COMMUNITY

Safety Tips

Beware of "Selfie" scams:

From ID verification to selfie spoofing by scammers

By **Annalise Kempen**
Photos and images courtesy of **Pixabay and Freepik**

The younger generation is skilled at taking selfies and uploading them to social media. They know how to strike the right pose to make the selfies look less amateurish using remote triggers or selfie sticks. When they are satisfied with the "look" they post these selfies across social media platforms for their friends and followers to like or for comment. In a world where cybercriminals are always on the prowl for their next victims, they are even taking advantage of our selfies to perpetrate fraud.

In 2024, one of South Africa's major banks warned us about a new digital banking scam linked to selfie verification, where scammers trick users into revealing details like their ID numbers. The scammer will ask someone to take a selfie of their intended victim, but by using their own (the fraudster's) smartphone. This step is important to enable them to load a banking app profile on their smartphones using a specific user's name and details, without their knowledge. In some cases, they use the app to change a user's cellphone number, allowing them to intercept any authorisation messages or notifications from the bank. Once they successfully set up a profile using a specific user's selfie and details, they gain full access to that user's bank account (Nedbank, 2024) to perpetrate fraud.

Another variation involves scammers reaching out to users via e-mail, imitating financial service providers such as banks, payment systems or even social network platforms, requiring users to update their security settings by confirming their identity. The link in the e-mail takes users to an online form, prompting them to provide their account credentials, payment card details, address, telephone number or other personal information, and to upload a selfie with a clearly visible ID card or another document. For users who have already reached this point, it is the best time to stop and ask: **Is it a good idea to upload your selfie along with your ID? Have you verified that you have accessed a legitimate website or have you accessed a spoofed website?** Chances are that scammers are waiting for your personal information on a spoofed website, enabling them to perpetrate fraud (Grustniy, 2019).

Another form of identity fraud

In 2024, Help Net Security, an independent cybersecurity publisher, reported that **document image-of-image** was the most prevalent **identity (ID)** document **fraud** technique in 2023, occurring in 63% of

rejected IDs, according to Socure, a leading platform for digital identity verification and trust. This happens when a user uses a screenshot image of an ID or takes a photograph, rather than providing a live capture of a document. Fraudsters then tamper with the document by purposefully manipulating the facial imagery (Help Net Security, 2024).

The purpose of **face spoofing** is to deceive biometric facial recognition systems by presenting false images, videos or even masks to impersonate another (Ughade, 2024). Selfie spoofing happens when a picture of an image on a computer screen is taken and printed or even of an actual headshot on a different document, with the intention of stealing identities or fraudulently accessing systems (Help Net Security, 2024).

How are selfies spoofed?

The South African Banking Risk Information Centre (SABRIC) has warned that scammers are using our selfies and biometrics to hack into our banking apps - and once they have access to our banking apps, they can steal our money. Nedbank (2024) explains the selfie scam as follows:

Step 1:

Fraudsters pose as cellphone or retail store employees and offer a user free airtime or shopping vouchers. We know that free offers are usually too good to be true.

Step 2:

To enable the scammer to upload the non-existent voucher, they ask the user for personal information, including their ID number, whereafter they take a "selfie" of the user by using their own device. While the user is being led to believe they are being registered for a voucher, the scammers are registering the user on the banking app but using their own cellphone number.

Step 3:

Once the scammers have the legitimate user's banking app information registered on their smartphone, using their selfie, they convince the user to hand them their phone, so they can secretly accept the Approve-it message for the registration of the user's device with the legitimate user's selfie. This means that the legitimate users will not even be aware that someone else has linked their device to their banking app profile.

Step 4:

Once the fraudster has the legitimate user's banking app on their device, they can change cellphone numbers, process transactions, and have full access to the victim's banking profile.

Why is this form of ID fraud such a grave concern?

In addition to financial institutions such as banks using selfie verification to grant users access to their banking apps, this form of verification is also used by some organisations and security agencies to verify the authenticity of a government-issued ID, including driving licences and passports, by matching it to a selfie. This step is critical if an organisation needs to verify a customer's age and identity when opening an account or it can be used to verify a driving licence before allowing a customer to rent a car. In some countries, it is also used to confirm a younger person's age who wants to purchase alcohol online (Help Net Security, 2024).

