KUBERVEILIGHEIDSGIDS

Begryp die algemeenste kubermisdaadbedreigings – en hoe om dit te vermy

AfriForum

Inhoud

Inleiding

Suid-Afrika bly een van die lande in Afrika en wêreldwyd wat die meeste onder kubermisdaad deurloop. In 2025 het telekommunikasiebedrog alleen operateurs meer as R5,3 miljard gekos (volgens COMRiC). Terselfdertyd het verliese weens aanlyn bankbedrog aansienlik gestyg, meestal deur uitvissing (Engels: *phishing*). SABRIC-verslae beklemtoon dat uitvissing verantwoordelik is vir ongeveer 78% van aanlyn bankbedrog in onlangse jare, en meer as 40% van Suid-Afrikaners is in 2025 volgens wêreldwye opnames bedrieg.

Die meeste kubermisdaad behels nie gesofistikeerde kuberkrakery (Engels: *hacking*) nie. Misdadigers maak op misleiding, manipulasie, sosiale manipulasie en, toenemend, KI staat om mense te mislei om toegang tot hul bankbesonderhede of geld te kry.

Hierdie gids stel die algemeenste bedreigings uiteen wat Suid-Afrikaners vandag raak (bygewerk vir 2026-tendense) en bied praktiese, bygewerkte stappe om jouself te beskerm.

Uitvissingaanvalle

Uitvissing is steeds die algemeenste kubermisdaadbedreiging in Suid-Afrika.

Misdadigers stuur bedrieglike e-posse, SMS'e (Engels: *smishing*), WhatsApps of oproepe, en gee voor dat hulle wettige organisasies soos banke, koeriers, die SAID, regeringsdepartemente of diensverskaffers is.

Die doel is om jou te mislei om die aantekeningbesonderhede van jou aanlyn bankdienste, wagwoorde, eenmalige persoonlike identifikasienommers (PIN's; Engels: *OTPs*), kredietkaartnommers te verklap of op kwaadwillige skakels of QR-kodes te klik.

Algemene uitvissingsbedrog in Suid-Afrika

- Vervalste banksekuriteitswaarskuwings of "verdagte aantekening"-waarskuwings
- Vervalste koerieraflewerings boodskappe wat 'n klein vrystellingsfooi of doeanebetaling versoek
- Vervalste belastingterugbetaling of SAID-kennisgewings
- Vervalste intekeninghernuwings (Netflix, Showmax, Amazon)
- Vervalste werkaanbiedinge, pryse of dringende gesinsnoodgevalle
- Quishing: bedrieglike QR-kodes in e-posse, plakkate of boodskappe wat jou na vervalste aantekenbladsye neem

Waarskuwingstekens

- Dringende taal: "Tree onmiddellik op of jou rekening sal geblok/gesluit word."
- Versoeke om jou persoonlike inligting te verifieer of by te werk, of 'n QR-kode te skandeer
- Skakels of QR-kodes na onbekende of effens verkeerd gespelde webtuistes
- Swak spelling of grammatika (alhoewel KI nou die grammatika van baie hiervan korrigeer)
- Onverwagte oproepe of stemnotas met gekloonde stemme

Hoe om jouself te beskerm

- Moet nooit op skakels klik of QR-kodes skandeer in ongevraagde boodskappe oor bankdienste of sekuriteit nie.

- Kry altyd toegang tot jou bank deur die amptelike **webtuiste** of toepassing direk in jou blaaier se lyn in te tik.
- Moet nooit wagwoorde, **eenmalige PIN's** of persoonlike besonderhede via skakels, oproepe of boodskappe deel nie.
- Indien jy onseker is, beëindig die oproep en kontak die organisasie deur die amptelike nommers van hul webwerf of toepassing te gebruik.
- Gebruik oproeper-ID-programme soos Truecaller om verdagte oproepe te sif.

SIM-ruilbedrog

SIM-ruilbedrog bly 'n groot bankbedreiging in Suid-Afrika, met telekommunikasieverliese wat R5,3 miljard in 2025 oorskry het.

Misdadigers mislei jou selfoonverskaffer om jou nommer na hul SIM oor te dra. Hulle onderskep dan eenmalige PIN's, verander wagwoorde en kry toegang tot bankrekeninge.

Hoe misdadigers SIM-ruilbedrog pleeg

- Hulle versamel jou persoonlike inligting vanaf sosiale media, datalekkasies of uitvissing.
- Hulle gee voor om jy te wees om 'n SIM-ruil aan te vra (dikwels deur vervalste ID's of dokumente te gebruik).
- Hulle gebruik dié nuwe SIM om eenmalige bank-PIN's te kaap en al jou geld te onttrek.

