August 2022

Oregon State Credit Union **difference**

Oregon State Credit Union

Build a strong password

Passwords or passphrases are your first line of defense against people who want to steal your money, your identity, your social media accounts and anything else they can get their digital hands on. Make your passwords and passphrases long and strong to protect your accounts and private information.

A passphrase is a phrase or sentence that is meaningful to you, but not to the bad guys. Passphrases are stronger than passwords because the tools hackers use to crack your passwords begin to lose effectiveness after 10 characters. A passphrase of 40 characters or more is a daunting challenge to hack. Don't use book titles, song lyrics or other publicly available information. Instead, use something very personal to you.

Build a strong password, continued on page 2 ➜

Be fraud aware

The best way to avoid fraud is to know how to recognize it. There are many kinds of fraud schemes, but most share certain telltale characteristics.

1. There's no time to wait

Many fraud schemes depend on speed. Scammers can't wait around for you to wise up to their tricks. This is especially true for scams that involve checks, money wires and pre-paid cards. If you receive a check from a stranger with instructions to deposit the check into your account and wire a portion to someone, don't do it. When you deposit a check, federal law requires that at least some portion of the funds is made available to you in one to five days, which may lull you into thinking the check is good. But the actual processing takes longer. It can take weeks before you know if the check is bad. Scammers will try to get you to act before the check bounces.

Other scams will try to frighten you into handing over money or personal information. They may claim you're delinquent on paying your taxes, or you may receive a text alert claiming there is an issue with your account. (Just click this link and confirm your account details.) Whatever the ruse, take time and don't act just because the pressure is on.

If you receive an email, text message or phone call from a stranger who pressures you to hand over money or information quickly, suspect fraud. Step back, take a breath and investigate their claims.

2. It feels personal

In addition to money, scammers want your personal information so they can steal your identity and sell it on the black market or use it to take out loans and credit cards. Be on the lookout for bad actors who may impersonate a legitimate business or familiar person to try to trick you into revealing your personal information or financial credentials. They may pretend to be your financial institution, online retailer, package delivery service, a friend or even a potential love interest.

Don't be fooled. Lotteries don't need your account numbers to direct deposit your "winnings." That love interest you met online (but who can't seem to meet up in person) doesn't need to know your mother's maiden name. The financial institution that issued your credit card already knows your CVV

Be fraud aware, continued on page 2 ➜

Be fraud aware, continued from page 1 ➜

number. And no one EVER needs to know your credit union account login and password.

Your credit union will never initiate a phone call, email or text to you and then ask for your account login and password. If you receive communication asking for this information, don't respond.

3. Trust your gut

Which brings us to point number 3: If it seems wrong, check it out.

Does the message contain misspelled words or grammar errors? Does it seem odd—not like the usual text your friend or co-worker would normally send? Is the request unusual?

Scammers are very good at putting you at ease, but it's hard to silence that voice deep in your gut that says, "This is odd." If you have any doubt about a phone call, email or text, do a final verification before you click on any links, open any attachments or respond with information. If it's from a friend, call them for confirmation. If it's from a company, call them to confirm the request. If the message is legitimate, there's no harm in verifying it before you act.

4. Suspect the unexpected

Be suspicious of any unexpected requests, links or attachments you may receive in person or by phone, email or text. Whether it's good news or bad, don't act on unexpected information until you have had time to validate the details.

If you receive an unexpected request to verify an account or personal information, an announcement that you've won a prize (just click here), or even an attached photo of your friend's new puppy, be suspicious. If you can, verify with the sender that the request, link or attachment is legitimate. If you can't verify, don't respond.

Build a strong password, continued from page 1 ➜

You can make your passphrases even stronger by adding numbers, spaces and special characters. Look for opportunities to substitute letters of the alphabet with characters or numbers. For instance, an "a" can be represented by the @ symbol.

The strongest passwords are randomly created by software called a password generator, but randomly created passwords can be difficult to remember. To help, you can manage all your passwords using a password manager. Some password managers include a password generator for the best of both worlds.

The most commonly used passwords are based on family names, hobbies or simple patterns. Avoid these kinds of passwords if you want to make your accounts as secure as possible.

The credit union difference

Social purpose; people helping people

Credit unions exist to serve their members' financial needs, not provide a profit to third-party investors. They know their credit union will be there for them in bad times, as well as good. The same people-first philosophy is at the heart of why credit unions and our employees get involved in the local community through charitable and other worthwhile causes.