Tuscaloosa VA FEDERAL CREDIT UNION

A Community Chartered Credit Union

GRADES 6–12 & ADULTS



Guard It

Protecting Your Money Online

A TUSCALOOSA VA FEDERAL CREDIT UNION WORKBOOK

MY NAME _____

Nobody thinks it will be them

That is exactly what scammers count on. Fraud is not about being gullible. It is about being caught at a busy moment by a message built to rush you. This book shows you the patterns, so you recognize them before your money moves instead of after.

WHAT IS INSIDE

Six lessons

1. Passwords & Personal Information — p. 3
2. Phishing by Email, Text & Phone — p. 5
3. Fake Stores and Too-Good Deals — p. 7
4. The Scam Playbook — p. 9
5. Your Digital Footprint — p. 11
6. If It Happens to You — p. 13

For teachers and families: This one works across ages. Middle schoolers focus on lessons 1 through 3, high schoolers and adults on all six. Lesson 6 is the one worth reading before you need it.

Passwords & Personal Information

Most accounts are not broken into. They are guessed into. People build passwords out of things they have already posted publicly, and a stranger with ten minutes on your profile can often assemble one.

THINK LIKE A THIEF

Build a password from a public profile

> **WHAT ALEX'S PROFILE SHOWS**
>
> Birthday 4/12/2007 · Dog named Biscuit, adopted 2019 · Went to Maple Ridge Elementary · Posts constantly about the Westbrook Falcons · Favorite food is clearly pizza · Born in Westbrook

Fill in the formulas people actually use. Capitalize the first letter of each word and use no spaces.

1. Pet name + adoption year: _____
2. Go + team mascot + "!": _____
3. Favorite food + birth year: _____

Now answer the security questions a website would ask, using only the profile:

4. What elementary school did you attend? _____
5. What city were you born in? _____

See how fast that was? Security questions are often weaker than the password itself, because the answers are usually public. You are allowed to answer them with something false, as long as you can remember it.

Building One That Holds

A strong password is long and unrelated to you. Length matters more than symbols, which is why a phrase of several random words beats a short scramble of characters.

THE RULES

Good password habits: check the ones you already do

- [ ] At least 12 characters, and longer is better
- [ ] No names, birthdays, pets, schools, or teams connected to you
- [ ] Not reused on any other account
- [ ] Let a password manager create and remember most of your passwords for you
- [ ] For the few you must memorize (your phone, your password manager), use four or more random words strung together. The pattern looks like “word-word-word-word-7,” but never use one you have seen printed anywhere, including here.

Now make one up for Alex, for practice only. Use nothing from their profile, and never use it for real:

Explain why yours would be hard to guess:

TWO-FACTOR

The single most useful thing you can turn on

Two-factor authentication asks for a second proof after your password, usually a code sent to your phone. Then a stolen password alone is not enough. One rule matters most: **a code sent to you is yours alone.**

> **THE MOST COMMON ATTACK RIGHT NOW**
>
> Someone calls claiming to be your credit union’s fraud department. They say they need to verify your identity and ask you to read back the code that just arrived by text. That code is the last thing standing between them and your account.

What should you do instead?

Phishing by Email, Text & Phone

Phishing is when a scammer pretends to be an organization you trust so you will click a link, enter a password, or hand over account details. It arrives by email, by text (sometimes called smishing), and by phone call (vishing). The shape is always the same.

ANATOMY

The five parts of almost every phishing message

1. **A trusted name.** Your bank, a delivery service, a streaming account, the IRS, your employer.
2. **A problem.** Suspicious activity, a failed payment, a package held up, an account about to close.
3. **Urgency.** Act within 24 hours. Respond immediately. Your account will be locked.
4. **A link or number they supply.** Never the one you would have looked up yourself.
5. **A request for something only you should have.** Password, PIN, one-time code, full card number, Social Security number.

> **The one habit that defeats all of it:** Never use the contact route the message gave you. Close it, and reach the organization the way you already know: the number on the back of your card, the app you already have, the website you type yourself.

Spot the Red Flags

Three real-shaped messages. Circle what is wrong with each, then write the biggest warning sign.

THREE MESSAGES

Circle what is wrong, then name the biggest warning sign

> **FROM: +1 (447) 022-9183**
>
> TAVCU ALERT: A $420.00 debit to AMAZON was attempted on your card. If this was NOT you reply NO and our agent will call you within 5 minutes to reverse it. Ref#88213

Biggest warning sign:

> **FROM: SECURITY@TVACU-VERIFY.COM**
>
> Dear Valued Member, We have detected unusual sign-in activity. Your account has been temporarily limited. Please click here to re-verify your online banking username, password, and Social Security number within 24 hours or your account will be permanently closed.

Biggest warning sign:

> **CALLER ID SHOWS YOUR CREDIT UNION'S REAL NUMBER**
>
> "This is the fraud department. We stopped a charge in another state. To confirm you are the cardholder, I'm sending a six-digit code to your phone now. Can you read it back to me? Also, to secure the funds we'll need to move them to a protected account I'll set up for you."

