# Protect Yourself Online

## from Banking Fraud and Social Engineering Scams

### Use Strong, Unique Passwords

- Use at least 15 characters with a mix of letters, numbers, and symbols.
- Leverage the passphrase technique.
- Don’t reuse passwords across accounts.

### Enable Multi-Factor Authentication (MFA)

- Always opt for MFA on your financial, email and other important accounts.
- Use an authenticator app, when possible, instead of SMS-based MFA.

### Watch Out for Social Engineering Tricks

- Don’t trust unsolicited calls, texts, or emails claiming to be from your credit union - even if the caller ID/ sender appears to be legitimate.
- Never share your passwords, PINs, or verification codes with anyone—even if they claim to be from your credit union.

### Avoid Clicking on Suspicious Links

- Hover over links in emails before clicking.
- Look for misspellings or strange domain names.
- Access your credit union only through their official website not through search engine results. Bookmark the official website to your browser favourites.

# Protect Yourself Online

## from Banking Fraud and Social Engineering Scams

### Keep Personal Info Private

- Don't overshare on social media.
- Tighten the default privacy settings on social media accounts.
- Shred documents containing personal information.

### Verify Requests for Money or Information

- Always confirm requests for funds or sensitive information using a trusted method.
- When selling items online, watch out for fake e-transfer links.
- Watch out for fraudulent items sold online such as event tickets.

### Update Software and Apps Regularly

- Install security updates for your phone, computer, and apps as soon as they're available.
- Enable automatic updates where possible.

### Avoid Public Wi-Fi for banking

- Don't log in to your credit union account using public or unsecured Wi-Fi.
- If needed, use a VPN to protect your connection.

# Protect Yourself Online

## from Banking Fraud and Social Engineering Scams

### Set Up Alerts and Monitor Your Accounts

- Enable real-time alerts for logins, large withdrawals, or other unusual activity.
- Review your statements regularly and report any unfamiliar activity.

### Educate Yourself and Your Family

- Stay informed on common scams like phishing, vishing (voice phishing), and smishing (SMS phishing).
- Share tips with family members, especially seniors and teens, who may be more vulnerable.

### Use Official Credit Union Channels Only

- Download mobile apps only from trusted sources like the Apple App Store or Google Play.
- Ensure the app is published by your actual credit union—not a copycat.

### Report Fraud Immediately

If you suspect fraud or believe you've been scammed, contact your credit union right away.

**REMEMBER**:

- Stop. Think. Verify.
- Scammers rely on urgency and emotion. Taking a moment to double-check can make all the difference.