Welcome to the December Security Awareness Update

Theme: Online Shopping

Online Shoppers Beware
Online shopping fraud represents over two thirds (65%) of consumer fraud reports and has cost over $39 million during the first half of 2020. Do your research before buying and look for tips for a safe shopping experience.”

The online shopping landscape, while convenient, is filled with opportunity for the criminal to take advantage. They do this by intercepting unsecure financial transactions, targeting unsecure computers, or using social engineering tactics on shoppers. When trying to navigate the online mall, here are some warning signs:

Fake offers and discounts
- Bargain basement prices on popular items (check discounts over 55%)
- ‘Once in a lifetime’ offers on top brands (Tiffany jewelry, Burberry purses or Timberland boots)
- Special bonus perks like free or overnight shipping
- Special coupons or discount codes that require your personal information

Fake websites, mobile apps or social media ads
- Shortened URLs or URLs with extraneous words or character
- New websites created within the last six months or so
- Unusual Domains instead of .com, .net or .ca (example: .app, .bargain)
- Fake e-stories or ratings or bogus contact information

Also watch for:
- Random requests for your personal or financial information, give only what is required
- Requests to click for your order confirmation or to track a lost package
- Requests for remote access to your computer for any reason
- Requests to send money via PayPal, prepaid debit cards, gift cards or wire transfers, use credit cards as there is fraud protection built in

Online shopping has been very lucrative for criminals, the US Federal Trade Commission has received over 26,000 online shopping fraud reports in only the first 6 months of the year.

Here are some ways to protect yourself:
- Check that the website is encrypted (has a lock or https:// in the URL address)
- Check the Whois Public Internet Directory for the retailer’s domain registration info
- Check the company’s history on the Better Business Bureau website
- Check for reviews and complaints on other websites
- Check the ‘Contact’ information to ensure it’s valid (be wary of ‘free’ email addresses, i.e.: Gmail)
- Check the delivery, exchange, refund and privacy policies. If they are vague or nonexistent, move on

- Check your financial records and orders regularly, be aware of your purchases and charges

As our shopping world and everything else becomes more complicated, and the criminals become more sophisticated, the old adage still rings true – 'Buyer Beware'."

Information and Resources

NEW - 5 Ways to Spot a Phishing Email Video
https://www.youtube.com/watch?v=NZwkymDykUY
NEW – Cyber Incidents 101 - 3 Reasons Incidents Occur
https://www.youtube.com/watch?v=_gqqLHnuKYM
Consumer Protection BC - Our Top 5 Tips for Online Shopping
https://www.consumerprotectionbc.ca/2015/11/our-top-5-tips-for-online-shopping/
Cyber Security Alliance – Online Shopping
https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/
Get Cyber Safe – Secure Your Accounts
https://www.getcybersafe.gc.ca/en/secure-your-accounts
Better Business Bureau – Smart Shopping Online
https://www.bbb.org/article/tips/14040-bbb-tip-smart-shopping-online

FTC – Shopping Online
https://www.consumer.ftc.gov/articles/0020-shopping-online
AARP – Online Shopping Scams
https://www.aarp.org/money/scams-fraud/info-2019/online-shopping.html
IC3 Alert - FBI Reports Increase in Online Shopping Scams
https://www.ic3.gov/Media/Y2020/PSA200803
CISA - Holiday Online Shopping
https://www.cisa.gov/shop-safely