

DATARIISK

MAGAZINE



HOLIDAY EDITION

FBI's Cyber Most Wanted
Criminals Spending The Holidays On The Run

Deceptive Ecommerce
Need to know: Spotting Dark Patterns

Cybersafety Tips
Freebies to See You Through 2024

Issue No. 2, December 2023



Bidding farewell to what may be the final year of low-tech scams

Am I the only one experiencing a sudden craving for vintage toys at Christmas? As much as I marvel at the technological sophistication of modern toys, I can't help but feel a pinch of nostalgia at the memory - some of it manufactured - of a simpler time, where the present was the new ownership of a fresh new object. Not that I'm knocking a lovely card for a subscription to a cloud service. Or that perfect tech gizmo requiring an always-on app...

On second thought, I'm pretty sure that at least a certain group - scammers, of all people - has been embracing rudimentary strategies for making a buck. From low-tech scratch-and-relabeling of gift cards in stores to straight up lying on social media (gasp!), simple apparently works best. For criminals, good old phishing (albeit now by text) message sent to a million people is probably a better use of illicit resources than investment in advanced malware.

Unfortunately all that is showing signs of changing, from AI-generated deepfakes to malware built right into the smart devices procured from the factory.

Further placing demands on our vigilance is the increasing use of tracking apps and deceptive advertising that seek to monetize personal data and what little attention span we have left.

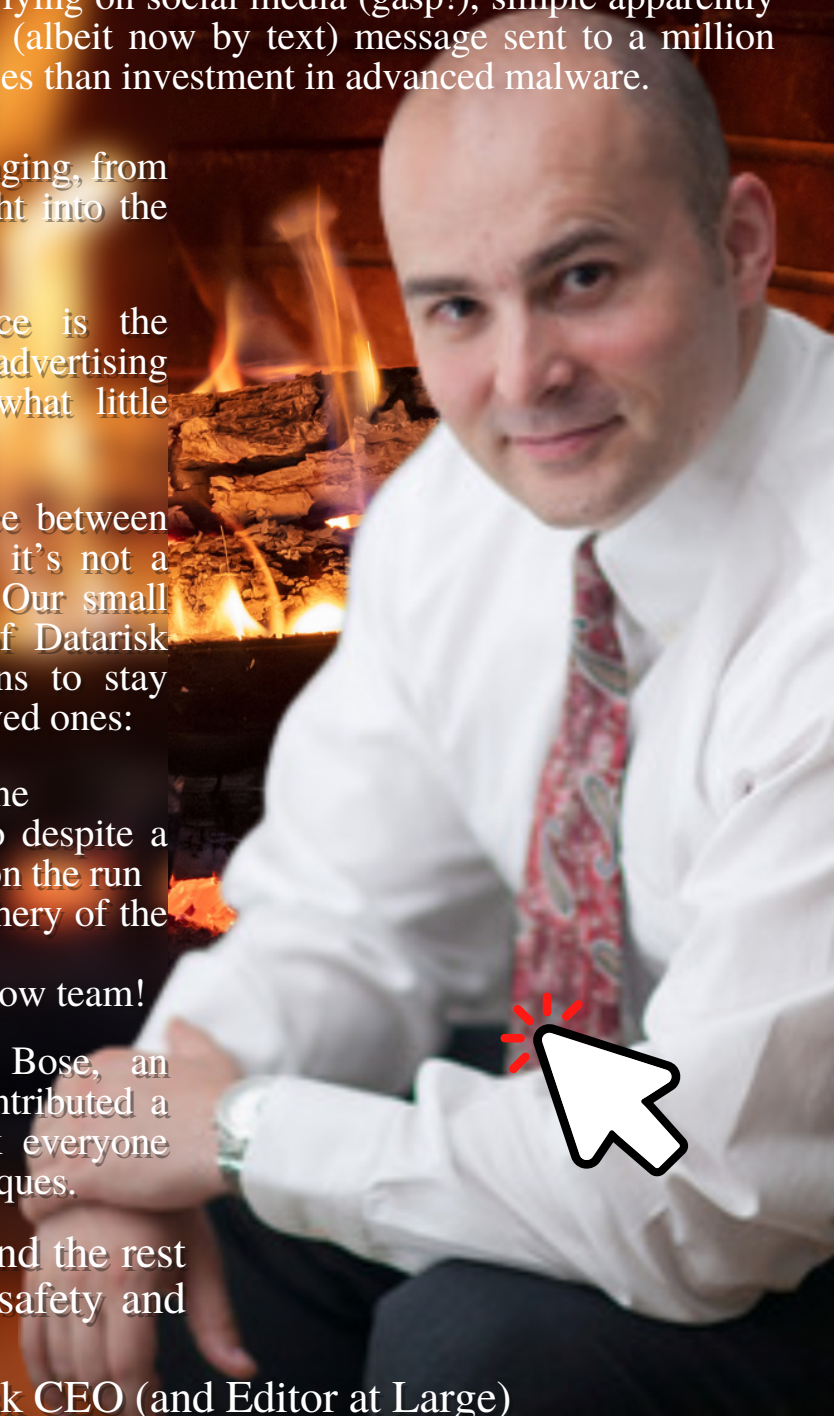
Although it's getting hard to see a difference between commercial spyware and criminal malware, it's not a reason to be a Grinch this holiday season. Our small team has put together a fresh new issue of Datarisk Magazine, with a whole set of new reasons to stay positive and hopefully share this issue with loved ones:

- a unique take on FUD-spotting for everyone
- spare a thought for cyber-criminals, who despite a profitable year are spending the holidays on the run
- salient things to look for after the debauchery of the New Year
- shareable resources from the Knowledgeflow team!

