



—
Investing for a
world of change



Samantha Rule
Chief Information
Security Officer

Stay cyber-savvy this festive season

Online scams surge during the festive season. In South Africa, online shopping fraud increased by nearly 20% in 2024, according to SABRIC, with phishing attacks, fake courier notifications, and fraudulent retail sites becoming even more sophisticated during Black Friday and the holidays.

To help you navigate this heightened risk, we asked Samantha Rule, Ninety One's Chief Information Security Officer (CISO), to share her expert guidance. With over 20 years of experience in cybersecurity, a background in digital forensics, and IT risk, including leading Ninety One's global information security programme, Samantha has seen how simple digital habits can protect both your personal information and your financial wellbeing.

Here are her top ten tips to stay cyber-secure this festive season.

1 Think before you click

Fraudsters thrive on urgency and emotion, often using tempting offers or fake alerts to prompt a quick reaction.

Fraudsters thrive on urgency and emotion.

- Be cautious of unsolicited messages. Pause before clicking on any link or attachment, even if it appears to come from a familiar brand or bank.
- Hover over links to verify their destination.
- Never share your passwords, PINs, or one-time passwords (OTPs) via email, SMS, or phone.
- If something feels off, it probably is – trust your instincts and verify through official channels.
- **Report suspicious activity to your bank or IT team; every report strengthens the ‘human firewall’, helping protect everyone.**

2 Own your digital footprint

Your online presence is powerful, and so are the risks that come with oversharing.

- Avoid posting personal details, such as travel plans or financial milestones.
- Use unique, complex passwords for each account, and never reuse your work credentials elsewhere.
- Regularly review privacy settings on social platforms to control who can see your information.
- Keep personal and work emails separate.
- If you notice unusual activity in an account, act fast: change your password and enable extra security checks immediately.

3 Protect your devices

Your phone and laptop are your digital wallets – treat them as such.

Your phone and laptop are your digital wallets – treat them as such.

- Keep antivirus and system software updated.
- Only download apps from official app stores.
- Turn off Bluetooth and Wi-Fi when not in use.
- Back up your data regularly because ransomware and theft can strike in seconds.
- Never leave devices unlocked or unattended in public spaces.

4 Shop smart online

Festive shopping attracts both great deals and fake stores.

- Shop from trusted retailers or official apps.
- Look for subtle misspellings or extra characters in website URLs.
- Avoid clicking through shopping links in emails or on social media ads; instead, navigate directly to the retailer's website.
- Do not save your card details online unless necessary.

5 Use secure payment methods

Your payment method is often the last line of defence.

- Use virtual or single-use cards when available.
- Enable real-time transaction alerts.
- Credit cards generally offer stronger consumer protection than debit cards.
- Avoid entering payment information on shared or public devices.

6 Watch out for courier and delivery scams

This is one of the fastest-growing festive-season scams.

- Validate delivery notifications directly through the retailer's website or official courier app.
- Be cautious of messages claiming you owe a small 'additional fee'.
- Do not share personal details or addresses via WhatsApp or SMS from unknown numbers.

7 Stay alert on social media

Social media platforms influence many online purchases, and scammers are aware of this.

- Verify the legitimacy of deals promoted by influencers or ads.
- Check independent reviews (not just social comments).
- Be wary of pressure tactics such as 'only 5 minutes left!' or 'limited stock'.

8

Prepare your family

Households often experience an increase in digital activity at this time of year.

- Talk to your children about safe online behaviour, especially in games or apps that involve in-app purchases.
- Consider using parental controls for spending and app downloads.
- Remind family members not to share personal data or passwords with others.

9

Be aware of AI-driven scams

Scammers now use AI to create convincing voices, messages, and fake support chats.

- If someone claims to be from your bank or an online retailer, hang up and call back using an official telephone number.
- Be aware when someone sounds ‘almost but not quite’ like a known person.

10

Be festive, but remain vigilant

The season is about joy and connection, not cybercrime.

- Pause before you click, pay, or post.
- Adopt small digital habits that protect your information and financial wellbeing.

Quick checklist

Five things to do before you shop online

- ✓ Update your device software.
- ✓ Enable multi-factor authentication (MFA) and ensure passwords are strong.
- ✓ Turn on transaction alerts.
- ✓ Verify websites before entering card details.
- ✓ Avoid public Wi-Fi when banking or shopping.

Being cyber-aware is no longer just about protecting data; it's about protecting your financial wellbeing. Every small action you take online strengthens your ability to safeguard what you've worked hard for.

When you stay alert, you stay in control, and that's what true financial confidence looks like.

| When you stay alert,
you stay in control.

Important information

All information and opinions provided are of a general nature and are not intended to address the circumstances of any particular individual or entity. We are not acting and do not purport to act in any way as an advisor or in a fiduciary capacity. No one should act upon such information or opinion without appropriate professional advice after a thorough examination of a particular situation. We endeavour to provide accurate and timely information, but we make no representation or warranty, express or implied, with respect to the correctness, accuracy or completeness of the information and opinions. We do not undertake to update, modify or amend the information on a frequent basis or to advise any person if such information subsequently becomes inaccurate. Any representation or opinion is provided for information purposes only. This is the copyright of Ninety One and its contents may not be re-used without Ninety One's prior permission. Ninety One Investment Platform (Pty) Ltd and Ninety One SA (Pty) Ltd are authorised financial services providers.

Contact information

36 Hans Strijdom Avenue
Foreshore, Cape Town 8001

Telephone: +27 (0)219011000
Client service support: 0860 500 100
Email: clientservice@ninetyone.com

Please contact our Advisor Service Centre on
telephone: 0860 444 487

Alternatively, please contact your Ninety One
investment consultant.

www.ninetyone.com