Financial Wellness

Protect yourself from fraudsters & scammers

Here are ways you can protect yourself from some of the most common fraud schemes and scams. Remember that UNFCU representatives will never ask for your private account information, such as your PIN or password.

6-minute read

In brief

Fraudsters and scammers use a sense of urgency to make you believe that you must act fast. If a message looks unusual, take your time to review it carefully.

If an offer sounds too good to be true, it probably is.

Minimize the amount of personal information that you share online.

Call scams regarding erroneous charges on

merchant accounts

This scam starts with a direct phone call from fraudsters posing as representatives of a merchant such as PayPal or Amazon. They will claim that there were erroneous charges posted to your account. To reverse the charges, they will claim they need your account information. They may also request remote access to your computer and ask you to log in to Digital Banking. The remote access allows them to see your login credentials.

Tip: Do not disclose your account details or any personal information. If a merchant posts an erroneous charge, they do not need this information to reverse the charge.

Computer repair scams

You may receive a pop-up message on your computer advising that a virus has been found. The message will include a phone number for you to call to fix the problem. Alternately, you may receive a phone call from someone who claims to be tech support from a well-known computer company.

In either case, the individual will try to convince you that your computer is infected and needs immediate attention. They can be very persistent and can become abusive.

If they are able to convince you, they will ask for remote access to your computer. They will give instructions on how to provide the access. Once they obtain control of your computer, they can access all information on the computer. They can also download malicious software onto that computer.

As if that's not enough, they may ask for payment at the end of the call for fixing your computer! This way, they can collect your personal and account information, or a credit card number.

Tip: Do not respond to unsolicited phone calls or computer pop-ups asking you to

call a phone number. Hang up or close your browser.

Online friendship scams

Online scammers may try to engage you into an online friendship or other relationship. After establishing trust, they will email you to report a crisis in their life for which they need money immediately. They will ask you to lend them the money by sending a wire transfer or by purchasing pre-paid gift cards. After getting as much money as possible, they will disappear.

Tip: Do not lend money to someone you have never met in person and you only know online. This is inclusive of dating sites. Remember that gift cards are never an authorized type of payment, unless you are going shopping. If someone contacts you and requests payment in the form of pre-paid gift cards, it is most definitely fraudulent.

Email scams

Fake emails, also known as phishing emails, appear to be from a trusted source, such as your financial institution. They may even appear to be from the World Health Organization or Centers for Disease Control and Prevention. They may ask you to:

- Verify your personal or financial information
- Provide your login ID and password to a secure site
- Open an attachment or click on a link in the email. Once you take the requested action, the link or attachment automatically installs malicious software onto your computer.

Here is what you should look for in an email before taking any action:

- Many times, phishing emails will try to instill a sense of urgency. Fraudsters want

to make you believe you must act fast. Instead, take your time and scrutinize the email carefully.

If you do not see your name, be suspicious.

Even the slightest misspellings are a red flag.

Legitimate institutions do not send you unsolicited emails requesting that you verify personal information.

Unusual content or unexpected attachments should first be verified.

Tip: If you have reason to question the validity of an email, contact the sender by phone to validate the message.

Fake check scams

This con can take several forms. It may start as a result of an advertisement you posted online to sell an item. Or someone may contact you to say you are the winner of a lottery or the recipient of an inheritance. Either way, you are told to expect a check.

The fraudsters will send you what appears to be a very legitimate looking check. It may be in a larger amount than what was supposed to be sent. They will ask you to deposit the check and return a certain amount to them by money transfer. The check, however, is counterfeit. Any amount you transfer to them will be debited from your account before the check is returned unpaid.

Tip: If the offer is too good to be true, it probably is. Listen to your intuition. It is never appropriate to be asked to return money to a stranger after receiving a check from them. Do not send any money until the check has cleared.

Property scams

The internet has made it convenient to browse listings for apartment, housing, or

vacation home rentals. As a result, scammers post fake listings on legitimate rental websites. They may even create a fictitious website displaying photos, descriptions, pricing, and fake reviews. The fraudsters may advertise excessive amenities for substantially lower rates. They will ask for payment in advance via wire transfers to cover both the rental and security fees. Once the money is sent, the scammers disappear.

Tip: Be suspicious of rentals that are below the market rate. Always conduct extensive research to ensure the legitimacy of the property and the person with whom you are dealing.

Using social media

Facebook, Twitter, LinkedIn, and other social media sites are convenient ways to stay in contact with family and friends. They can also be an identity thief's best resource for locating information about their victims.

Tip: Set your online profiles and personal pages with adequate privacy and security settings. Also, try to minimize the amount of personal information you post online. Always be careful with whom you connect on any social networking site.

Fake investment scams

It begins with an online offer, most likely for an investment opportunity, where you can make quick profits. Fraudsters request your account information, where money will be deposited from other supposed investors. You are then asked by the fraudster to send most of the money to them. Unwittingly, you become part of a theft and money laundering scheme as the money being transferred is actually stolen. As a result, you could get into legal trouble for helping fraudsters move stolen money.

Tip: Only disclose your account information to sources that you have verified to be legitimate.

US Internal Revenue Service (IRS) scams

This scam starts with a direct phone call from fraudsters. They will claim that they are agents of the IRS or other law enforcement agencies. The fraudsters will state that you owe unpaid taxes and that there is possibly a warrant for your arrest. They may be abusive and will threaten arrest or deportation if the taxes are not paid immediately. Payment in the form of pre-paid gift cards is often the requirement.

Tip: The IRS will never make initial contact with a taxpayer by email or phone. They will also never make threats of arrest to obtain payment of US taxes.

Benefits of a credit freeze

A credit freeze restricts access to your US credit report. You should consider this option if you have a US social security number and are not applying for a loan. You can learn more about a credit freeze on the Federal Trade Commission website . If you place a credit freeze, you will need to lift it prior to applying for a loan.