Two things are wrong here. Name both:

Caller ID can be faked. A number matching the real one proves nothing.

Fake Stores and Too-Good Deals

Online marketplaces and pop-up storefronts are easy to create and easy to abandon. A fake store does not need to fool you for long. It needs to fool you once.

RED FLAGS

What a fake storefront usually has

- ⚠ Prices far below everyone else, on an item that is in high demand
- ⚠ No physical address, no working phone, and a contact form only
- ⚠ “Privacy policy: coming soon” or pages that go nowhere
- ⚠ Countdown timers and “only 2 left” on every single product
- ⚠ Reviews that are all five stars, posted the same week, in similar phrasing
- ⚠ Payment only by gift card, wire, cryptocurrency, or a “friends and family” transfer
- ⚠ A web address that is almost right, like a real brand with an extra word or a different ending

Why the payment method matters most: A credit card purchase can be disputed. A debit card has fewer protections. A gift card, wire, or crypto payment is effectively cash handed to a stranger, and it is almost never recoverable. When a seller insists on one of those, that is the answer.

Evaluate This Listing

Read the storefront below, then mark it up.

THE SITE

shopsforbops-official-deals.com

> **FRONT ROW CONCERT TICKETS + MEET AND GREET**
>
> **$89** ~~$420~~ · BEST DEAL YOU WILL FIND!!! · Only 2 left, sale ends in 00:04:11
>
> Payment: Zelle, Cash App, or gift card only. No refunds.
> Privacy Policy: Coming Soon · Contact: form only
>
> **Reviews (4.9 stars):**
> "Great seller fast delivery!!" · "amazing deal thank you!!" · "Best experience ever!!"
> "This place is a scam. When I showed up to the venue they said my ticket was fake."

MARK IT UP

List four red flags you can find

1. _____
2. _____
3. _____
4. _____

DO IT RIGHT

You genuinely want to go to this concert. How would you buy tickets safely?

_____

_____

_____

The Scam Playbook

Scams get new names every year, but they run on a small set of scripts. Learn the scripts and the new version is recognizable on sight.

MATCHING

Write the letter of the definition next to each term

_____ 1. Phishing

_____ 2. Romance scam

_____ 3. Imposter scam

_____ 4. Prize or lottery scam

_____ 5. Affinity fraud

_____ 6. Debt collector scam

_____ 7. Overpayment scam

_____ 8. Ransomware

A.	Software that locks your device or files until you pay to get them back.
B.	Posing as a grandchild (the “grandparent scam”), a boss, the IRS, or a utility, and demanding payment right now.
C.	Sending a check for more than the agreed amount and asking you to return the difference before it bounces.
D.	A fake email or text from a company you trust, to get you to click a link or type a password.
E.	Threatening emails or calls about a debt you may not owe, demanding immediate payment.
F.	Building a romantic relationship online, then asking for money, gift cards, or help “moving funds.”
G.	Claiming you won something, but you must pay a fee or confirm private details to collect.
H.	Claiming shared membership in a church, military unit, or alumni group to borrow trust quickly.

What Would You Do?

Four situations. Name the scam (some fit more than one, so pick the best match), then write the next move you would actually make.

SCENARIOS

Name it, then act

> **1. A CALL AT 9PM**
>
> A shaky voice says “Grandma? I’m in trouble, I was in an accident and I need bail money, please don’t tell Mom.” A second person takes the phone, says they are a lawyer, and needs $2,000 in gift cards tonight.

Scam: _____

My move: _____

> **2. SIX WEEKS OF MESSAGES**
>
> Someone from a dating app is warm and attentive but always has a reason video chat will not work. They mention a crypto platform that has been good to them, and offer to walk you through your first deposit.

Scam: _____

My move: _____

> **3. SELLING A COUCH ONLINE**
>
> A buyer sends a check for $900 on a $300 couch, calls it an assistant’s error, and asks you to deposit it and send back $600 by Cash App today so they can arrange pickup.

Scam: _____

My move: _____

> **4. AT CHURCH**
>
> A new member mentions an investment returning 3% a month, guaranteed, open only to people in the congregation. Several members you respect have already put money in.

Scam: _____

My move: _____

Your Digital Footprint

Your **digital footprint** is the trail of information about you online: what you posted deliberately, and what was collected about you along the way. Scammers do not start by attacking your account. They start by reading it.

AUDIT

What can a stranger learn about you in ten minutes?

Search your own name. Check your own profiles while logged out. Check each one that is publicly visible.

- [ ] My full birthday, including the year
- [ ] My hometown or current city
- [ ] My school, workplace, or employer
- [ ] My pets' names
- [ ] Family members' names and relationships
- [ ] Photos showing my street, house number, or car plate
- [ ] My phone number or email address
- [ ] When I am away from home

How many did you check? _____ of 8

CONNECT IT

Go back to Lesson 1

Which items above could be used to guess a password or answer a security question?

Identity Theft and Locking It Down

Personally identifiable information is the set of details that can be used to impersonate you: Social Security number, date of birth, full account numbers, driver's license, mother's maiden name. Never post these, and only give them out when you started the contact yourself.

