Specialised Security Services

PROJECT:
CYBER MONDAY WARNING
27 NOVEMBER 2023

A huge spike in scam activity is expected!

Every year, people spend millions of Rand on online transactions on Cyber Monday. The increase in online activity in the buildup to the big day, combined with a "bargain hunting" mindset, has opened the door for scammers and other cybercriminals to flourish.

EXPECTED SCAMS ON CYBER MONDAY:

SOCIAL MEDIA ADVERTISEMENTS FOR "TOO-GOOD-TO-BE-TRUE" DEALS:

- Mostly all scams come from Facebook, TikTok and Instagram advertisements.

- Scammers post advertisements with discounted prices to entice shoppers, but when you click, you will be taken to a fake website designed to scam you out of your money or you will be directed to a fake store that steals your personal information.
- In other instances, a person might receive his/her order from one of these stores, but the products will be fake grey market stock that was overpaid for by the customer.
- The bottom line: Don't blindly trust social media advertisements. If you see a deal you're interested in, navigate to the online store or retailer directly (not via the advertisement link) to see if the deal exists.

SELLERS ASKING FOR NON-TRADITIONAL PAYMENT OPTIONS:

- Online retailers will almost always accept traditional payment methods, such as credit cards or trustworthy payment apps like Payfast.
- If a store or seller will only accept a non-traditional payment method, they may be trying to scam you as these methods are harder to trace or refund.

BE EXTRA CAUTIOUS IF A STORE OR SELLER ASKS YOU TO PAY WITH:

- Cryptocurrencies:
    - Hackers love cryptocurrencies as they allow for anonymous transactions that can't be refunded or traced.
- Payment apps like Zelle, Venmo, and Cash App:
    - While some payment apps offer payment protection if you mark the payment as for a business, scammers will try to get you to mark it as personal — so it cannot be refunded.
- Gift cards:
    - Unless you're using a gift card on the retailer's official website (using an Apple gift card to buy an iPhone from the official Apple Store), this is a red flag for a scam.

FRAUDULENT DELIVERY NOTIFICATION MESSAGES:

- In this well-known phishing scam, fraudsters target you with a different type of message, a fake delivery notification from a courier service.
- These scams are most common over text messages or even WhatsApp and include a link to a site to "fix" the shipping issue

by entering your personal information on an auto-generated form.
- Always check on deliveries directly with the courier. Don't click on links in unsolicited text messages or emails.
- Instead, find your original email and use the included tracking number on the shipper's official website.

INCORRECT BANK DETAILS SCAM:

- One of the most common scams is scammers emailing shoppers to say their payment information is incorrect and that it needs changing immediately or the order will be cancelled.
- If a retailer asks you to change your bank details with urgency, it will be done through official channels and not through SMS or emails from unknown senders.
- Essentially, they are hoping to draw you into entering your bank details into a fake website that they have made to look real.
- Some of these websites look so real that even the trained eye needs to look twice to distinguish between the original and the fake.
- Regardless of whether you believe your bank details are correct or not, you should contact the retailer directly with any order confirmation or information so you can receive legitimate information on your account.
- Never enter banking information into a site that you reached by clicking on a link.

BOGUS DISCOUNT COUPON OR VOUCHER SCAMS:

- Even though Cyber Monday automatically includes some of the best deals of the shopping season, scammers know people always want a better deal.
- In these scams, they create fake websites that claim to house special discount codes, coupons, or vouchers for popular retailers.
- Avoid these scams by doing your own research.
- Companies almost never publicly share valid discount codes over 15 or 20%.
- Always ensure you check discount codes on the retailer's official site during the checkout process.

MEASURES TO HELP YOU AVOID THE MOST COMMON TRAPS:

BEWARE OF SKETCHY WEBSITES:

- You can usually spot knock-off websites due to their strange design features and functionality flaws like broken links, typos, and slow-loading pages.
- The company might also lack a physical address or contact details.
- Check for SSL encryption to ensure that the website is legitimate.
- You can spot this as there will be “HTTPS” and a padlock icon at the start of the web address.
- Don’t save your credit card information in online stores.
- This way, your payment details won’t be leaked if the store gets hit with a data breach.

NEVER CLICK ON UNFAMILIAR LINKS:

- If you receive an unsolicited text message from a strange phone number or a suspicious email about an order that you don't remember placing, resist the urge to react.
- If you know you have not ordered a product, there is no need to be concerned about a product delivery.
- If you know that you have not entered a competition, there is no competition to win or lose.
- Scammers want to disorient you with high-pressure tactics, so you'll quickly click a link to try and resolve "the problem," meanwhile you are being trapped.
- Don't click on links from unfamiliar senders.
- If you have any doubts about a sketchy text message or email, just delete it.
- You can always contact customer service directly if you have concerns about fraud.
- Your bank will never ask you for personal information via SMS or email.
- If you get a call from someone claiming to be from the bank, hang up and call your bank on a familiar phone number.

