

Moet nooit KI vir 'n regte, egte mens misgis nie

Tegnologie is hier om die lewe te vergemaklik, maar dis belangrik dat jy ook waaksaam moet wees. **Tasneem van Rooyen** deel wenke oor hoe jy jouself in die digitale era kan beveilig.

Die meeste dinge kan deesdae met die klik van 'n knoppie gedoen word. Jy kan alles van betalings en inkopies tot gesels met jou geliefdes oorsee nou aanlyn doen. Net 'n dekade of twee gelede was dit alles onmoontlik.

Daar is ook 'n toename in kunsmatige intelligensie (KI), wat dit moeiliker maak om die waarheid van fopnuus te onderskei en swendelaars uit te ken.

Dit is jou verantwoordelikheid om seker te maak dat vreemdelinge (of kennisse) jou nie met 'n slap riem vang as dit by jou geldsake en tegnologie kom nie.

Dylan Coetzee, die praktykbestuurder van Oracle Netsuite by Steltix, gee die volgende wenke:

- Moenie aanlyn of telefonies persoonlike inligting soos jou ID-nummer of bankbesonderhede met enigiemand deel nie.

- Moenie op skakels klik of aanhegels in e-posse of teksboodskappe (ook WhatsApp) van onbekendes oopmaak nie. Selfs al ken jy die persoon en jy is onseker, bel eerder en vra.

- Sodra iemand geld of privaat inligting vra, verbreek kontak.

- Gebruik sterk wagwoorde (baie letters en syfers) en hou dit privaat. 'n Wagwoordbestuurder-app kan help om sterk wagwoorde te genereer en dit te onthou.

- Hou die sagteware op jou rekenaar en telefoon op datum om te verseker dat jy teen nuwe bedreigings beskerm is.

- Verander gereeld jou bank-app se wagwoord en moenie die ou wagwoord weer gebruik nie.

- Verifieer altyd 'n maatskappy se bankbesonderhede voordat jy 'n betaling maak.

Anné Verhoef, direkteur by die NWU se afdeling vir Kuns-

matige Intelligensie, sê dis ook belangrik om waaksaam te wees as dit by KI-apps kom, wat toeneemend gewild is.

“Die meeste KI-apps wat gratis beskikbaar is, het nie baie goeie sekuriteitsstelsels in plek nie. Dit is gewoonlik eers wanneer jy 'n betaalde weergawe gebruik dat jy byvoorbeeld die verstelling kan maak dat jou inligting nie gedeel mag word nie.”

Anné voeg by dat jy dan kan aandui of dié app jou inligting mag gebruik. Gewoonlik vra die KI jou inligting sodat dit daaruit kan leer en verbeter.

“Indien jy dus wel sensitiewe inligting op KI-apps wil plaas (byvoorbeeld vrae oor jou finansiële beplanning), moet jy eerder die betaalde weergawe gebruik.”

Moenie die volgende op KI-apps deel nie:

- Persoonlike inligting soos jou naam en van, jou adres, e-posadres en ander kontakbesonderhede, jou ID en ander persoonlike inligting.

- Persoonlike finansiële inligting soos jou inkomste, rekeningnommers, ens.

- Persoonlike inligting van jou familie en vriende.

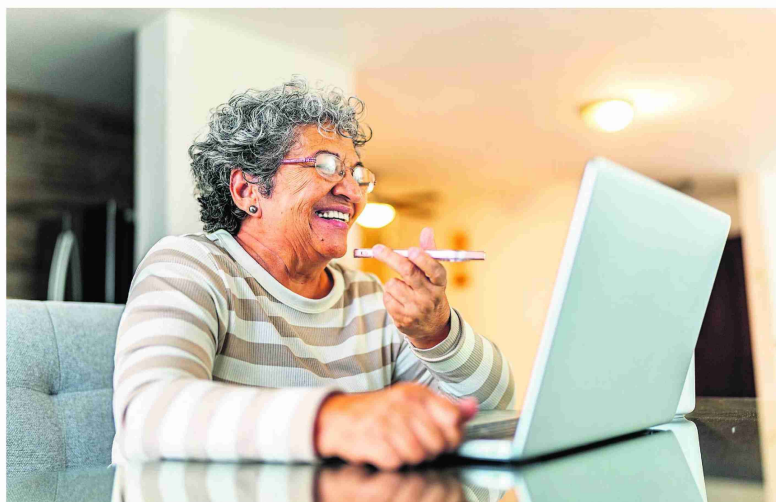
- Inligting oor jou ras, geslag, politieke en geloofsoortuigings, en mediese data.

- Inligting oor moontlike regsake wat steeds aan die gang is, sowel as persoonlike kontrakte en ooreenkomste.

- Onvanpaste inligting soos haatspraak, onwettige aktiwiteite en inhoud wat die landswette oortree.

Veiligheidsmaatreëls aanlyn

Dylan sê jy kan begin deur slegs die amptelike webtuistes of apps



Maak seker jy gebruik betroubare apps om jouself te beveilig teen swendelaars.

Foto: GETTY IMAGES

van jou bank en winkels te gebruik. “Kyk vir die hangslot-simbool in jou webblaaier en kyk vir webtuistes wat begin met https (die s staan vir *secure*).

“Maak ook seker dat jy nie openbare Wi-Fi gebruik met jou bank of inkopies-app nie.”

Hy beveel aan dat jy die waarskuwings (*alerts*) op jou bankrekening stel sodat jy weet wanneer geld bestee word. Dit sal ook van hulp wees as jy die bank se hulplyn as kontak stoor.

Met KI moet jy onthou dat

daar nie 'n mens aan die ander kant is nie. “Wanneer 'n KI-app met jou in gesprek tree, kan dit vinnig al jou inligting wat vrylik beskikbaar is, byvoorbeeld op Facebook, nagaan en deel maak van die gesprek,” sê Anné.

Hy sê dit leer jou ook só ken en maak dan die gesprek so persoonlik moontlik.

“Dit kan baie gou baie oortuigend lyk of jy werklik met 'n persoon gesels wat jou verstaan en jou goed ken. Wees bedag daarop dat dit steeds 'n rekenaar

is wat met jou kommunikeer en bloot daarin slaag om patrone korrek te identifiseer en toe te pas om so menslik as moontlik voor te kom.

“Moenie toelaat dat die KI-toepassing jou vertrouwe wen om uiteindelik jou persoonlike finansiële inligting te deel nie.”

Hy voeg by dat dit belangrik is om mooi te dink oor watter KI-apps jy gebruik.

“Gebruik eerder 'n bekende toepassing soos ChatGPT as die nuwes wat elke dag verskyn.”

Wees op die uitkyk vir dié gevaartekens

Swendelaars probeer om al hoe meer hulself geloofwaardig te laat kyk.

Volgens Dylan moet jy waaksaam wees vir die volgende:

- E-posse of teksboodskappe wat sê “dringend” of vra vir geld of geskenkbewyse.

- Boodskappe wat sê jou reke-

naar het 'n virus – moenie daarop klik nie!

- Vreemdelinge wat aanlyn geld vra of pryse aanbied.

- Oproepe of e-posse wat voor-gee om van die SAID, mediese fonds, of jou bank te wees en jou persoonlike inligting vra.

- Spelfoute of swak taalge-

bruik – dit beteken dikwels dit is 'n swendelaar.

- Vals kompetisies vanaf bekende winkels of handelsname word dikwels gebruik om data in te win.

Dié inligting word later vir bedrog gebruik of jou persoonlike inligting word aan datamakelaars verkoop.