Reporting Scams

If you believe you've been targeted , contact the following:

- Your Credit Union or Bank to place an alert on your account & close debit card if compromised.
- Your local police department
- Internet Crime Complaint Center (IC3) www.ic3.gov
- Federal Trade Commission (FTC) www.FTC.gov/complaint

Staying Safe

Buying some time—In an emergency, it's natural to act before you have time to think. It's no coincidence that many scams are designed to encourage an immediate reaction before you have a chance to spot any red flags. Allow yourself to take a minute to assess a situation even if it seems urgent.

Use the Address Bar—Get in the habit of visiting websites directly instead of following links contained in emails. It takes only a few extra seconds and helps you be more mindful about your online activity.

Cross-Reference—It's perfectly reasonable to verify the identity of the person or business you're in contact with. Use a means outside of the original communication, like doing a separate web search or returning a call through a publicly listed number.

Learn more information on Identity Theft and

Foiling Identity Theft!

Identity theft is the fastest-growing non-violent crime in North America. Globally, it costs its victims billions of dollars, not to mention the time and hassle involved in recovering a stolen identity. The key to preventing identity theft is being smart with your personal data in all its various forms.

5 Easy things you can do right now to prevent identity theft:

1. Change up your PIN—Do you use the same PIN to unlock your phone as to use your debit card? If so, change it! Also, use our bio-metric options available on our mobile app for safer access to your credit union account.
2. Get a Shredder—Bank statements, expired credit cards, bills, pre-approval notices, anything with account numbers and personal information should be shredded before they make their way to your trash or recycle bin.
3. Slim Down your Wallet—It's time to clean out those receipts and store cards you never use. If your wallet is lost or stolen, every extra item you carry gives identity thieves an extra chance to steal your information.
4. Update your Software—New computer viruses are circulated every day. The best way to stay ahead of the curve is to install regular updates to firewall, anti-virus and operating systems. Resist the urge to hit "Remind me Later".
5. #Social Media Share—Does your social media

Cal Poly Federal Credit Union

How to spot SCAMS

CAL POLY
• Federal Credit Union •

How to Spot a Scam?

If you use a cellphone or have an email account, you've likely been exposed to an attempted scam. This brochure shares some common types of scams. But criminals are cleaver and always changing the narrative, so it's always **a good practice to be skeptical of anything that is too good to be true.**

Types of Scams

Familiarizing yourself with common scams can help you spot them before they turn into costly mistakes.

Unexpected Money

The Set-up—A wealthy person asks the target for help with the transfer of a large sum of money, or an estate lawyer notifies the target of a large inheritance form a distant relative.

The Swindle—The target is required to pay fees or taxes before the transfer of money can be processed. The target writes a check or provide bank account access in order to complete the transfer. The target never receives the money.

Unexpected Winnings

The Set-up—The target is notified that they've won a lottery, contest, sweepstakes or some other prize giveaway.

The Swindle—In order to claim the prize, the target is instructed to pay a lottery tax or provide personal information. The prize winnings are never received.

Dating Schemes

The Set-up—The target is charmed by a new

Dating Scheme Continued

The Swindle—The new sweetheart is actually a scammer; once the relationship has developed the scammer asks for expensive gifts, travel or cash.

Employment

The Set-up—this scam's details change, but the premise remains the same. The target answers an ad for part-time or work from home employment.

The Swindle—the scammer sends the target checks to deposit to their bank/credit union account or asks for the target's online banking access to make deposits. The scammer will ask the "employee" to "mystery shop" a store to buy gift cards or send money through Western Union. The employee fills out a Mystery Shopper questionnaire about the store's service. Only to learn from their bank or credit union that the checks deposited where fraudulent.

Other versions of this scam—The "employer" may also ask the "employee" to order a service online from the deposited funds. Or ask them to buy gift cards for a charity and submit the gift card numbers electronically. Whatever the method the end result is the same, the "employee" is stuck with their bank account charged for the fraudulent deposited checks.

Fake Charities

The Set-up—The target is contacted by a charitable organization and asked to make a donation.

The Swindle—Scammers pose as existing charities or invent fake ones and then pocket the donations.

Buyer-Seller Fraud

The Set-up—The target comes across a tempting online listing for a premium item at an extremely low price.

The Swindle—Scammers collect the payment but never deliver on the product; multiple accounts and fake accounts and fake reviews are used to disguise their deceptive practices.

Get Rich Quick Schemes

The Set-up—A job placement service offers to find a position for an unemployed target, or the target is approached by a businessperson with an investment opportunity.

The Swindle—The scammer collects placement fees for their fraudulent job placement service, or takes off with the target's investment money.

Threats and Extortion

The Set-up—The target receives urgent demands for money from a government official or from law enforcement, or the target discovers ransomware on their computer.

The Swindle—The scammer poses as an authority figure to scare the target into paying them; the scammer holds computer files hostage to pressure the target into paying them.

Identity Theft

The Set-up—The target is asked to log into their account or confirm their password, or the target is contacted by a friend or relative and asked a series of personal questions.

The Swindle—The scammer impersonates the