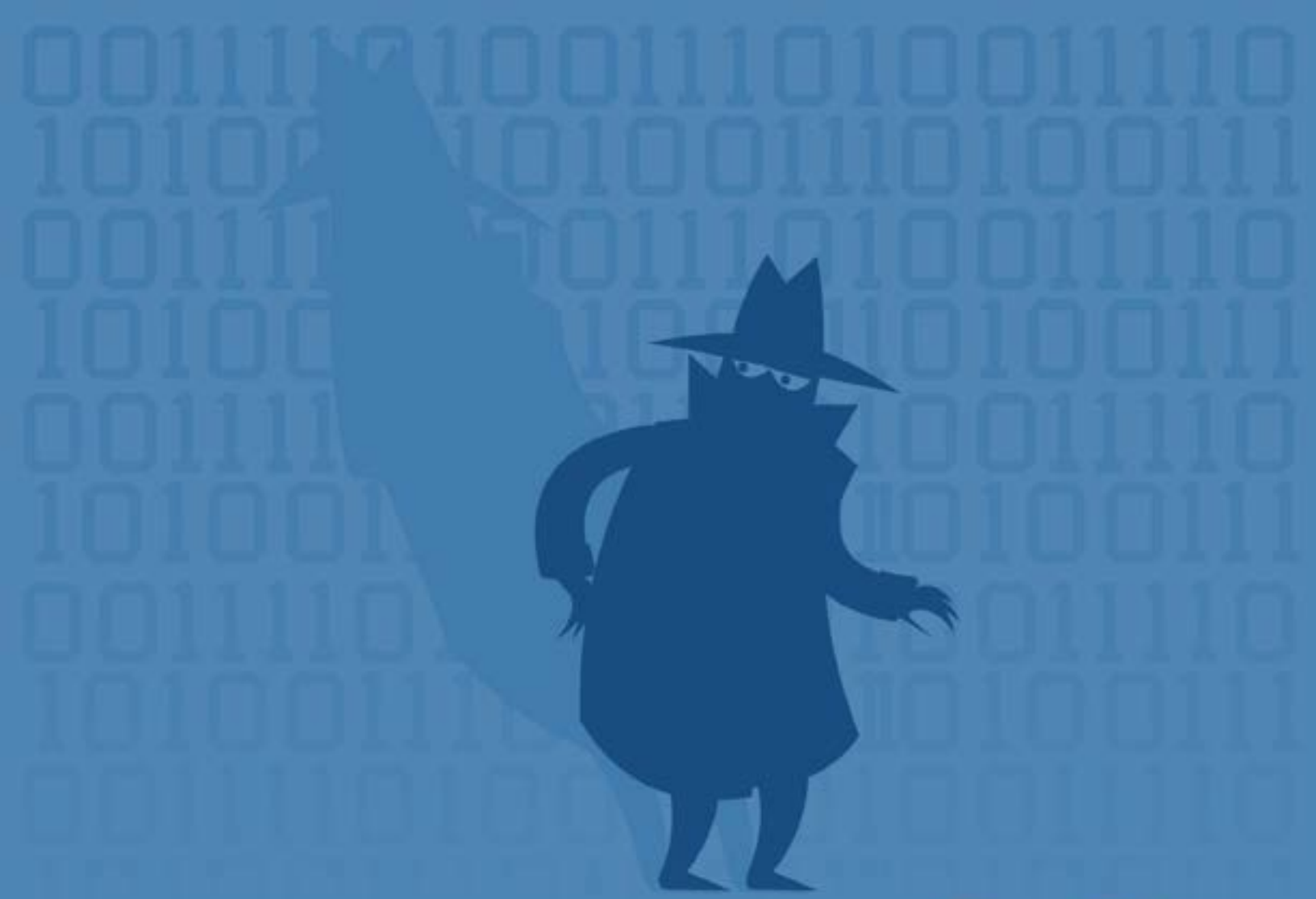

CSE
FEDERAL CREDIT UNION

Fraud Prevention Guide

CSE's goal with this Fraud Prevention Guide is to make our members aware of the types of common and not so common fraud that is out there. We want to make our members knowledgable of what to look for so they do not fall victim to fraud.

Table of Contents

Scenario:

- You meet your soul mate online - they live over seas and are everything you have ever been missing in your life. You message back and forth for months, but never meet or speak with this person over the phone.

- Soon enough, it is time to meet. But, something happens while they're traveling and they need your help! Of course the only help that they need is financially.