As an added treat, my friend Anindita Bose, an exceptional privacy advocate, generously contributed a lovely piece on a topic that we both think everyone needs to know more about: dark pattern techniques.

Along with the cybersafety foundation and the rest of our Datarisk team, I wish you cybersafety and peace in 2024!

Claudiu Popa - Datarisk CEO (and Editor at Large)



SAY NO TO CLICKBAIT

BY THE DATARISK EDITORIAL TEAM

If you're tired of **shameless scam attempts** during the holiday season, you're in the right place. At this point, its tradition for petty thieves and scammers to emerge from the woodwork and prey on the deep pockets of holiday consumers to make a quick buck. The holiday season is busy enough, and this year we want to enjoy it without worrying about **opportunistic cybercriminals**.

Thankfully, these trivialities are often scraped together and easy to spot, even hilarious to see if you know what to look out for. While mainstream media uses **fear, uncertainty, and doubt** to raise public anxiety, we're here to give you the cold, hard truth on what to watch out for during and after the holiday season.



You Can Make a Difference

This year, we say **#NotonMYinternet** and encourage our readers to report hilarious scams and ridiculous attempts at using dark pattern techniques to separate people from their money. Send your comments and screenshots to us at editor@datarisk.ca and we will feature them in future blogs. Who knows, there might be an extra present under your tree for some of our lucky readers!



The Gallery of Grinches



BY MILES LOWRY, EDITORIAL STAFF

The holiday season is synonymous with a dramatic increase in consumer spending, primarily on gifts, travel, and charitable donations. Unfortunately, this comes hand in hand with a rise in online scams. According to [a survey by AARP](#), **80% of individuals** aged 18 or older have experienced some form of **fraud this holiday season**.

Online scams come in many forms, and with the vast number of legitimate retailers offering discounts and limited-time offers it's difficult to identify what's legitimate and what's a scam. One prominent example of holiday scams is the **fake charity scam**. This is exactly what it sounds like, scammers position themselves as representatives from legitimate charity organisations and capitalize on people's goodwill, tricking them into making donations.

FBI Cyber Hall of Shame

This scam is particularly successful during the holiday season as people are often more generous and kinder ('tis the season!). The most elaborate charity scams involve a legitimate-looking website and email addresses to match, or they impersonate a real charity. When in doubt, verify that the organization has a **charitable number registered with the federal government**. They will send thousands of phishing emails and phone calls, hoping to catch some unlucky souls in their web of lies.

These scammers (like most) have tossed away their moral compass, and it's up to us, as consumers, to **report this nefarious activity to the proper authorities**. For more information on how fake charity scams work, visit: [How to identify and avoid charity scams | PayPal US](#)

Click to check out the FBI's "Cyber Most Wanted" List 2023. These cybercriminals will spend their holidays on the run.

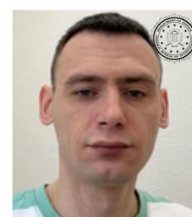
FBI Cyber's Most Wanted 



ANDREY STANISLAVOVICH KORINETS



RUSLAN ALEKSANDROVICH



MIKHAIL PAVLOVICH MATVEEV



MINH QUỐC NGUYỄN



Tis the Season for Dark Deeds: Spotlighting the Use of Dark Patterns in E-Commerce and by Fraudsters

BY ANINDITA BOSE (MI, CIPP/C, CISM)
CONTRIBUTING AUTHOR

Malicious By Design

Although we've focused on fraudsters thus far, this time of year continues to be ripe for legitimate e-commerce platforms to deploy various tactics and techniques to boost their sales. The commonality between both legitimate e-commerce platforms and fraudsters is their use of **dark patterns**.

Dark patterns are user interface design tactics and techniques that manipulate and deceive users into taking actions that the user otherwise might not initially choose to do.

Over the years, dark patterns have become notoriously prevalent and as per the Federal Trade Commission (FTC) Staff Report from September 2022, "dark patterns have grown in scale and sophistication, allowing companies to develop complex analytical techniques, collect more personal data". In this article, we will shine the spotlight on both legitimate e-commerce businesses and fraudulent actors that leverage dark patterns during the holiday season to influence the public.

Urgency and Scarcity Tactics: Phrases like "Limited Stock!" or "Offer Ends Soon!" create a sense of urgency and scarcity, prompting users to make quick purchasing decisions without thoroughly considering their options. Fraudulent e-commerce sites may fabricate positive reviews, ratings, and testimonials to convince users to make purchases based on false social proof.

