Monitor your accounts.

Use our free digital resources* to track your accounts and **catch fraud early**.

eAlerts

By text, email, or phone, we can let you know when your account balance goes above or below your chosen limit or when a specific charge or check number clears your account. To receive custom alerts with your own rules, click ***Manage Alerts*** under the ***Profile and Settings*** tab in digital banking.

eNotices

Instead of waiting days for the mail to arrive, sign up for eNotices and receive important notifications by email. Want to enroll? Log into digital banking and click ***eNotices*** under the ***Profile and Settings*** tab.

eStatements

With a permanent digital copy of your Visions accounts, you can review current or past transactions without sorting through stacks of paper. When logged into our secure server, you can find ***Statement Delivery Preferences*** and the ***eStatements*** menu under the ***Services*** tab.

IDNotify™ by Experian®

As a Visions member, you have access to **free** identity theft protection, including credit monitoring, family protection, and more. For details, go to **visionsfcu.org/idnotify**.

VISA® Purchase Alerts

Want to know when your credit or debit card is being used outside the country? Or when a purchase exceeds $250? Enroll in Purchase Alerts for your peace of mind. More information is available at **visionsfcu.org/creditcards**.

We're more secure together.

As you know, protecting your money is essential. While we have dozens of security measures in place to protect your funds and personal information, remember that fraudsters don't only target banks and credit unions with their scams – they often target you directly.

If you have questions about the information in this pamphlet or need assistance adding security features to your online banking, reach out to us.

And if you suspect you've been the target of fraud, you can file a complaint with the Internet Crime Complaint Center at **IC3.gov**.

To report fraud on a Visions account, call **800.242.2120** or send the details to **reportscams@visionsfcu.org** ***(do not include your account number or other identifying information)***.

We're more secure together.

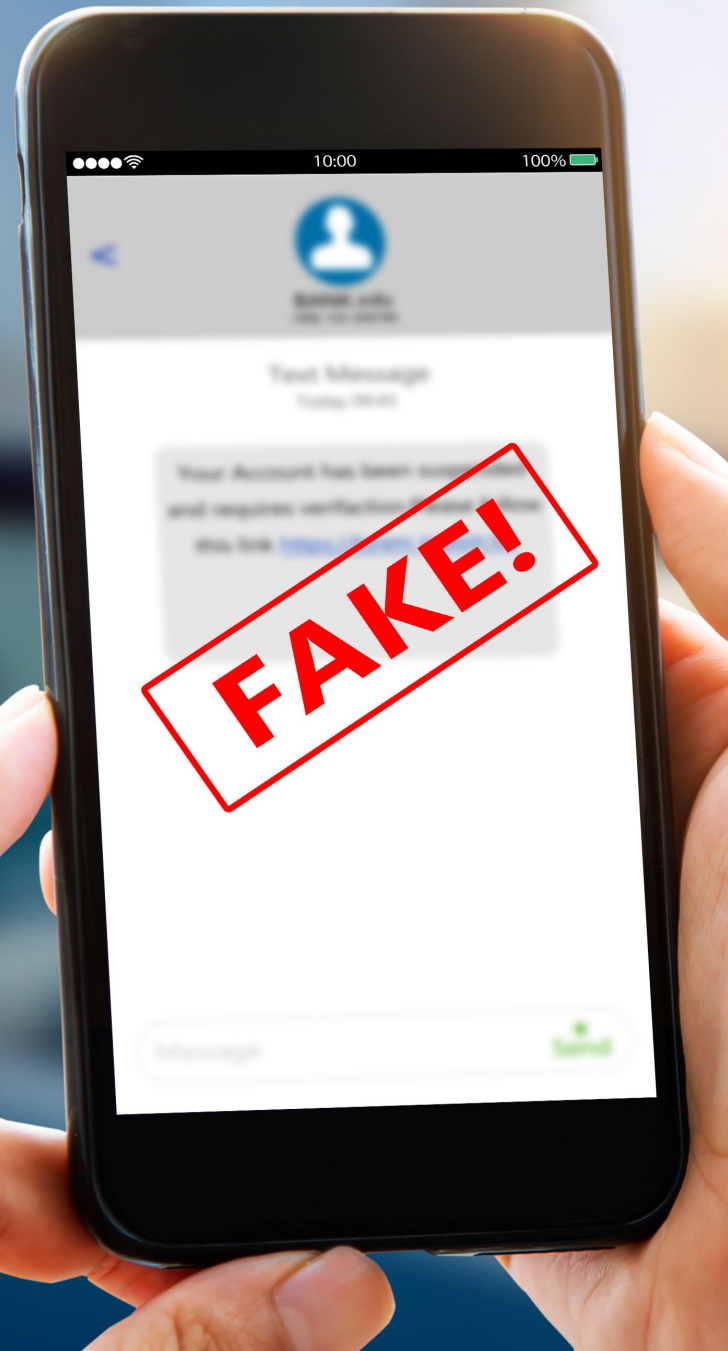
**Visions membership requires a $1 minimum deposit. New members are subject to membership requirements. Ask a representative or visit visionsfcu.org/join for eligibility details.*

