The CYBER GURU

Ed Kipp
Cybersecurity

A few years back, I worked as a seasonal employee doing phone and web order support for a company called Deckers Outdoors. Deckers owned several shoe companies – Teva, Ahnu, Hoka One One, and most famously, Ugg Australia. I learned more than anyone ever needs to about sheepskin boots, but I also was made aware of how prevalent counterfeiters and scammers are when it comes specifically to Ugg boots.

All scammers need to do is go to the official Ugg Australia website, find images that they can use, and save them to their computer. Then they create a webpage with the photos and logos, register the URL, and start taking orders. They collect the money and send an order confirmation. While the customer is waiting, they have all the personal information needed to make fraudulent charges on their credit cards. Maybe an order with counterfeit boots is on the way, but most scammers don't even waste their time sending anything that can be traced back to them. When the customer does not get their order, they look for any customer support number, and eventually they call the Deckers call center. It's heartbreaking taking those calls, people who tried to get something nice for someone they care about, only to find they were deceived and likely have fraudulent charges on their cards. We could give them resources to try and help, but many times their cards were still charged.

Deckers spends millions of dollars trying to take down fraudulent websites, but it is very easy for a scammer to keep a website up for a couple days, have some search engine optimization display their page when “cheap uggs” is searched, and then rake in the cash (and record and resell credit card numbers). It's impossible for Deckers to stay ahead of the websites, but the one thing that they do is to be up front and honest about discounts - you will never see Ugg boots on sale for 60 percent off. It just won't happen. There is a feature on the Ugg website that allows you to put in the URL where you see a deal and see if they are authorized retailers.

It is important to remember to be wary during the gift-giving season, and understand that some deals truly are too good to be true. Many other retailers will verify if a website is legitimate, but like phishing attempts, criminals are counting on someone doing a quick search and trying to get the cheap instant gratification. Unfortunately, when this happens, usually the person making the order doesn't find out until it is too late, and their card has been charged multiple times for boots they never receive. Or maybe they do receive a package of skunkskin boots or poorly glued imitation sheepskin. And that doesn't make for a happy holiday.