



Watch Out for Holiday Shopping Scams



Holiday shopping is upon us.

Those looking for a little retail therapy, might also find themselves becoming victims of fraud. Here are the top holiday shopping scams you need to watch out for.

#1 Online Shopping Scams

If a deal seems too good to be true, it probably is.



Watch out for fictitious retail sites spoofing real sites or for completely fabricated retail brands. Double check the domain name and look out for spelling errors or non-.com or HTTPS URLs. Also, watch out for deals that are too good to be true.

For example, if a luxury item is selling at an unreasonably low price, it might be a fraudulent retailer phishing for payment information.

#2 Charity Rip-Offs

It's the season for giving – not giving away.



Unfortunately, fraudsters use the holidays to play off of our charitable spirit. Through email, text and phone calls, fraudsters will pressure victims into check, cash or money order contributions.

If you're thinking about charitable giving this year, give to an organization you know and trust.

#3 Holiday E-Card Scams

Getting 'Seasons greetings' from strangers?



Watch for phishing scams -- an email-based fraud tactic that leverages malware or social engineering to get victims to pay. Don't open emails if you don't recognize the sender.

Further, don't click on any links if the email looks suspicious – this might inadvertently install malicious software on your computer, giving fraudsters access.

#4 Don't Overshare

Rule of thumb for staying safe online: Do not overshare.



That includes posting pictures that accidentally have your credit card or driver's license in the background, or giving an app or website an inordinate amount of personal information.

Always bring a healthy amount of skepticism when transacting online.



Happy Holidays from



Advanced
Fraud SolutionsSM

