Beware of These Six Sneaky Holiday Phishing Scams

Fraud Won’t Stop After the Holidays

It always happens this time of year, an influx of holiday related scams circulating the interwebs. Scams don't wait for the holidays, but scammers do take advantage of the increased shopping and distraction when things get busy to take your money and personal information. Jon French, security analyst at business security solutions provider AppRiver, warns of six holiday threats that you and your customers/members should watch out for.

Look Out for Fake Purchase Invoices

With holiday shopping starting to ramp up and the daily deluge of holiday discounts in your inbox, it can be confusing to remember which online stores you actually purchased items from. This creates a vector where attackers can be more successful in attacks utilizing tricks such as fake purchase receipts. An unexpected receipt from Amazon or Wal-Mart during most of the year would hopefully raise some red flags for most users, but during the prime time for shopping for the holidays, users will likely be more susceptible to take the bait and click on a malicious link. Victims could find themselves installing malware or landing on a phishing page if they aren’t cautious.

Shipping Status Malware Messages

Along the same lines as fake email receipt messages, fake shipping notifications usually increase each year around the holidays. Oh the heels of cyber Monday and the bustle of online holiday shopping, consumers again might be more likely to click something they wouldn’t normally click. If you just placed an order that shipped via UPS, and then you get a zipped virus with the vague wording about your recent order being delayed, you may be more likely to click it.

Be Cautious of Email Deals

Not all email flyers and sales are going to be legitimate this shopping season. While communications from stores where you have a previous relationship

could be generally assumed to be OK and legitimate, exercise caution when receiving unexpected deals or product promotions from stores or sellers you have never dealt with. There will be people trying to take advantage of buyers where the victim could be subject to phishing tactics or just stolen money for an order that will never come in.

Take Care When Looking at Links and URLs

Phishing websites are around all year, but sometimes the busyness of the season and the generous spirit of the season can be cause for consumers to let their guard down and fall victim to phishing attempts. Hovering over links in webpages and emails as well as taking that extra second to just look at the address bar and see what site you're really being directed to can save you from falling for a phishing page.

Keep an Eye on Your Accounts

Some people may be spending money on whatever catches their eye, and others may be planning every purchase out. Regardless, holiday shoppers should keep an eye on their accounts and verify their accounts are only being debited for purchases actually made. It would only take one store you shop at being compromised to give criminals the chance to drain your bank account, whether it be via a card scanner at a gas pump, POS malware at a retailer store or an online store with lax web security.

Watch for Fake Surveys

Emails promising some sort of money or gift card in exchange for completing a survey can end up being a scam. Often the surveys are very short and generic, but at the end they may ask for some personal information. This can be what the attackers are really after. By gathering this information, they can use it to further a more advanced phishing attack. Some may even directly ask you for account details or credit card information, while promising you that you won't lose any money.

Source: PCWorld.com