



HOLIDAY SCAMS

BY JAY BORDEN

This is the season where everyone is shopping. The hope is to give gifts that are meaningful and wanted. With money being so tight people want to get good gifts at good prices. Time is also in short supply, so they look for good prices and ease of shopping. Very understandable.

Cybercriminals know that and have several scams designed to fool you and capture your money, credit card information, identity, and more.

The FBI has issued warnings to help people stay safe during this holiday shopping season. The warnings are really good for all year but especially when people typically buy more and are rushed for time.

No matter how rushed you are, no matter how much you have to get done, remember to take time to be careful. It will be far less time than it will take to try to reclaim your identity or get your card company to issue a new card and refund what was stolen.

What to look for?

If you have never heard of the company or the website, investigate it thoroughly by looking for reviews in multiple places. But not on their site. Those are too easy to fake. Remember reviews even on other sites can be bought or faked these days. So still be careful. That is why we recommend looking at multiple sites for reviews and to look at multiple reviews on each site. Read them, don't just skim. If they all sound similar, they're fake.

HOLIDAY SCAMS

CONTINUED

If there are no reviews or only poor ones for a site, don't buy. No matter how attractive the price. It is doubtful you will get the product at all. But your information will be taken and used by the cybercriminals for their benefit.

Cybercriminals are good at creating fake sites that look enough like well-known companies that it is easy to be fooled.

Examine the website address, does it begin with https? The "s" is very important. It stands for secure. Without it, the website is not secure, and your information can be stolen easily. You should also see a padlock to the left of the website address. This is another indication it is secure. Both the padlock and the "s" are necessary. Look at the rest of the web address, is it really the site you wanted? If not, leave immediately.

If a site says they are an authorized representative for a company, investigate that on the company's site. Or call the company and ask. Never click a link in the email from the person you suspect. It is easy to claim you are an authorized representative. Many companies don't have authorized representatives. Ask yourself, why would a company selling in my country need authorized reps or agents? The answer is they don't.

Auction sites are a popular alternative to stores. But be careful. You don't know the person you are buying from. Look on the auction site for reviews and number of completed transactions. If there are no reviews or a very small number of completed transactions, that is a red flag. It will be very difficult to get your money back if you buy from a fraudulent seller who doesn't send the item. Another red flag is if the seller claims to be from your country but says they are away now and can't meet, or they provide a foreign address or phone number. A plausible reason may be given such as family emergency, but don't trust it.

If the website looks legitimate but specifies an unusual shipping method, be wary. If the site or person says they can save you money by bypassing customs, it is illegal.

Sellers specifying a direct transfer of funds is another red flag. Always use a credit card. Then you have the power of the card issuer behind you. That doesn't mean they will always refund the money, but it is safer than a direct transfer of funds.

HOLIDAY SCAMS

CONTINUED

Never buy from a site or from someone who asks you to use prepaid gift cards for the transaction. These are always scams. The gift card number and pin that you send will be used by the scammer for their own purchases.

Even if the site looks okay, if the price is much lower than what you see in other places it is most probably a scam.

Remember the old adage, if it is too good to be true, it probably is.

Be very careful during the holiday season and at all times. Don't let it be a good season for cybercriminals by giving them a present of your money or your identity.

We wish you a very happy and cyber safe holiday season.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.