INSTALL ANTIVIRUS SOFTWARE AND USE A VPN WHERE POSSIBLE:

- Hackers use the Cyber Monday shopping frenzy as an easy way to infect devices with ransomware, malware, and other cyber threats.
- Not only that but shopping while on public Wi-Fi networks can also open you up to a whole host of security risks.
- Always use a computer that you feel comfortable with, always have an antivirus installed and whenever connecting to an unknown network, make use of a VPN service.

USE STRONG PASSWORDS AND A PASSWORD MANAGER:

- If hackers can break into your social or other online accounts, they can steal your personal information, financial details, and more.
- Make sure you're always using strong and unique passwords.
- For added security, always enable two-factor authentication (2FA) whenever possible and store your credentials in a secure password manager.

Use common sense and make informed decisions.

People mostly get caught by scammers because they allow themselves to be trapped by emotional thinking and tunnel vision induced by greed and/or a lack of information. When you spot a good deal, investigate and contact the retailers directly.

Do not overreact to unknown emails, SMSs or other forms of communication because you feel stressed out. Instead, take a breath and allow yourself a moment to properly evaluate the information, investigate the information and then react to the information.

It is imperative to bear in mind that ensuring safety during Cyber Monday necessitates a judicious blend of comprehensive knowledge, prudence, and attentive awareness of your surroundings.

Visit our Facebook page and our website for other current projects:

- https://www.facebook.com/MikeBolhuisOfficial
- http://www.mikebolhuis.co.za

Specialised Security Services invites the public to the Mike Bolhuis Daily Projects WhatsApp Group.
We have decided to close the previous WhatsApp channel to avoid any duplication and to centralise our efforts in one place.

This group is important in delivering insights into the latest crime trends, awareness, warnings and the exposure of criminals.

HOW TO JOIN THE MIKE BOLHUIS DAILY PROJECTS WHATSAPP GROUP:

- Simply follow the link to our dedicated WhatsApp group: https://chat.whatsapp.com/Ew1H1dbUR988qoG8gei2sE
- Hit the "FOLLOW" button to ensure you never miss our daily updates.
- Tap on the "BELL" icon to receive instant notifications whenever a new post is placed.
- Please share this with family, friends and colleagues.

ALL INFORMATION RECEIVED WITH REGARD TO THE PROJECTS WILL BE TREATED IN THE STRICTEST CONFIDENTIALITY AND EVERY IDENTITY WILL BE PROTECTED.

You may forward this document.

Regards,

Mike Bolhuis
Specialist Investigators into
Serious Violent, Serious Economic Crimes & Serious Cybercrimes
PSIRA Reg. 1590364/421949
Mobile: +27 82 447 6116
E-mail: mike@mikebolhuis.co.za
Fax: 086 585 4924
Follow us on Facebook to view our projects -
https://www.facebook.com/MikeBolhuisOfficial

EXTREMELY IMPORTANT: All potential clients need to be aware that owing to the nature of our work as specialist investigators there are people who have been caught on the wrong side of the law - who are trying to discredit me - Mike Bolhuis and my organisation Specialised Security Services - to get themselves off the hook.

This retaliation happens on social media and creates doubt about our integrity and ability. Doubt created on social media platforms is both unwarranted and untrue.

We strongly recommend that you make up your minds concerning me and our organisation only after considering all the factual information - to the exclusion of hearsay and assumptions.

Furthermore, you are welcome to address your concerns directly with me should you still be unsatisfied with your conclusions. While the internet provides a lot of valuable information, it is also a platform that distributes a lot of false information. The distribution of false information, fake news, slander and hate speech constitutes a crime that can be prosecuted by law. Your own research discretion and discernment are imperative when choosing what and what not to believe.

STANDARD RULES APPLY: Upon appointment, we require a formal mandate with detailed instructions. Please take note that should you not make use of our services – you may not under any circumstance use my name or the name of my organisation as a means to achieve whatever end.

POPI ACT 4 of 2013 South Africa: Mike Bolhuis' "Specialised Security Services" falls under Section 6 of the act. Read more here: https://mikebolhuis.co.za/popi-act-4-of-2013-section-6-mike-bolhuis/

SSS TASK TEAM:
https://mikebh.link/sss-task-team

SSS CYBERCRIME UNIT:
https://mikebh.link/sss-cyber-team

Specialised Security Services

You are receiving this email to inform and keep you up to date with violent and/or economic crimes. So that you can inform and protect your loved ones and everyone you know.

Our mailing address is:

Mike Bolhuis Specialised Security Services

Po Box 15075 Lynn East

Pretoria, Gauteng 0039

South Africa

Add us to your address book

Want to change how you receive these emails?

You can update your preferences or unsubscribe from this list.
