NUVISION CREDIT UNION

Fraud & Scam Protection Hygiene

Part 1: Prevention Hygiene –Protecting Yourself

1. **Digital "Cleanliness"**
    a. Use strong, unique passwords (and change them often)
    b. Enable multifactor authentication (MFA) wherever possible
    c. Avoid savingpasswords in browsers–use a secure password manager instead
    d. Keep devices and apps updated
2. **Communication Caution**
    a. Don't click links or open attachments from unknown sources
    b. Confirm requests for money, gift cards, or personal information–especially If it feels urgent
    c. Be wary of spoofed caller IDs and fake email domains. When in doubt, contact the sender directly through official channels.
    d. Avoid engaging with scammers; even replying "stop" can validate your contact information
3. **Financial Vigilance**
    a. Monitor bank and credit card accounts regularly
    b. Set-up transaction alerts
    c. Freeze your credit if you're not actively applying for loans
    d. Beware of "too good to be true" deals or urgent investment opportunities
4. **Privacy Protection**
    a. Limit what you share on social media (scammers use information from these sites to build convincing stories or to glean details that may be used for identity verification / challenge questions
    b. Review privacy settings often
    c. Shred sensitive documents before discarding
    d. Opt out of data broker lists where possible

Part 2: Recovery Hygiene –What to Do if It Happens to You

1. **Act fast!**
    a. Report the scam to the credit union immediately
    b. Freeze your credit if identity theft is involved
    c. Reset passwords for affected account (and any others that reused the password)

2. **Report It**
    a. File a report with the FTC at reportfraud.ftc.gov
    b. Report phishing to your email provider and/or if the phishing email was related to Federal taxes, tophishing@irs.gov
    c. If money was requested or sent via a platform like Zelle® or CashApp, report to them as well
3. **Monitor for Fallout**
    a. Check credit reports at annualcreditreport.com
    b. Watch for new accounts, changes to your existing account/credit lines, or IRS/tax notices
    c. Consider enrolling in an identity theft monitoring or protection program
4. **Be Kind to Yourself**
    a. Shame thrives in silence–talk about it. Remember, scams are designed to trick everyone.
    b. Help others by sharing your story
    c. Stay updated on new scams and tactics