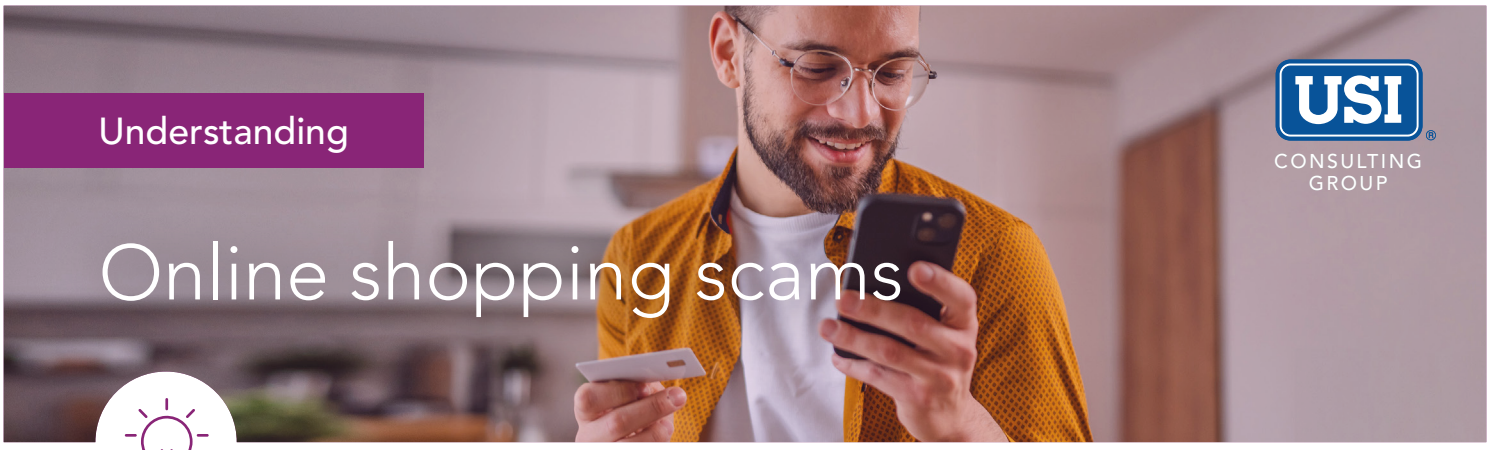

Understanding

Online shopping scams

Cybercrime is an unfortunate fact of modern life. Criminals are constantly on the lookout for ways to get their hands on information that they can monetize through fraud or outright theft. Their scams range from the simple to those that are extremely complex. Online shopping scams are becoming more frequent and are ensnaring larger numbers of victims. These scams work in a variety of ways, but savvy consumers can take countermeasures to protect themselves from becoming a victim.

Social media can be a gateway to cyber scams

The Federal Trade Commission has noted that a significant number of fraud losses reported by consumers in the 18-29 age group originate on a social media site. Consumers in this age group frequently respond to pop-up ads and often purchase goods advertised on such ads. Others buy from popular online marketplaces.

Unfortunately, not all sellers are who they claim to be and many buyers end up being scammed. Sometimes the scam is straightforward -- the "seller" takes the money and doesn't deliver the promised goods. Other fraudsters deliver a knock-off, a counterfeit, or something that bears little resemblance to what the buyer was expecting.

However, a larger concern for buyers should be the possibility that that they are dealing with scammers whose primary focus is on stealing data. Some will sell consumers' credit card numbers and their names and addresses to other criminals. Others will use the credit cards of consumers to buy gift cards and cryptocurrencies for themselves.

Consumers who use debit cards in their online transactions are also at risk. Bank debit card issuers will typically reimburse customers who suffer losses due to cybercrime – but not always. And when banks do make their customers whole again, it can be a time-consuming process.

Take steps to protect yourself

You can take several simple, common-sense precautions to minimize the risk that you will be scammed while shopping online:

Be skeptical of great deals

The saying "buyer beware" still holds true as much today as ever. If a deal seems too good to be true, it probably isn't true. Think carefully before you press the "Buy now" button and send personal financial information to an unknown destination.

(Continued)

Click carefully

Cybercriminals use common phishing techniques such as free offers, spam emails, and online quizzes to trick you into sharing personal or sensitive information. The safest way to protect yourself is to not click on unknown or suspicious emails.

Shop with caution

Criminals create copycat websites that mimic those of legitimate retailers. Only shop online when you can ensure that the website's address starts with "https" instead of just http. Check also that there is a padlock icon in the URL to ensure that the site is secure and uses encryption to scramble your data. Frequent misspellings of common words and incorrect grammar are also red flags that can identify a copycat website.

Do not respond directly to ads

Do not respond directly to a pop-up ad. If you are interested in what's being advertised, open up a new page and go directly to the advertiser's website. Even then, before you buy anything, look for and check out ways to contact the business directly and review the business's return policy.

Read customer reviews

Google the company you are interested in and read customer reviews. There are certain websites that rate businesses based on customer feedback. These can be very helpful.

If you have questions about your workplace retirement plan, please contact your Human Resources department or your retirement plan provider's customer service center.

USI CONSULTING GROUP