Cybersecurity Awareness Month: 3 Super Scary Scams to Watch Out For

Don’t let a Halloween scam spook you! Stay a step ahead of those cyber crooks by looking out for these four scams this season.

1. The shipping scam

The internet is brimming with Halloween-themed stores in the months leading up to Oct. 31. Lots of these retailers offer an impressive selection of costumes, accessories and decorations at great prices.

Unfortunately, though, some of the retailers that own such sites will never deliver the ordered goods. That’s because, though the company may exist, and will appear legit, at the end of the day there was never a real intent to ship the item(s). The delivery date may be postponed until after Halloween, or the order might get canceled without notification. Sometimes, the shopper will receive the promised package on time – only the package is empty!

Before placing an order with a seasonal store, look for the company’s physical address and phone number. Check what the Better Business Bureau (BBB) has to say about it and look for information about return and refund policies in case things go south. Finally, as always, be careful about sharing

your credit card information with an unsecure site. Look for the lock icon near the URL and the “s” after the “http” in the web address; both indicate you’re on a secure site.

It’s also a good idea to order your costumes and décor in September. This way, you’ll have time on your side if you need to return a costume or a product that didn’t turn out as expected. You’re also less likely to purchase goods from iffy retailers and vendors you don’t recognize when you aren’t pressed for time. Finally, you won’t be forced to spend a ton of money on last-minute shipping costs when you make your purchase early in the season.

2. The fraudulent offer

In this scam, a bogus company advertises online a “Super Special Deal” for “Today Only” offer, or something similar. It will offer amazing Halloween goods for prices that are too good to be true and lure lots of unsuspecting customers into the trap. Unfortunately, the company is bogus and the offer doesn’t actually exist. If you purchase the advertised product, you’ll never see the product – or your money.

As with all potential scams, check out a company’s authenticity and a website’s security before purchasing.

3. The bogus purchase scam

In this scenario, scammers try to convince you that you ordered something you have no recollection of purchasing just to get you to share your personal information. Once the scammers have this data, they’ll do anything from emptying your accounts to taking out loans in your name or committing full-blown identity theft.

If you receive any emails, phone calls or text messages asking you about a costume you never ordered or a ticket you never purchased, do not engage with the sender or caller. Delete the emails or flag them as spam. Also, block the contact from calling or texting you again. With any luck, the scammer will get the message that you’re not an easy target and leave you alone.