TOP 10 SECURITY DOS & DON'TS

CO-OP FINANCIAL SERVICES

DO

1. **Be observant when withdrawing cash from ATMs.**
Look for wobbly parts and malfunctioning screens as these may indicate the presence of a card skimmer. Contact your card issuer immediately if you inadvertently insert a card into a suspicious ATM.

2. **Know your daily balance for checking and savings accounts.**
Even better, sign up for mobile card controls and alerts that notify you of transactions – with the option to block those you don't recognize.

3. **Check your own credit.**
Identity thieves are hard at work opening accounts in the names of innocent consumers – don't let this be you. Every consumer in the U.S. is entitled to receive a copy of his or her credit report once a year. Here is a link to get you started: https://www.annualcreditreport.com/index.action.

4. **Check your FICO score on a regular basis.**
Many credit unions display it when you log into their online banking systems. You can also access your FICO score at www.MyFICO.com for a nominal fee.

5. **Read the fine print.**
Before submitting payment information or even clicking links, double check all URLs and e-mail addresses. Make sure there are no extra commas or other unusual characters. Fraudsters are masters at impersonating brands and individuals. Run frequent virus scans on all home PCs and Android devices as well.

DON'T

6. **Just download apps from anywhere.**
There are many unlicensed banking apps out there, and many popular smartphone apps today that appear harmless – but that contain risky code. If you need to access mobile banking, get the app from your credit union's website – not Snapchat.

7. **Believe everything you hear or read.**
Fraudsters love to catch people when their resistance is down and frequently attach a sense of urgency to their requests. If someone calls or texts you 'with a very important message from your card issuer,' don't pick up and don't respond. Place a separate call to your card issuer to assess the situation.

8. **Talk to unknown callers.**
If you don't recognize the phone number on the other end of the line, don't answer. Fraudsters are aggressive, and there are many tools out there they can use to synthesize human voice now. Don't give away a sample of yours.

9. **Swipe cards.**
EMV chip cards and digital wallets like Apple Pay are much more secure than that old magnetic stripe. If a business is still asking you to swipe at checkout, shop elsewhere.

10. **Store card numbers on merchant sites you don't frequent for future use.**
A breach on any site can send your card data straight to the dark web. Use Visa Checkout and Masterpass instead to protect sensitive card data, and always look for that little lock in your browser window to ensure that a webpage is secure.

TOP 10 SECURITY DOS & DON'TS

CO-OP FINANCIAL SERVICES

BOTTOM LINE:

Follow our **SEA** approach for smooth sailing.

S low down! If a caller or texting party unknown to you is urgently requesting your card or personal data, hang up or ignore the text until you can evaluate the situation.

E valuate: Do you own fact finding regarding calls and e-mails to determine why anyone needs your social security number, date of birth or PIN. Chances are, no one needs this information except a criminal.

A ct: Notify your credit union immediately if you think you have encountered a fraudster.