- They say they can give you some money up front to free up your credit limit on your credit card, and you give them the card information. They start using your credit card running up the bill. You then find out the payment they made is returned and now you owe even more on you credit card than before.

- You never meet this so called, soul mate.

In this scenario, people get burned because all along the person, is scamming you!

Now, you have credit card debt that will take you forever to pay off, and you're also without this person in your life...because the whole time they only wanted your money.

This is a new, but very effective scam for fraudsters to pull. Little did you know, that while they were making you feel special, they were also scamming 20 other people and never had any intention of ever being with you.

Scammers will often befriend you online only to eventually ask you for money or personal information.

If a person romances you online, but suddenly is in trouble and is in need of money...it's probably a scam!

Never share financial or personal information with anyone you don't know! Even if they seem trustworthy.

Hide ID-theft clues on Facebook. Things like your birthdate, high school alma mater, and your hometown. Facebook could reveal this information to potential hackers or scammers.

Scenario:

- You receive a letter with a check made out to you for a few thousand dollars.
- You don't know the person who sent this, but they request that you cash the check for them and send them back a specific dollar amount.
- For your trouble, you get to keep the remaining money for yourself.

If it seems too good to be true, it probably is! People don't send money for free. Generally, this scenario is a fraudster who likes to tug at your heart with a very sad story in the letter. This is one of the most common scams that people fall victim to.

In this situation, the check is a fraudulent check. It sounds good because you get money, but when that check comes back fraudulent, you, as the casher of the check, are liable to pay back the entire dollar amount of the check, plus fees.

Don't believe fake emails! If you get solicited with an odd email don't click it. Do research or call to see if it's legit.

Restrict file sharing that includes personal information on public WiFi

Keep your anti-virus software up to date.

Make sure your home WiFi is password protected.

Don't use public WiFi to make online purchases.

Consider encrypting personal files on your computer for extra security.

Back up your files in case there is a threat that you have been hacked by RANSOMWARE.

<u>What is Ransomware?</u>
A malicious software designed to block access to a computer system until a sum of money is paid.

Scenario:

- You receive a check or an email stating that you won a foreign lottery. All you need to do is go to a website and give them some personal information including bank account information, so they can send you your winnings!

Moral of this story – if you haven't played a foreign lottery, then you haven't won a foreign lottery! If it seems suspicious, then it should raise concerns...trash the letter.

Check links before you click!
Check the security of a site first if you think it may be suspicious.

Often scammers will send mail or emails stating you've won something for free. Even if you never entered for it.

When shopping online make sure the website is secure.
Look for <u>https</u> in the URL.

If your credit or debit card is lost or stolen, use your mobile app to turn your card on/off and contact the financial institution!

Your birthdate or last 4 of your social security number should not be used as your PIN numbers.

Never save your credit or debit card information on any website!

Change your statement settings to get e.statements to lessen the likelihood of a statement being intercepted in the mail.

Check your bank statements when you get them to ensure that all trasactions are yours!

Shred any documents with personal or financial information when you no longer need them.

Scenario:

- You receive a phone call from someone who claims that a loved one is in trouble.
- The caller knows this person's name, where they live and some other information.
- The only way to help this loved one is by sending some money – "right away"!
- You, concerned for this person don't bother to do any research on your own.
- You send them some money or give them your credit card information.
- When you check on that loved one, you find that they were never in any harm.
- You pull up your bank information only to see that you have fallen victim to fraud.

In this scenario, the fraudster is doing their best to create a sense of urgency. They know enough information about your loved one (that they could find on social media) to quickly build trust. Don't be afraid to check on your loved ones before you give out personal information to someone you don't know. Be diligent!

<u>Phishing:</u> is when scammers contact you in the form of an unsolicited email.

Many times, scammers will pretend to be IRS in order to get you to disclose your personal or financial information.

Make passwords unbreakable. Use a diverse mixture of upper & lowercase letters, numbers, & symbols.

Don't use the same password for every account. Diversify your passwords for all different accounts.

Change default settings. If you've never changed the username or password on an account, do that now!

Never save your usernames or passwords for any of your accounts on any website!

If you've been notified of any type of breach, be sure to change your passwords !

Check your credit report.
Make sure there aren't any discrepancies.
If there are, report them immediately!

Check on the kids.
A study showed that minors had their identity stolen 51 times more often than adults.
Source: Consumer Reports

Never forget rule #1
in fraud prevention..
If it sounds to good to be true,
it probably is...