Fraud Education

As fraudsters continue to become more sophisticated in their ability to access members' account information to commit fraud, DFDFCU would like to provide some helpful information on current scams and ways to protect your information.

Tips for Seasonal and Holiday Charity and Travel Scams:

- Fraudulent charity scams will "pressure" you to make donations immediately. Remember, a legitimate charity will welcome your donation whenever you choose to make it.
- Never send donations in the form of gift cards or wire transfers.
- Watch for travel deals that are too good to be true and know who you are booking your travel through.

Two-Factor Authentication Scams:

As fraud controls become smarter, fraudsters shift their attack patterns to bypass controls. For example, fraudsters have been using automated phone calls to steal consumers' two-factor authentication codes and hack into banking, merchant, and third-party payment accounts. These include Apple, Amazon, PayPal, and bank accounts.

An example of this type of call states, "To secure your account, please enter the code we have sent your mobile device now." You can tell this is an attempt of a fraudster to gain your information because financial institutions and valid merchants will ask cardholders to enter this code on their website or app, not by an automated phone call or a text. Communication like this indicates that the fraudster has already tried to access the account and was presented with a two-factor authentication request from either a merchant or financial institution. This type of phishing call attempts to secure the code sent to the phone number or email on file at the merchant or financial institution. Usually, the code has already popped up on your phone by a text message or has come through your email. Once entered, the automated message will say, "Thank you, your account has been secured, and this request has been blocked." Sometimes the call will say, “don't worry about any payments or fees; we will refund it” and then state, "you may now hang up." Scams like these require a hacker to know several details about a cardholder such as an email address, phone number, and passwords. Personal data like this is often found on the dark web, collected from previous breaches and hacks, sold by POS merchants to marketers, or given out by cardholders themselves.

To prevent fraud from occurring, hang up and do not provide any authentication codes over the phone.

Phishing/Smishing Attacks

Phishing and smishing (phishing by SMS texts) are used by fraudsters to trick members into providing sensitive and confidential information. They then use this information to perpetrate fraud. The frequency of these attacks continue to be on the rise and are becoming more sophisticated and difficult to identify. Instead of using only suspicious links in poorly designed emails, phishing emails mimic websites and appear legitimate and credible. In addition, the use of web address shortening tools, such as TinyURL, makes detecting suspicious links more difficult even by savvy online users.

All members must safeguard their financial data and online banking credentials against criminals trying to harvest them. We recommend you avoid clicking on links that appear in random emails and text messages. Some phishing emails will start with "Dear Customer," so be on the alert when coming across those emails. If you are ever in doubt, go directly to the source of the email rather than clicking on a potentially dangerous link.

In general, members should never give out whole card numbers, passwords (either to bank or merchant accounts), social security numbers, or other sensitive information over the phone.

Securing Digital Devices:

Members should avoid storing confidential card information in an unencrypted format on digital devices unless stored using a Digital Wallet or secure password management application. Security concerns to be aware of include:

- Unencrypted card information on digital devices is susceptible to malware attacks.
- Sensitive information, such as PIN, Social Security number, or answers to security questions can also be stolen through malware and remote access applications downloaded to a digital device.
- Choose *reputable* and *secure* applications to store passwords and other sensitive data on digital devices. Avoid installing applications from alternative online "stores" that are not reviewed for security before publication.