Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 214

ACG-CSB 081621214

Reference Number ACG-CSB 081621214

HOW TO AVOID ONLINE SHOPPING SCAM

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as **"Restricted"** pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

While many online sellers are legitimate, unfortunately scammers can use the anonymous nature of the internet to rip off unsuspecting shoppers.

Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores. They may use sophisticated designs and layouts, possibly stolen logos, and even a domain name similar to an authentic retailer.

Many of these websites offer luxury items such as popular brands of clothing, jewelry and electronics at very low prices. Sometimes you will receive the item you paid for but they will be fake, other times you will receive nothing at all.

The biggest tip-off that a retail website is a scam is the method of payment. Scammers will often ask you to pay using a money order, pre-loaded money card, or wire transfer, but if you send your money this way, it's unlikely you will see it again or receive your purchased item.

A newer version of online shopping scams involves the use of social media platforms to set up fake online stores. They open the store for a short time, often selling fake branded clothing or jewelry. After making a number of sales, the stores disappear. They also use social media to advertise their fake website, so do not trust a site just because you have seen it advertised or shared on social media. The best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing.

The typical shopping scam starts with a bogus website, mobile app or social media ad. Some faux e-stores are invented from whole cloth, but many mimic trusted retailers, with familiar logos and slogans and a URL that's easily mistaken for the real thing. They offer popular items at a fraction of the usual cost and promise perks like free shipping and overnight delivery, exploiting the premium online shoppers put on price and speed.

And your losses might not stop there: Scammers may seed phony sites, apps, or links in pop-up ads and email coupons with malware that infects your device and harvests personal information for use in identity theft.

Not surprisingly, these frauds flourish during the holiday season. A November 2020 AARP survey on holiday shopping found that while 72 percent of U.S. consumers are concerned about the security of their personal and financial information when buying something online, only 15 percent could correctly answer at least 7 of 10 true/false questions about safe shopping practices. You need not forgo the ease and endless selection of online shopping, but take precautions to make sure you get what you pay for.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of **ONLINE SHOPPING SCAM:**

- Do use trusted sites rather than shopping with a search engine. Scammers can game search results to lead you astray.
- Do comparison shop. Check prices from multiple retailers to help determine if a deal you've seen really is too good to be true.
- Do research an unfamiliar product or brand. Search for its name with terms like "scam" or "complaint," and look for reviews.
- Do check that phone numbers and addresses on store sites are genuine, so you can contact the seller in case of problems.
- Do carefully read delivery, exchange, refund and privacy policies. If they are vague or nonexistent, take your business elsewhere.
- Do look twice at URLs and app names. Misplaced or transposed letters are a scam giveaway but easy to miss.
- Do pay by credit card. Liability for fraudulent charges on credit cards is generally limited to $50, and some providers offer 100 percent purchase protection. Paying by debit card does not off offer such safeguards.

For additional information, please refer to the following websites:

- https://www.aarp.org/money/scams-fraud/info-2019/online-shopping.htmla
- https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Online-Shopping-Scams

POINT OF CONTACT

Please contact **PMAJ ROVELITA ROBIÑOS AGLIPAY** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723 0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.