September 2021

Oregon State Credit Union **difference**

Oregon State Credit Union

Five steps to protecting your digital home

More and more of our home devices – including thermostats, door locks, coffee machines, security cameras, baby monitors, appliances and smoke alarms – are now connected to the internet. This enables us to control our devices on our smartphones from anywhere. While convenient, these multiple connections to the internet pose a security risk that needs to be fixed to protect your increasingly digital home.

1. **Don't click and tell.** Limit the information you post on social media – from personal addresses to where you like to grab coffee. Criminals use this information to target you, your loved ones and your property both online and in the real world. Turn off location services that allow anyone to see where you are – and where you aren't – at any given time. Keep Social Security numbers, account numbers and passwords private, and never share your passwords with another person. Oregon State Credit Union will never call you to ask for your online banking password.
2. **Secure your Wi Fi network.** According to the United States Department of Homeland Security, your home s wireless router is the main way cybercriminals access all of your connected devices. Secure your Wi Fi network and your digital devices by changing the factory set

Five steps to protecting your digital home, continued on page 2 ➔

Shopping safely online

The internet offers convenience not available from other shopping outlets. You can search for items from multiple vendors, compare prices with a few mouse clicks and make purchases from your home. However, the internet is also convenient for cybercriminals, giving them many ways to access the personal and financial information of unsuspecting shoppers. Attackers who obtain this information may use it for their own financial gain, either by buying items themselves or by selling the information to someone else.

How do cybercriminals target online shoppers?

There are three common ways that criminals take advantage of online shoppers:

1. **Creating fraudulent websites and email messages –** Unlike traditional shopping, where you know that a store is actually the store it claims to be, cybercriminals can create malicious websites or email messages that look legitimate. Attackers may also misrepresent themselves as charities, especially after natural disasters or during holiday seasons. Criminals create these malicious sites and email messages to convince you to supply personal and financial information.

2. **Intercepting insecure transactions –** If a vendor does not use encryption, a cybercriminal may be able to intercept your information as it is being transmitted.
3. **Targeting vulnerable computers –** If you do not protect your computer from viruses or other malicious code, a criminal may be able to gain access to your computer and all the information on it.

How can you protect yourself?

- **Do business with reputable vendors –** Some cybercriminals may try to trick you by creating malicious websites that appear to be legitimate. Before giving any personal or financial information, make sure you are interacting with a vendor you know and trust.

Shopping safely online, continued on page 2 ➔

Shopping safely online, continued from page 1 ➔

- **Study the URL –** Check for spelling errors; some criminals will set up fake sites that are one letter off from the real site. If something seems off, avoid that site.

  A URL (Uniform Resource Locator) is a standard naming convention for addressing documents located on the internet. An example of a URL is https://www.oregonstatecu.com, which is the URL for Oregon State Credit Union.
- **Click on the padlock in the address bar –** A drop-down box will open that will provide security information about the site.
- **Use an online verification site –** If you're uncertain about a website, run the URL through an online verification site. URLVoid.com can give details about the site, and transparencyreport.google.com can tell you if a website is safe.
- **Don't click on links in an email –** Type the URL of the business into the search field, or use a search engine to find the business.
- **Make sure your information is being encrypted –** Look for a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted.
- **Be wary of emails requesting information –** Attackers may try to gather information by sending emails asking that you confirm purchase or account information. Legitimate businesses will not ask for this type of information through email. Oregon State Credit Union will never send you an email asking for your password.
- **Use a credit card –** You have fraud protection on all your Oregon State Credit Union Visa® credit and debit cards, but there is a difference. Using your credit card is like taking out a loan: If there is fraud, you aren't out any money. But your debit card draws money directly from your credit union accounts. Unauthorized charges could leave you without enough money for a few days while the fraud is confirmed and your account refunded. You can minimize potential damage by using a single, low-limit credit card to make all of your online purchases, like your Oregon State Credit Union Visa Value or Visa Rewards credit card.
- **Check your statements –** Keep a record of your purchases and copies of receipts and confirmation pages, and compare them to your credit and debit card statements. If you see something wrong, report it immediately.
- **Check privacy policies –** Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your personal information will be stored and used.

Five steps to protecting your digital home, continued from page 1 ➔

default password and username that come with your device.

3. **Double your login protection.** Set up multi factor authentication to make sure the only person who can get to your account is you. Use it for email, online banking, social media or any service that requires logging in.
4. **Protect what's connected.** Whether it s your computer, smartphone, game device or other network devices, make sure you are using the latest security software, web browser and operating systems. If you have the option to set up automatic updates, turn it on. And, if you re putting something into your device (like a USB), make sure your device s security software scans for viruses and malware. Finally, protect your devices with antivirus software, and be sure to frequently back up any data that cannot be replaced, such as photos and personal documents.
5. **Keep tabs on your apps.** Who doesn't love a good app? Your mobile device could be filled with apps running in the background or using permissions you never realized you approved gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and apply the "rule of least privilege" to delete what you don't need or no longer use. Say no to privilege requests that don't make sense. Only download apps from trusted vendors and sources.

We're hiring!
Are you looking for a rewarding career with a great company?
Check out our job openings at
oregonstatecu.com/careers.

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.

Visit **oregonstatecu.com**

Call 800-732-0173

Insured by NCUA

EQUAL HOUSING OPPORTUNITY