THINK ABOUT IT

Short answers

1. Why is it risky to let a shopping site save your card and autofill your details?

2. A quiz asks for your first car, your street growing up, and your mother's maiden name to reveal your "spy name." What is actually happening?

3. An employer can see your public posts. Name one thing you would clean up before applying for a job.

LOCK IT DOWN

Six things worth doing this week

Check each one as you finish it.

- [ ] Set social accounts to private, and review who is actually on the list
- [ ] Remove your birth year and hometown from public profiles
- [ ] Turn on two-factor authentication on email first, since email resets everything else
- [ ] Turn on transaction alerts in your credit union app
- [ ] Check your credit report free at annualcreditreport.com
- [ ] Stop posting travel plans until after you are home

Protect email above all: Whoever controls your email can reset the password on nearly every other account you own. If you only harden one thing, harden that.

If It Happens to You

Being scammed is not a character flaw, and shame is the reason most fraud goes unreported. Speed matters far more than blame. The first hours are when money can still be stopped.

FIRST 24 HOURS

In this order

1. **Call your credit union immediately** using the number on the back of your card or its official website. Report the transaction and ask them to freeze or close the affected account.
2. **Change the password** on the affected account and on your email. Turn on two-factor if it is not already on.
3. **Write down everything** while it is fresh: dates, amounts, phone numbers, screenshots, what was said.
4. **Report it at reportfraud.ftc.gov**, and at identitytheft.gov if your identity was used.
5. **File a police report** locally. Some institutions require one to proceed.
6. **Freeze your credit** at all three bureaus. It is free, and it stops new accounts from being opened in your name.

> **Tell someone.** Scammers rely on embarrassment to keep victims quiet, which is exactly what lets them keep working. Reporting it protects the next person as much as it helps you.

Your Emergency Card

Fill this in now, while nothing is wrong, and keep it somewhere you can find it fast.

FILL IT IN

Who I call

My credit union, from my card or its website	
My card issuer, if different	
Local police non-emergency line	
A person I trust to talk it through with	

REFERENCE

Where to report and freeze

Report fraud	reportfraud.ftc.gov
Identity theft recovery plan	identitytheft.gov
Free credit reports	annualcreditreport.com
Credit freeze	Equifax, Experian, and TransUnion, each separately

PRACTICE THE SENTENCE

Write what you will say when a call feels wrong

Having a sentence ready makes it far easier to use. Example: “I’m going to hang up and call the number on my card.”

You are allowed to be rude. Hanging up on someone who might be legitimate costs you thirty seconds. Staying polite with someone who is not can cost you everything in the account.

Your Credit Union Is on Your Side

Where you keep your money changes who picks up the phone when something goes wrong. Here is what protects you, and the one thing that does not.

COMPARE

Bank vs. credit union

	BANK	CREDIT UNION
Who owns it	Investors who buy its stock	Its members, the people who save and borrow there
Who it works for	Its shareholders, who expect a profit	Its members. It is not-for-profit
Deposits insured by	The FDIC, up to $250,000	The NCUA, up to $250,000
Unauthorized debit charges	Federal rules limit your loss if you report fast	The same federal rules apply
Money you were tricked into sending	Often not recoverable	Often not recoverable

Deposit insurance protects your money if the institution itself fails. It does **not** cover money you send to a scammer yourself. That is why speed matters: the sooner you call, the better the chance a payment can be stopped.

BEFORE YOU NEED IT

Write down the real contact details now

Copy these from your card, a statement or the official website, not from a text or email.

TVACU phone number	
Website I type in myself	tvacu.com
Card lost or stolen line	

Calling quickly gives the credit union the best chance to stop the money and to warn other members about the same scam.

The Short Version

If you remember nothing else from this book, remember these.

SIX RULES

Fill in the missing words

WORD BANK

hang up · urgency · never · freeze · two-factor · gift cards

1. Your credit union will _____ call and ask you for a one-time code, your PIN, or your password.
2. Any message that creates _____ is suspicious by default. Real institutions let you take your time.
3. Nobody legitimate asks to be paid in _____, wire transfers, or cryptocurrency.
4. When a call feels wrong, _____ and dial the number on the back of your card instead.
5. Turn on _____ authentication everywhere it is offered.
6. If your identity is stolen, _____ your credit at all three bureaus.

TEACH SOMEONE

Who in your life is most at risk, and what is the one thing you will tell them?

Stay sharp.

Scams change constantly, but the pressure tactics behind them almost never do. Slow down, verify separately, and you will catch nearly all of them.

TUSCALOOSA VA FEDERAL CREDIT UNION

Serving Tuscaloosa and Sumter Counties since 1951.

tvacu.com

Teachers and group leaders: request class sets and the free answer key.

Request class sets →

Scan or visit **tvacu.getostrich.com/classroom**

This workbook is provided for educational purposes only and is not financial advice.
Anyone who lives, works, worships, or attends school in Tuscaloosa and Sumter Counties, Alabama, plus their family, can join.
Federally insured by NCUA. Equal Housing Opportunity.