
# Why Cybercriminals Feast During the Holidays Too

WHITE PAPER

cyberconIQ

cyberconIQ

# Why Cybercriminals Feast During the Holidays Too

## By Dr. James Norrie, Founder & CEO

Cybercriminals follow the money...and holidays, especially seasonal ones like Thanksgiving and Christmas. These holidays represent important spikes in spending. Think about it – Black Friday, Cyber Monday, price matching, coupon doubling, and how many days of Christmas shopping left. Wow! It just never ends.

During this upcoming busy holiday season, that also means as the traditional retail sector is the focus of continued Covid-19 restrictions, that more retail sales will occur online, which means e-commerce sites are in hackers' crosshairs more than ever. And shoppers are also likely to be more anxious than ever.

At cyberconIQ, our unique understanding of the intersection of cybersecurity and behavioral science gives us insights into how these two distinct, but related factors increase the online risk for both corporations and consumers alike.

Let us use a classic attack from last year to better frame your understanding of how these overlap: gift card fraud. This hurts both the consumers who pay for these fake cards and the brands that are portrayed in the theft. Hackers can use stolen credit card information to buy gift cards. Sold on the dark web, these gift cards are then converted to cash without your knowledge. Even if you can reverse the transaction, another kind of financial harm is now underway.

Because fake gift cards can be a double whammy for retailers. The stolen credit card data used to purchase gift cards lead to chargebacks, while the customer service imperative of the retail industry makes it hard for brands to deny transactions based on fraud their marketing efforts promoted.

Both the consumer and the corporation are hurt, although in different ways. The brand is also left with the heart-breaking question of redeeming, or not, fake gift cards that maybe someone's only lifeline to a happy Christmas. Imagine the heartbreak, wallet wrecks, and embarrassment that ensue round when these cybercriminals feast on our folly.

Other potential types of attacks that are common around this time of year further include spoofed email addresses used to gain access to supplier or customer logins, phony websites made to look exactly like those of major retailers offering outstanding deals on in-demand merchandise – never to arrive for instance. Some devilishly good fake apps contain adware and ad-clickers, or malware that steals personal information, or ransomware that locks the device until the user pays a ransom. Or not – because who has the money to do that at Christmas? Retailers are also beginning to pay attention to credit card sniffers. These are undetected malicious scripts that are injected onto payment pages of real e-commerce sites that scrape customer payment information, including crediting your online card data.

And let's not forget devices that capture and record credit card information and your PIN at physical points of purchase toot, especially for that last-minute gift purchased at a less than mainstream retailer where you barely notice anything at all about it because of the rush you are in!

Why do I highlight all this? Because we know around this upcoming time of year – "that most wonderful time of the year" to quote the famous carol – we are all already just a little bit more stressed, a little bit more frantic, and often far more vulnerable than the sugary sweet words of that song suggest.

In fact, for many, this is one of the most awful times of the year and our defenses fall. As a result, our research shows even more present online vulnerability than would normally be the case – and so it becomes simple holiday thugs to take advantage of our distracted state of mind.

What is one to do? Well, we would suggest this simple acronym:


I find of all the things that we do here, simple mnemonics are some of our most popular assets. They help us remember, in easy steps, some of the basics of what we need to do to keep ourselves safer online. These simple steps – all explained online at cyberconIQ.com – can help any consumer stay more alert and focused on avoiding the criminal feast that so often lurks around us this time of year.

So, if you have not started planning your cybersecurity strategy for the holidays, now is the time to do so. Threat activity will increase considerably over the next few weeks, but we are not yet in the thick of the holiday season. So, planning now is the only way to avoid getting breached this holiday season. And we hope you will let us help you accomplish that by visiting cyberconiq.com to learn more!

**For more information or to learn more about the cyberconIQ solution, please contact us at info@cyberconiq.com**