accountant or another person you trust to look out for you. Click here for more information.

Four Questions to Ask Before You Send Money

When something feels exciting or urgent, slow down and take a moment to think. Ask yourself:

- **Who is contacting me?**
- **Have I independently verified them?**
- **Is the investment or firm properly registered?**
- **Why am I being pressured to act right now?**

Your best defense: Scammers want you to act first and think later. Do the opposite. Pause. Verify. Ask questions. Talk to someone you trust. A few extra minutes of skepticism can save you a lot of money—and a lot of headaches.

Remember: Anyone selling or promoting an investment opportunity generally must be registered with the Secretary of State’s Securities Division. Call our **Investor Hotline at (800) 688-4507** to verify that they are BEFORE you hand your money over. For more information, visit our website at www.sosnc.gov. If you think you may have been scammed, consider filing a complaint.

The NC Department of the Secretary of State is responsible for enforcing the state's securities laws. We are the "go-to" agency for help determining if the investment and its promoters are registered.

This article was written with the help of information and language provided by North American Securities Administrator's Association and the Alerts and Advisories Project Group.

Financial Literacy in Action

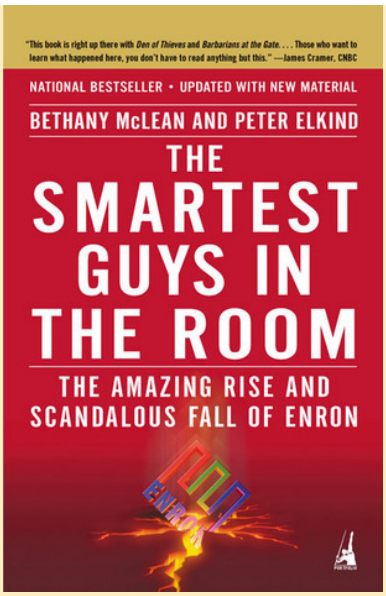
1. *Finance Fridays* editor Loretta Boniti (third from left) was on hand as Roxboro Savings Bank showed its support for financial literacy and our new Cash Clubs by presenting a check to Person High School to help it launch its club. Community support for this effort is not only appreciated but helps to make this program flourish.
2. North Carolina Investment Authority's Ming Xu (center) judged "Shark Tank" style presentations from personal finance and economic students in Person County.





Recommended Reading: *The Smartest Guys In The Room*

This month, Brad's recommended reading is *The Smartest Guys in the Room* by Bethany McLean and Peter Elkin. This book takes the reader through energy company Enron's meteoric rise in the business world and then its disastrous collapse. You can buy this book here, or find a library to borrow it here.





TEST YOUR KNOWLEDGE

For Teens:

A message appears to be from your school and asks you to log in. What should you check first?

- A. Whether it arrived during school hours
- B. Whether the message uses correct grammar and punctuation
- C. The sender's full email address and the link destination

What is a family safe word meant to do?

- A. Help family members verify an emergency request
- B. Help family members unlock a phone
- C. Identify fake emails from scammers

You spot a purchase on your debit card that you didn't make. What should you do?

- A. Contact your bank using the number on your card
- B. Ask your parents if one of them made the purchase
- C. Message the seller on Instagram

For Adults:

You scan a QR code on an unexpected package notice. It opens a login page that looks legitimate. What should you do?

- A. Log in because it came with your package
- B. Close the page and visit the company's official website independently
- C. Tell another family member to scan it and get their opinion

You receive a multifactor authentication prompt that you did not initiate. What should you do?

- A. Change your password by using the link in the prompt
- B. Approve it in case it's a delayed sign-in
- C. Decline it and investigate your account through a trusted route

You receive an urgent email claiming your account will be closed unless you call the number in the message. What should you do?

- A. Call right away to avoid losing access
- B. Forward the email to friends to ask what they think
- C. Look up the organization's contact information independently and contact it directly.

Click here for the answers.

BRADFORD B. BRINER
STATE TREASURER OF NORTH CAROLINA

North Carolina State Treasurer
3200 Atlantic Avenue
Raleigh, N.C. 27604
(919) 814-4000

Questions? Contact us.

Get info about Cash Clubs.

Subscribe to Finance Fridays.

Disclaimer: Any statement made in this Financial Literacy Newsletter ("Newsletter") is not intended as investment, financial, legal, accounting, or tax advice, and any person who subscribes to the Newsletter should consult a qualified professional to address their own specific financial situation. Any use of trade names or trademarks of third parties does not imply affiliation with, endorsement by, or association between them and NCDST. Articles submitted by guest authors for publication in the Newsletter may contain links or QR codes to provide additional references or information to the subscriber, and NCDST cannot guarantee the security or content of these links or QR codes.