SA shoppers warned of online scams ahead of shopping season

By Dan Thornton

20 Oct 2022

Black Friday and Cyber Monday will soon start the holiday shopping season. After a long year of financial strain, South Africans are going to be more focused than ever on bargain-hunting for the best deals on offer. Apart from November's key e-commerce sales days, the pandemic's acceleration of the uptake in online shopping will mean that a significant portion of purchasing this festive season is going to happen online.

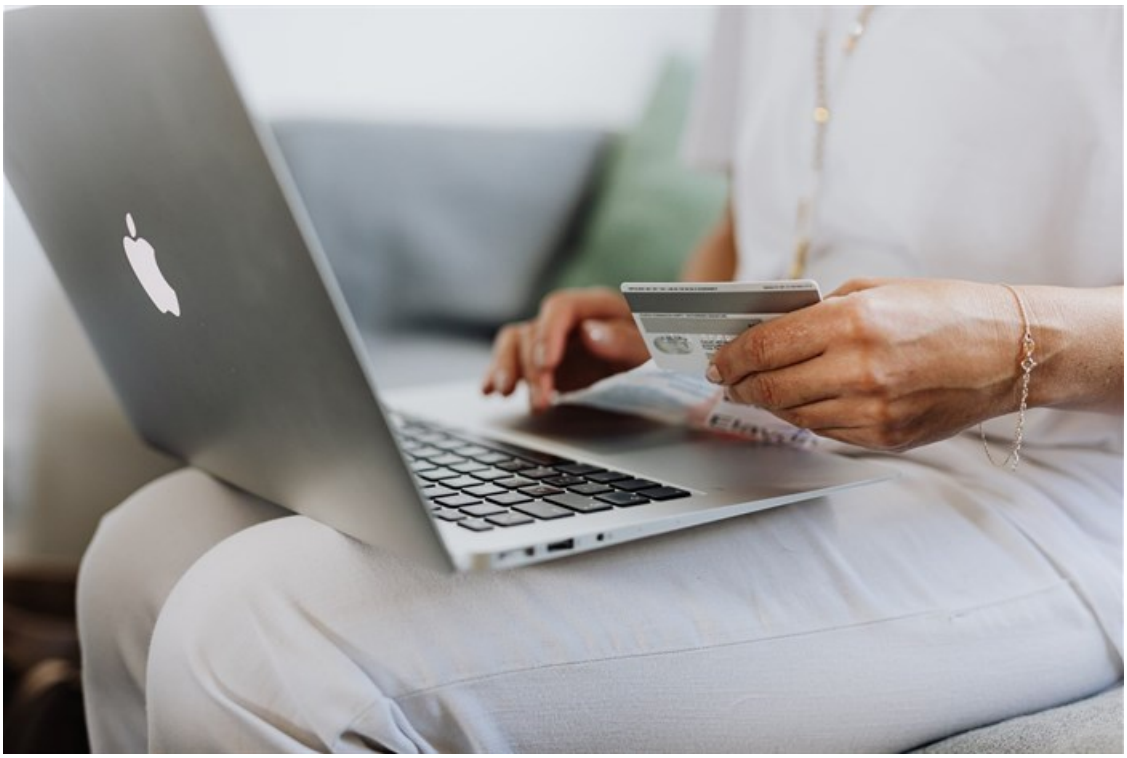

Image supplied

But it's not just the e-tailers and customers that are getting ready for the traditional end-of-year shopping bonanza, the scammers and fraudsters intend to get in on the action too. We have to be on the lookout for dodgy deals and be smart about prices that seem too good to be true.

Unfortunately, more online shopping activity means more opportunities for cybercrimes to take place. Global retail sales were estimated at $5.2tn last year and are predicted that global payment fraud over $40bn by 2027.

This holiday season, we can expect an array of shopping-related scams where you won't get what you have paid for, as well as an uptick in crimes such as identity theft and bank fraud. It's important to recognise the warning signs and to take immediate action to protect yourself and your loved ones.

Staying cyber-savvy during the silly season

Scam calls: Scammers around the world will still use landline and mobile phone numbers to reach unsuspecting victims during the holiday season.

They are likely to claim that they work for one of the big retailers or banks, and tell the victim that the company has become aware of a problem with their account.

