Don’t Fall Victim During the Season of Giving

For most of us, the holidays are full of giving and goodwill. But fraudsters use the season to take advantage of our generous spirit. They’re smart and getting harder to spot. Unfortunately, scams are common year-round, but we’re more likely to fall victim during a time when we’re busy, preoccupied, and even stressed out.

Here are a few scams you may see fraudsters attempt this holiday, and tips on how to protect yourself from becoming a victim:

Mail Scams. The higher volume of mail and shipments during the holiday season provides many avenues for scammers. Your deliveries can be easy targets. The packages sitting outside your house can be tempting for thieves, and porch pirates may steal them from your doorstep. Track your deliveries so you’ll know when they’re scheduled to arrive. You can also set up a different delivery address to your workplace or even with a neighbor who is home during the day. This will ensure your packages arrive and remain safe.

And speaking of deliveries, shipping services like UPS and FedEx often provide us with tracking and status updates via email. Fraudsters know this and will send phishing emails pretending to be from one of these companies. This is an attempt to lure you to phony webpages and get you to share your personal information. Look closely at delivery notifications and email updates before you click on any links or provide sensitive information. And remember, UPS and FedEx won’t ask for your personal information via email.

Cloned Websites. As mentioned above, scammers will create phony webpages, cloned from the legitimate websites of companies that you know and trust. They may send you a sale coupon or link that, when clicked, takes you to a fake webpage that looks just like the real thing. These criminals aren't necessarily looking for your credit card information. The cloned site might simply ask you to log in and then redirect you to the real website. But once a thief has your login credentials, they can access your account to make unauthorized purchases.

Pay attention to the URL addresses of webpages. Fake URLs will look similar to the legitimate site they're replicating but aren't exactly the same. They may use special characters that resemble letters or add numbers to the end of a retailer’s name. For example, a scammer may create a cloned URL of www.am@zon123.com to make you think you’re really visiting www.amazon.com.

Pro tip: Shop and place your orders from a retailer’s app instead of their website online. Most major stores have them, and they offer a more secure way to shop from home.

Charity Scams. Criminals often take advantage of our generous nature during the holidays. They may send emails or make phone calls posing as representatives from charitable organizations. Spoofing technology will make it look like the email or call is coming directly from the actual charity.

Before giving out any personal information like credit card or checking account numbers, take a look at the organization's website to find a legitimate phone number or online donation option. Make sure to go directly to the charity’s site using an external browser; don’t click any links found within an email

soliciting your donation. If you're ready to donate but remain unsure about the authenticity of a charitable organization, you can look it up online using Charity Navigator or CharityWatch.

As a final reminder, legitimate retailers, companies, banks and credit unions, including Emerald Credit Union, will never contact you via phone call, email, or text message requesting personal identification or account information. This includes Social Security numbers, account numbers and passwords, and any other personal confidential information.