Fraudsters use various tactics to circumvent identity verification systems, including:

- Acquiring access to buildings with facial recognition systems, often to steal important corporate data stored in the building (ID theft);
- creating false identities to sign up for services and engage in other types of fraud, including insurance or iGaming fraud;
- adopting somebody else's identity (attacks involving impersonation); and/or
- avoiding KYC and screening processes, or more generally, to avoid system recognition (Ughade, 2024).

SABRIC (nd) adds that scammers perpetrate identity fraud using various methods, including deepfake attacks; SIM swap fraud; fake KYC (know your customer) and phishing scams.

Selfie verification

The rise in data breaches, compromising and exposing personal and sensitive information of thousands of customers, necessitates that businesses seek additional methods to verify and protect identities. One of the solutions is selfie verification, enabling organisations to verify users' or customers' identities and reducing the risk of identity fraud.

Selfie verification is typically based on six steps, namely:

- Capturing a government-issued ID
- Uploading the ID
- Taking a live selfie
- Performing liveness detection
- Face matching
- Validation and approval (Arku, nd).

Selfie ID or biometric verification is also called liveness detection, referring to a security feature allowing digital users to remotely verify their identity by taking a real-time photo of themselves. This process enhances ID document verification and requires users to do a live capture through "active liveness". The user is typically asked to look in different directions by turning their head or making certain facial expressions (Socure, nd), such as blinking or smiling (Incode, 2022).

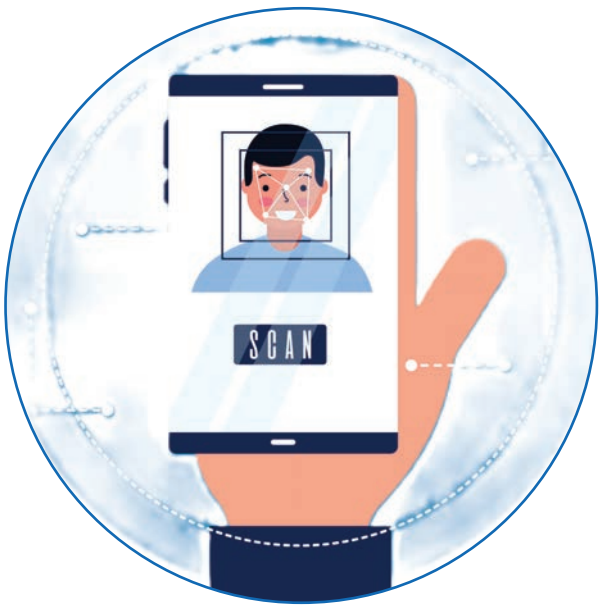
Incode (2022) explains that liveness detection is important for combating spoofing and fraud and for complying with know your customer (KYC) standards. This method aims to spot if the user is a living, physically present person, rather than a fraudulently used image. Users may complain that liveness tests for selfie verification are time-consuming or cause user irritation during the onboarding process, but it is vital to verify identity. Liveness tests can also be passive, using technology to detect spoofs by examining skin texture or motion. Organisations may choose this method to offer security against fraud without compromising user experience.

Another method of limiting the risk of selfie spoofing and combating fraud is to implement a process of capturing selfies in real-time to validate the user's identity during the verification process. This process requires a user to take and submit their photo on the spot as prompted by a verification system. This method aims to confirm the person's current presence and deters the submission of photos or images of someone else (Socure, nd).

TIPS TO PROTECT OURSELVES

Users can take various steps to protect their identity and money, ranging from being more vigilant before accepting offers about "freebies" to implementing additional security measures. Relating to the selfie scam, Nedbank (2024) provides the following tips to keep users safe:

- Never hand your phone to a stranger or pose for a selfie taken on their smartphone;
- never accept any promotion on face value. Do your own homework by checking any promotions independently with the store or organisation; and
- always read "Approve-it" messages carefully before accepting them.



SABRIC provides the following advice as a measure of protection against selfie spoofing and identity fraud:

- Only upload your selfie or biometrics onto official banking apps or websites;
- never share your selfie or biometrics, ID or other personal information via WhatsApp, e-mail or SMS if you have not verified the use thereof for legitimate purposes that you have initiated; and
- enable 2FA (two-factor authentication) on ALL your banking apps and Internet banking (SABRIC, nd).

