The holiday season is upon us, and it is prime time for those nefarious holiday scammers to attempt to take advantage of those in the giving spirit. Be it donating to a cause, buying presents, or receiving one of the many scam calls trying to get your personally identifiable information (PII) to use for their profit.

Be on the lookout for some of the scams that ramp up during this time of year:

- Online Shopping Scams: Deals offered through phishing e-mails or advertisements.
- Social Media Scams: Social media sites offer holiday promotions, vouchers, or gift cards. You should avoid completing surveys intended to gather and compromise your personal information.
- Gift Card Scams: A spoofed e-mail, call, or text asking you to purchase multiple gift cards for personal or business reasons.
- Charity Scams: Fake charities set up to profit from persons who believe they are donating to a legitimate organization. Many charities are legitimate, but some are not, and it is essential to research and verify a charity's legitimacy before giving.
- Smartphone App Scams: Mobile apps designed as free games that steal personal information.

Be proactive and attentive when you are surfing the web or checking your email for deals at your favorite stores:

- Do not click on emails/texts from unknown senders.
- Be cautious about purchases or services requiring payment with gift cards, cryptocurrency, or wire transfers.
- Make sure all financial accounts have strong passwords or passphrases.
- Never make purchases over public Wi-Fi.
- Purchase gift cards directly from a trusted merchant.
- Ensure the anti-virus/malware software is up to date on your computer and block pop-up windows.

Another way these holiday scammers can ruin your day is by identity theft. Identity theft is when someone uses your personal or financial information without your permission. They can get your information by:

- Going through trash cans and stealing bills and documents that have sensitive data,
- Misuse the name of a legitimate business and call or send emails that trick you into revealing personal information,
- Pretend to offer you a job, a loan, or an apartment and ask you to transmit personal data to "qualify."

- They can do it the old-fashioned way by stealing your wallet, purse, backpack, or mail and removing your credit cards, driver's license, passport, health insurance card, and other items that show PII.

They might steal your name and address, credit card or bank account numbers, Social Security numbers, or medical insurance account numbers. And they could use them to:

- Buy things with your credit cards
- Get new credit cards in your name
- Open a phone, electricity, or gas account in your name
- Steal your tax refund
- Use your health insurance to get medical care
- Pretend to be you if they are arrested

If your PII is lost or exposed, the following steps can help against fraud:

- Check your credit reports at www.annualcreditreport.com (Experian, TransUnion, Equifax).
- Consider placing a credit freeze or fraud alert on your credit report.
- If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- Monitor all bank, credit card, and insurance statements for fraudulent transactions. If you suspect or discover fraudulent activity, contact your bank or insurance provider to report the crime to law enforcement.

Don't let these scammers and thieves ruin your holiday cheer. Be aware of what methods these Scrooges use to tap into your holiday hustle and safeguard your information.