

Holiday Headaches

And How To Avoid Being Scammed This Holiday Shopping Season

What puts criminals and scammers in the holiday spirit?

Poor security practices, of course! For many, the holiday season ushers in positive spirits, selflessness, and generosity. But it also brings tidings of scammers who seek to use your good spirits against you. Social Engineering 101 says leverage emotions to get to the heart of victims. And there's no better time of year to do just that! So, as you're out shopping, giving, volunteering, or whatever your traditions are, keep your guard up, and spread the news that criminals and scammers get into the spirit, too.

Safety Checklist (Check It Twice)

Swipe safely.

If possible, avoid using debit cards to make purchases. Opt for credit cards instead. Most credit card companies offer fraud protection that covers any fraudulent charges should your card be lost or stolen. If you must get cash from an ATM, choose one that's physically inside a bank and inspect machines thoroughly for card skimmers.

Joining the crowds?

Some deals get marketed as "only available in stores" and might draw massive crowds as a result. If you join them, use a healthy dose of situational awareness. **Keep an eye on your things. Know where the exits are. And be kind to those around you!**

Shopping from the house?

Cyber Monday and other holiday-related online deals provide great discounts with the convenience of shopping in your pajamas. But they're also convenient for cybercriminals who set up bogus websites to steal your info or sell inferior products. **Stick to recognizable websites, and always verify the URL before entering any personal info (look for the green padlock and HTTPS).**

Find a great deal?

As cliché as this may be, if something looks too good to be true, then it's likely a scam. Reputable sellers won't offer super expensive computers and electronics for pennies on the dollar. **Use common sense!** And avoid giving out personal details in order to secure discounts or enter drawings for free prizes. These can sometimes be fraudulent attempts to steal info.

Receive an unsolicited offer?

Beware of any offers that you receive via email or text which come from merchants you don't recognize or just look *spammy*. The offer could be real. Or it could be a phishing attack. **Always think before you click!**

© The Security Awareness Company, LLC

