



'Tis the season for cybersecurity!

DECEMBER 2020

'Twas the night before the spending grand slam,
the fraduster was laughing as he plotted his scam.
If you are too busy to check the clues of a phish,
you will grant the criminal his holiday wish.

Beware of his mischievous ploy,
his goal is to steal your holiday joy!
As a target on the cyberthief's radar,
use caution this season and be a security star!

Take action to avoid **three** common holiday scams:



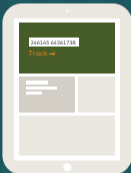
SHIPPING EMAIL NOTIFICATIONS

Cybercriminals may send a phishing email that appeals to your emotion regarding the status of your package and lures you to immediate action by clicking on a link.

Security Star Action



Do not click the link.



Visit the shipping company's website to track the package using the tracking number,



or call the merchant you made the purchase with to validate shipping detail.



FAKE CHARITY

Cybercriminals appeal to your goodwill this holiday season to make a donation to a charitable cause through a vishing phone call or sending you a phishing email or smishing text message.

Security Star Action



Never provide your banking detail or credit card number to someone who calls, texts or emails you.

Use a charity checker such as



[https:// www.charitynavigator.org/](https://www.charitynavigator.org/)

to validate the legitimacy of a charity before you donate.



FAKE SHOPPING WEBSITE

Cybercriminals create fake shopping websites that may "look like" a familiar retailer's site. They may email you a link for a special offer that routes you to the fake site in an attempt to obtain your login credentials and credit card details.

Security Star Action



Do not click the link.



[https:// www.amazon.com](https://www.amazon.com)



[http:// www.arnazon.com](http://www.arnazon.com)



Review the domain name/URL address to ensure there are no additional letters, numbers or characters that trick your eye into thinking you are visiting a legitimate site. Example: amazon.com (legitimate) vs. arnazon.com (fake).

Search online for the offer or site vs. clicking the link in the email.

Use a website checker such as <https://www.urlvoid.com/> to check the legitimacy of a website.

Take notice and back out if your browser or system displays a "not secure" message when you visit the site.



[https:// www.urlvoid.com/](https://www.urlvoid.com/)