Rooi ligte

- Skielike verlies van die netwerksein
- Onverwagte SIM-ruilkennisgewings van jou verskaffer
- Ongevraagde wagwoordherstelboodskappe of eenmalige-PIN-versoeke

Hoe om jouself te beskerm

- Kontak onmiddellik jou diensverskaffer (Vodacom, MTN, ens.) indien jou sein onverwags verswak.
- Vra jou diensverskaffer om 'n SIM-ruil-PIN, bykomende sekuriteitswagwoord of SIM-ruilwaarskuwing op jou profiel te laai.
- Moenie sensitiewe persoonlike inligting op sosiale media plaas nie.
- Aktiveer banktoepwaarskuwings en gebruik toepgebaseerde of biometriese verifikasie eerder as eenmalige PIN's wat per SMS gestuur word waar dit ook al moontlik is.

Sake-e-pos-bedrog (faktuurbedrog)

Dit raak besighede en individue, veral in eiendomstransaksies, verskaffersbetalings of groot transaksies. Misdadigers moniteer e-posse of boots wettige partye na om vervalste "bygewerkte bankbesonderhede" te stuur.

Hoe die bedrog werk

1. Die misdadigers spioeneer op regte e-poskommunikasie.
2. Hulle stuur dan 'n boodskap as 'n verskaffer, prokureur of kollega.
3. Hulle verskaf bedrieglike betalingsinstruksies.
4. Die slagoffer dra die geld oor, en die fondse word vinnig verder oorgeplaas.

Hoe om jouself te beskerm

- Verifieer altyd die bankbesonderhede per telefoon (deur bekende of gestoorde nommers te gebruik) voordat jy enige faktuur betaal.
- Moet nooit net op e-pos staatmaak vir finansiële wysigings nie.
- Wees agterdogtig oor skielike "bygewerkte" besonderhede, selfs al lyk dit wettig.
- Bevestig groot of hoëbedragbetalings deur 'n sekondêre kanaal ('n telefoonoproep of WhatsApp-stemnota van 'n bekende kontak).

Bank- en selfoontoepbedrog

Bankdienste-toeps op selfone word swaar geteiken. Aanvalle sluit in vervalste programme, indringerware (Engels: *malware*), vervalste ondersteuningsoproepe en sosiale manipulasie. Misdadigers bel dikwels en gee voor dat hulle "bedrogafdelings" is, en dring daarop aan dat jy inligting deel of hul afstandtoegang (Engels: *remote access*) gee.

Belangrike reël

Banke vra **nooit** oor die telefoon vir wagwoorde, eenmalige PIN's, afstandtoegang of om programme te installeer nie.

Hoe om jouself te beskerm

- Laai banktoeps slegs by die amptelike Google Play of App Store af.
- Moet nooit eenmalige PIN's met enigiemand deel nie, insluitend mense wat jou bel en beweer dat hulle van jou bank is.
- Moenie vreemdelinge afstandtoegang tot jou foon of rekenaar gee nie.
- Gebruik sterk, unieke wagwoorde en aktiveer biometrie (jou vingerafdruk of gesig-ID).

Indringerware en kwaadwillige aflaaie

Indringerware steel inligting deur besmette lêers, toepassings of webtuistes. Dit versprei dan deur e-posaanhangsels, vervalste sagteware, geroofde (Engels: *pirated*) inhoud of gekompromitteerde webtuistes. Dit kan die vingerdrukke (Engels: *keystrokes*) op jou sleutelbord en bankbesonderhede vasvang, of jou lêers sluit. Selfoondiefstal (toestelle wat nie gesluit is nie) is 'n belangrike toegangspunt.

Hoe om jouself te beskerm

- Vermy geroofde sagteware, films of speletjies.
- Moenie verdagte aanhegsels oopmaak of lêers van onbekende bronne aflaai nie.
- Installeer betroubare anti-virussagteware (bv. van Google Play of App Store).
- Sorg dat jou foon of rekenaar se bedryfstelsel en toepassings altyd die nuutste weergawes is.
- Sluit jou toestelle met 'n PIN of biometrie, en aktiveer afstanduitvee (Engels: *remote wiping*), ingeval jou foon gesteel word.

Losprysaanvalle

Losprysaanvalle enkripteer lêers en stelsels, en die oortreders eis dan betaling in kriptogeld. Hulle teiken hoofsaaklik organisasies, maar individue (veral mense met swak rugsteuning (Engels: *backup*) het) kan ook slagoffers van hierdie aanvalle word.

Hoe om jouself te beskerm

- Rugsteun gereeld belangrike data na eksterne bedieners of die wolk (waar moontlik nie aanlyn nie).
- Vermy verdagte aanhegsels of skakels.
- Sorg dat jou toestel se sagteware altyd die nuutste weergawe is.
- Gebruik slegs betroubare kuberveiligheidsagteware.
- Moet nooit hierdie lospryse betaal nie; dit befonds misdaad en die herstel van jou inligting kan nooit gewaarborg word nie.

