Volume 10 | Issue 5

BCSI Investigations Inc.

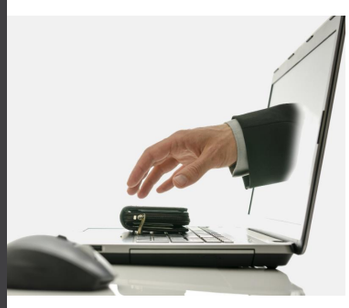
THE INVESTIGATOR

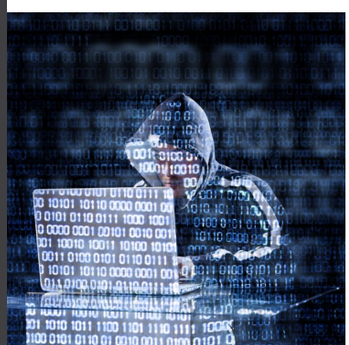
About Us

Since 2000, BCSI Investigations Inc. has performed thousands of successful investigations. Our integrated team of investigators and support services ensure that the investigations are conducted in a timely fashion with leading edge techniques.

BCSI Investigations Inc. is considered the platinum standard of the industry based on the quality and the wide spectrum of its services as well as the expertise of the investigators.

Visit our Website





Staying Safe Online this Holiday Season
Part 1: Phishing Emails

With the holiday season gearing up, many of us will be turning to online shopping to finish up our list to avoid busy shopping centres during the pandemic. Statistics Canada has reported from February to May 2020, total retail sales fell 17.9%. However, retail e-commerce sales nearly doubled (+99.3%). Scams related to online purchases, already on the rise in 2019, spiked further following the start of the COVID-19 pandemic, according to new research by the Better Business Bureau. A staggering 80.5 percent of consumers reporting online purchase scams in 2020 lost money.

One of the most popular scams used by fraudsters is phishing emails. A cybercriminal targets several email addresses with a message containing a malicious link often attached to a fake website in a typical phishing campaign. Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores; this is called “spoofing.” They may use sophisticated designs and layouts, even stolen logos and domain names. Many of these emails will advertise items like clothing and electronics for an extremely low price, making it hard to resist. But please do!

How to spot a phishing email:

- Check for spelling mistakes both in the body of the email and in the domain name and sender’s email address. One typical red flag is that the email domain doesn’t match the organization that the sender claims they are emailing on behalf of.
- Read through the email, and if it is poorly written, it is probably a phishing attempt.
- Hover over the embedded link, and you can usually see the real hyperlink. If the hyperlinked address is not the same as what appears in the email or looks suspicious, it’s probably a phishing attempt.

How to protect yourself:

- Invest in security software on your computer and update your mobile phone software regularly.
- People are urged to only buy from established retailers, check reviews of the seller, and be wary of offers that seem too good to be true.
- An easy check if a deal is legitimate is simply opening a new browser and looking up the company’s legitimate website. You can then check if the discount offered is a real one.
- Buy local! With the COVID-19 pandemic wreaking havoc on our economy, buying local over the holiday season will benefit both yourself and the community, all while preventing fraudsters from stealing your money.

If you or someone you know has been a victim of a phishing scam or is worried about their online safety this holiday season, please contact BCSI at 604-922-6572 or visit our website at www.picanada.ca.

Contact Us

With over 20 years of experience in investigations, BCSI Investigations Inc. is the platinum standard for private investigations. Contact us at 604-922-6572 or visit our website at www.picanada.ca to learn more.