Online identity verification

Introduction

Users can show themselves as an online profile on e-commerce sites, wechat, or LinkedIn, and by using these profiles, users can set up a variety of online social relationships in a well-liked manner. Users may appear under multiple identities on internet social networks because of their open nature. Therefore, from the perspective of security and privacy, confirming users' identities is one of the most important challenges. Users must authenticate their identities to one another in order to establish any social relationships in an authenticated manner. This is necessary to prevent the development of fraudulent communications. The way users' identities are now verified in online social networks is insufficient to stop the creation of fictitious accounts, which allows a single user to represent his identity across several profiles without the use of a reliable identity verification system. The attackers can construct a wide range of phony profiles thanks to this vulnerability in order to attack the online social system. For instance, profile hijacking allows an attacker to take over certain existing profiles on a e-commerce and social network website. The adversary uses a profiling attack to try and learn more about your online e-commerce network usage. Another harmful act that targets multimedia material like transactions, products, etc. The attack is therefore classified as a reverse engineering attack, in which the attacker tries to coerce the victim into openly communicating with the hacker either by telling the customers to send them money inform of buying a product which they will never deliver. One of the most common and effective attacks against e-commerce network platforms is identity attack, in which the adversary attempts to gain the trust of a particular user’s account or community by using several fake accounts to impersonate the identities of real users across online networks. Unfortunately, platforms for online e-commerce networks lack reliable authentication methods for defending users' profiles against identity attacks in Africa, with the exception of more conventional methods like CAPTCHA, which are regularly answered by devoted staff.

For thieves who target online e-commerce networks, creating phony profiles there has become an appealing strategy privacy and security. For instance, scammers frequently employ phishing techniques to get consumers to accept phony friend requests, false supplier adverts, customer identity. The e-commerce website to execute spying and eavesdropping activities, criminals can construct false profiles by either replicating the presence of a certain account or by generating phony accounts from nothing. According to a statistical analysis by African cyberthreat assessment report, fraudulent profiles of Southern part make up between 1% and 45.2% of all newly established accounts. South Afirca is the leading country with 48.2% e-commerce threats followed by Botswana with 15%, Zambia with 19% and the rest of southern part including Zimbabwe with 1% as in 2021 african cybersecurity report.

1. commerce applications login

Every new user is required to have

Ecommerce applications - login

Ecommerce shop owners - proof of reality

Parcel Delivery - id verification and code