Beleggings- en kriptogeldeenheidsbedrog

Hierdie bedrog belowe hoë opbrengste uit laerisikobeleggings, dikwels via WhatsApp-groepe, sosialemedia-advertensies of vervalste platforms. Baie gebruik vervalste aanbevelings deur bekende persone of inhoud wat deur kunsmatige intelligensie geskep is.

Rooi ligte

- Gewaarborgte winste of “geheime” geleenthede
- Druk om onmiddellik te belê of op te tree
- Versoeke vir kriptobetalings
- Moeite om fondse te onttrek

Hoe om jouself te beskerm

- Doen deeglike navorsing oor hierdie tipe platforms (gaan FSCA-registrasie na).
- Wees skepties oor gewaarborgde opbrengste.
- Vermy onbekende beleggingskemas of -groepe.
- Raadpleeg ’n gelisensieerde finansiële adviseur.

KI-aangedrewe en gevorderde sosiale-ingenieurswesebedrog

KI gee in 2026 bykomende mag aan swendelaars, wat hulle dan in staat stel om beter uitvissing, diep vervalsing en stemkloning te kan bewerkstellig.

Algemeen in Suid-Afrika

- Diep vervalste video’s of klank wat familie, bankpersoneel of bekendes naboots
- Gekloonde oproepe (“noodoproepe” van “familielede” wat geld nodig het)
- KI-geskepte perfekte uitvissingsboodskappe
- Vervalste beleggingsadvertensies met gekloonde aanbeveling

Rooi ligte

- Ongewone stemme of vreemde sinskonstruksies in oproepe en/of stemnotas
- Dringende versoeke vir oordragte (veral in kriptorekeninge)
- Geleenthede wat te goed is om waar te wees op sosiale media en WhatsApp
- Jou versoeke vir regstreekse videobewys word geïgnoreer.

Hoe om jouself te beskerm

- Verifieer onverwagte versoeke deur bekende of gestoorde kontakmetodes.
- Vra vir lewendige bewyse (bv. spesifieke gebare of woorde) op video-oproepe.
- Wees skepties oor ongevraagde stemoproepe of video's; beëindig die oproep en bel terug.
- Moenie toeps via oproepe of boodskappe aflaai nie.
- Meld verdagte inhoud onmiddellik by die toepaslike platform of die owerhede aan.

Onontbeerlike kuberveiligheidsgewoontes

Hierdie gewoontes kan die meeste insidente keer:

1. Beskerm wagwoorde: Gebruik sterk, unieke wagwoorde (oorweeg 'n toep wat jou wagwoorde bestuur).
2. Moet nooit eenmalige PIN's deel nie: Wettige entiteite vra nooit hiervoor nie.
3. Dink voordat jy klik of skandeer: Vermy verdagte skakels, QR-kodes en aanhegsels.
4. Verifieer die besonderhede voordat jy geld oorbetaal: Bevestig die besonderhede deur 'n direkte oproep.
5. Beskerm jou persoonlike inligting: Moenie persoonlike inligting aanlyn deel nie.
6. Aktiveer multifaktorverifikasie: Verkies toeps of biometrie eerder as SMS'e.
7. Moniteer data-uitlekke: Gebruik webwerwe soos https://haveibeenpwned.com/.
8. Sluit jou toestelle en meld diefstal onmiddellik aan.
9. Gebruik bedrogvoorkomende toeps soos Truecaller en bankwaarskuwings.
10. Bly op hoogte: Volg SABRIC, jou bank of vertroude bronne.

Wat om te doen as jy 'n slagoffer is

1. Kontak jou bank onmiddellik om jou rekeninge te vries en jou kaarte te blok.
2. Meld die misdaad by die SAPD aan (by die kubermisdaadeenheid of jou plaaslike stasie).
3. Stel jou selfoonverskaffer in kennis van SIM-probleme.
4. Verander al jou wagwoorde en aktiveer ekstra waarskuwings.
5. Rapporteer uitvissing aan die organisasie wat nageboots word.
6. Soek hulp van SABRIC-hulpbronne of verbruikersbeskerming, indien nodig.

Laaste gedagtes

Kubermisdadigers floreer op spoed, verwarring, dringendheid en vertroue. Met KI wat bedrog meer oortuigend maak, is die beste verdediging bewustheid, waaksaamheid, versigtigheid en verifikasie. Kubersekuriteit gaan oor gewoontes en ingeligte besluite, en nie net tegnologie nie. Bly waaksaam – bedreigings ontwikkel vinnig.