Misleading Markdowns, Dubious Discounts, and Freebies: Prominently marketed discount prices or percentages are often exaggerated or applied to inflated base prices, manipulating users to believe they are scoring a better deal than they actually are. Fraudsters take it up a notch by offering unrealistically low prices or promoting a free product that will be provided upon signing up during a limited time period.

Confusing Opt-Out Mechanisms: Businesses may make it difficult for users to opt-out of email newsletters or promotional messages, increasing the chances of continued engagement by spamming inboxes.




How to Take Back Control

As dark patterns continue to permeate the e-commerce landscape during the holidays, consumers must remain vigilant. Here are some tips to help **protect yourself** from falling victim to manipulative tactics:

- **Research Before You Buy:** Take the time to research products and sellers, especially if the deal seems too good to be true. When in doubt, check it out!
- **Slow Down and Read the Fine Print:** Always read terms and conditions, return policies, and subscription agreements carefully before making a purchase. If a deal seems too good to be true, it likely is.
- **Use Secure Payment Methods:** Use secure and reputable payment methods that offer fraud protection, such as credit cards. Avoid sharing sensitive personal information on websites when registering for online accounts and ask yourself if what is being requested is proportional to process the transaction.



- **Report Suspicious Activity:** If you come across a website or offer that seems fraudulent, report it to relevant authorities or consumer protection agencies.


Users and online **consumers must remain vigilant and informed** to protect themselves from fraudulent e-commerce websites that exploit dark patterns for malicious purposes. Ultimately, the key to a safe and enjoyable online shopping experience during the holidays lies in awareness, education, and responsible business practices. For more information about dark patterns and the types of deceptive patterns that are out in the wild, visit: <https://www.deceptive.design/types> 



BY MILES LOWRY, EDITORIAL STAFF

Post-Holiday Pandemonium

IF you survive the holidays, you'll wonder whether any of your purchases were fraudulent, how much identity data you've left behind and what data leaks you have to look forward to in 2024.

 A survey by [Yahoo Finance](#) found shocking results that, although **94% of Americans** acknowledge the importance of protecting their personal data online, **55%** of them consciously do nothing when a data leak occurs. This problem is no different in Canada and around the world, that's why we're here to give you the low-down on becoming more digitally resilient and aware of the types of threats you're likely to see this coming year.

In 2022, the **CAFC** reported fraud and cybercrime losses of \$530 million, and they estimate losses of nearly \$450 million in 2023. Considering this is likely to represent only **5%** of total losses for the year, **Canadians have likely lost close to \$9 Billion from fraud and cybercrime in 2023.**

Online scammers don't magically disappear on January 1st. They often use the holidays to collect tons of personal data and then make their move in the new year.

Don't let them take advantage of you this year: monitor and scrutinize your bank statements for unauthorized charges and contact your bank immediately if any appear. Beyond the bank, watch out for social engineering tactics that take advantage of human emotion to extract your information and your money. To learn more about social engineering tactics, visit: [10 Types of Social Engineering Attacks - CrowdStrike](#)

Take Action

If you notice any suspicious behaviour, report it to the proper authorities immediately, as well as any other parties involved like your bank and the local police. It is to your advantage to report suspicious and unusual activities ASAP. For more information on how to effectively report scams, click to visit:

Shareable Cybersafety

Some online tips can be weaponized malware masquerading as helpful information, while others are produced by underqualified people. **Datarisk Magazine** is completely free, and so are the tip sheets you can share with your network. We strive to make these easily digestible by everyone, because the more people we can educate, the more people we can help. So pass it on!



For more freebies, visit: KnowledgeFlow.org



Claudiu's Cyber Holiday FAQ

(we've agreed to let him have his own "corner" of the magazine to keep him away from the other articles)



Why you should stop opening digital e-cards

Holidays are a great time to easily share attractive e-cards with people you haven't seen in a long time. Your best bet is to avoid **e-card sites** and their privacy invasive trackers. Instead, fire up Canva and create a custom image that people will appreciate!



Can you afford two clicks for each website?

Without protection, your Web browser discloses information about you before you even view the page. Always use an **ad blocker** to protect yourself from **malvertising**, and supplement it with a **Javascript filter** to control what runs of your device.



How do you properly read a Privacy Policy?

Privacy policies are long and daunting but accepting them without a summary skim is always a risk. Simply use **CTRL+F** to search for key terms like "Data Collection", "Cookie Use", and "Data Usage" to determine if you should trust the site. And use the contact info at bottom to ask questions!



Keep that Antivirus software up to date!

Antivirus software can work wonders if you don't let it lapse. **Pro tip:** use the free malware scanners offered by many antivirus websites to get a second opinion about your security hygiene.

Got questions? Send them to editor@datarisk.ca with your comments and suggestions. **Thank you for reading and sharing** this special Holiday Edition of Datarisk Magazine! Surf Safe!



DATARISK MAGAZINE



We want to hear from you!

- Feedback
- Contributions
- Editorial letters

Reach us at editor@datarisk.ca 
with your ideas and reactions!

Issue No. 2, December 2023

www.datarisk.ca



12345678