Many financial institutions have implemented two-factor authentication as an additional layer of security. Microsoft (nd) explains it as "an identity and access management security method that requires two forms of identification to access resources and data". This can be in the form of an SMS verification with a one-time pin (OTP), a hardware token, a push notification or voice biometrics. Two-factor authentication has become a non-negotiable feature, especially when dealing with financial institutions, as even our selfies alone are no longer effective to confirm our identification because of scams.

Kaspersky, a global cybersecurity company, reminds us that to prevent fraudsters from stealing our identity, we must be wary of any requests for data, especially relating to documents. They offer the following advice:

- Be suspicious of requests to verify your identity for services you have been using for a while. If you are unsure about the legitimacy of a particular message, verify the information independently on the company's official website.
- Pay attention to the quality of the text, specifically relating to grammatical errors, missing words and typing mistakes. These mistakes are extremely rare in authentic corporate communications.
- Check the origin of the message and where the link points by hovering over the link and the sender’s e-mail address with your computer's mouse. Companies send e-mails from official domains (beware of small variations in the domain name). Companies do not use free providers such as Gmail or Yahoo. Any exceptions will be explained on their websites, as will surveys, login forms and other official pages be cited on official resources.
- Resist responding to messages where you are urged to act immediately without having time to verify the legitimacy of the message. Rather miss the deadline than send your data to cybercriminals.
- If you have any doubt, always call the company or organisation's customer services by using the number that you sourced independently from the company's website or by using the number that you previously used for communication.
- Download a reliable antivirus program with protection against phishing and online fraud. Remember to run regular scans, preferably automated to run daily and enable regular security updates for your devices (Grustniy, 2019).

In a world where cybercrime is growing exponentially as fraudsters constantly try to be one step ahead of our efforts to protect personal and sensitive information, we can never rest on our laurels. We should never trust anyone on face value, especially when they offer a freebie or special offer requiring our personal information and/or biometrics, ie, selfies if we did not initiate the process to acquire or sign up for a legitimate service. Please remain vigilant and always verify the authenticity of any message or offer with the organisation independently. We have a responsibility and an urgency to protect our personal data with much more effort than we used to.

Editor’s note

The list of references is published on p79.

Arku, G. 2024. "Selfie ID verification: What is it and how does it work? - Accessed at https://usesmileid.com/blog/selfie-id-verification/ Accessed on 10 January 2026.
Grustniy, L. 2019. "Kaspersky daily." - Accessed at https://www.kaspersky.co.za/blog/selfie-with-id-card-scam/23148/. Accessed on 10 January 2026.
Help net Security. 2024. "Selfie spoofing becomes popular identity document fraud technique." Accessed at https://www.helpnetsecurity.com/2024/05/10/identity-document-selfie-spoofing/ Accessed on 10 January 2026.
Incode. 2022. "Using iBeta-certified facial liveness detection to combat digital identity fraud." - Accessed at https://incode.com/blog/using-ibeta-certified-facial-liveness-detection-to-combat-digital-identity-fraud/. Accessed on 12 January 2026.
Microsoft. Nd. "What is two-factor authentication?" - Accessed at https://www.microsoft.com/en-za/security/business/security-101/what-is-two-factor-authentication-2fa. Accessed on 14 January 2026.
Nedbank staff writer. 2024. "Beware the fake selfie-verification scam." Nedbank. 2 October. - Accessed at https://personal.nedbank.co.za/learn/blog/beware-of-fake-selfie-verification-scam.html. Accessed on 10 January 2026.
Socure. Nd. "Selfie ID verification." - Accessed at https://www.socure.com/glossary/selfie-id-verification. Accessed on 13 January 2026.
South African Banking Risk Information Centre (SABRIC). Nd. "Beware: Selfie and Biometric fraud is on the rise." - Accessed at https://www.sabric.co.za/resources/. Accessed on 10 January 2026.
Ughade, N. 2024. "A complete guide on face spoofing." HyperVerge. 26 December. - Accessed at https://hyperverge.co/blog/what-is-face-spoofing/. Accessed on 13 January 2026.