They will then encourage the victim to download a tool on their computer to fix the problem, but the downloaded file will give them access to the victim's computer system where they can steal passwords, and financial and other personal information.

Phishing emails: Phishing emails are a staple scam and unfortunately, they're perfect for Black Friday as consumers will be receiving and reading more emails from retailers at this time of year.

Scammers can mimic the email designs of bona fide retailers making it hard, at first glance to identify the communication as a scam. Two common phishing email scams are:

- The 'account verification' scam email is a popular choice among scam artists. They typically claim that someone tried to hack into your account or that they need to update your information for security purposes. The email message will include a link for you to input your account information which they will then steal.

- 'Order confirmation' email scams are another common phishing technique to look out for.

  These emails will claim that one of your orders from a major retailer such as Takealot has been confirmed – but they won't tell you what the order actually is. Instead, you'll be encouraged to click on a link to find out.

  If you oblige, you'll be directed to a page that looks just like the Takealot site, but it'll be the fraudsters who receive your personal information if you log into what you think is your account.

When the seller is the scammer

Bargain hunting and feeling frantic for the best deal can take you to some dodgy digital spaces. During the holiday season, scammers set up shop and try to get you to pay them for what you want, but never deliver the goods. Beware of a product that is advertised at an unbelievably low price, or advertised to have amazing benefits or features that sound too good to be true.

The seller may insist on immediate payment or payment by electronic funds transfer or a wire service. They may want you to pay up-front for a voucher before you can access a cheap deal or a giveaway.

Your suspicions should also be aroused if you come across a new social media-based store selling products at very low prices but offering limited information about delivery and other policies; or an online retailer you've never heard of which does not provide adequate information about privacy, terms and conditions of use, dispute resolution or contact details.

Be wary if a seller does not allow payment through a secure payment service such as PayFast or a credit card transaction.

Here are six pitfalls to help you avoid shopping scams this holiday season:

1. **If a deal is too good to be true, it probably is** – Of course, Black Friday is all about discounts you can't get at any

time of the year, but don't let that cloud your common sense. If you're unsure about a link or a voucher, or a price just seems too low, head over to the retailer's site directly – if the deal is legitimate, it will be there.

2. **Don't give out any of your personal information** – Legitimate companies will never ask for you to share your bank details or passwords via text messages. If they're an online retailer, they will be aware of the prevalence of scams and will confidently provide you with proof of their legitimacy.

3. **Treat social media marketplaces with extreme caution** – If you're considering purchasing a product from a social media profile page, check how long the business has been around, how many followers it has, and whether the customer reviews come from real accounts.

Cybercrime on the rise in SA: How to protect your business, customers and employees

Business Partners Limited 18 Aug 2022

4. **Only sign off on secure payments** – When entering your details into a website, make sure there is a little padlock symbol in the address bar. In addition, always check that the URL from the site you're inputting details into begins with https:// as this signals that your data will be encrypted.

5. **Only use credit cards** - It is a lot easier for your bank to refund you if you've been scammed and you used a credit card to make the transaction. Transferring money directly from your account or using a debit card can make the refund process much more difficult.

6. **If you've been scammed, react immediately** - Your top priority is to contact your bank. Your credit cards must be replaced, and you must change your security details on your bank accounts. In addition, you need to be quick about resetting passwords and maximising the security settings on your online shopping accounts.

ABOUT DAN THORNTON

Dan Thornton, CEO and co-founder of GoldPhish Cyber Security Training, is a former Royal Marine Commandos Officer. During his seven years of service, he was deployed all over the world including multiple operational deployments leading teams in both Iraq and Afghanistan. He then transitioned from the military into a career in Corporate Security Risk Management helping international oil and gas companies operate safely and securely in some of the most high-risk locations around the world, including West Africa, North Africa, and the Middle East.

- SA shoppers warned of online scams ahead of shopping season - 20 Oct 2022
- Building cyber-savvy workplaces in SA - 3 Oct 2022
- Cyber savvy parents keep kids safer online - 22 Aug 2022
- Cyber fraud has steep collective costs - 27 Jul 2022
- Why cybersecurity needs to tighten up as cryptocurrencies plummet - 22 Jun 2022

View my profile and articles...