VISIONS
FEDERAL CREDIT UNION

Federally insured by NCUA BC2 221024 7.5M 6/22

Your Role in Fraud Protection

Common Threats • Helpful Tips • Resources



Know the threat.

Vehicles for fraud

Most fraud involves spoofing, the attempt to mimic legitimate companies as a disguise to gain your trust. Once you're convinced that the spoof is a trusted source, it's easy for scammers to get your personal information – or your money! Here's how they do it.

Emails – When a fraudulent email attempts to obtain your personal information, it's known as phishing. Not all phishing attempts will be sent to your junk folder.

Text messages – SMiShing is a scam that uses fraudulent text message or SMS (short message service) to get your information. They usually include fake links and sometimes spoof legitimate phone numbers.

Phone calls and voicemail – Informing you of an urgent matter, a caller might ask you to reply with your personal information or make a "late payment."

QR codes – Think before you click. Crooks are able to replace physical or digital QR codes, linking you to a malicious or spoofed website.

Common scams

When fraudsters lure you in, they use tactics to rouse your emotions to get what they want. Look out for their common strategies:

- Messages from tech support, verifying your account information or warning you of a recent cyberattack
- Customer service, asking you to verify a recent purchase or update your account details
- Con artists who develop romantic relationships online, eventually requesting money transfers
- Savings and holiday deals that seem "too good to be true" tend to end in non-delivery or non-payment
- Unsolicited requests for charitable support or disasters relief, coming from organizations or people you don't recognize
- Business opportunities that promise no risk, low risk, or a "guaranteed return on investment"

Remember: if you receive an email, text message, or phone call from a company – even if it's Visions – you can hang up and call back at a trusted number. That way you can be sure you're speaking to the right company. For Visions, that number is **800.242.2120**.

Protect your information.

To protect your accounts, protect your information. Follow these five guidelines to reduce your chances of being scammed.

1. **If it seems fishy, it's probably phishing.**
   Examine the message for spelling, fake URLs, and other indicators of spoofing, and avoid clicking any links or downloads unless you completely trust the source.

2. **When in doubt, verify the source.**
   Don't trust the contact information or links provided in the message. Instead, look up the company's information using a trusted site.

3. **Never give anyone your account information**
   Remember: no company – not even Visions – will ever call to ask you for your user ID, password, PIN, or one-time passcode. These items should only be entered by **YOU** when **YOU'RE** logging into a trusted source. If someone requests this information from you – you should **NEVER** under any circumstances provide it to anyone.

4. **Only send money to people you trust.**
   Treat your funds like cash and resist the pressure to act quickly – scammers love to create a sense of urgency. If making a payment online, verify the seller and use a secure payment method.

5. **Regularly review your cybersecurity.**
   This includes keeping the most recent software updates on your phone and computer, anti-virus and firewall protection, and strong, unique passwords with two-factor authentication for your online accounts.