

South Africans warned not to post vaccination cards online

According to Anna Collard, senior vice president of content strategy and an evangelist at KnowBe4 Africa, cybercrime organisations are using bots and artificial intelligence (AI) to sift through social media profiles to capture personal information (such as your ID number on your vaccination card) that they can use to send you personalised phishing attacks, impersonate you on other sites, or sell your information to professional criminal organisations.



Source: [Pixabay](#)

“It’s a disappointing reality when you can’t even post a selfie of yourself with your vaccination card without fear of having that information stolen,” says Collard. “The problem is that there are cybercriminals and tools out there designed to capture your personal information. From full names to ID numbers to other vital personal facts and stats, your personal details can put you and your identity at risk.”

One of the ways in which this information can be used is to create believable phishing emails that leverage the details captured, which makes it far easier for people to fall for them. Phishing emails have come a long way from the days of poor spelling and obvious scams. Now they use research, fear tactics and emotional messages to get people to make knee-jerk reactions that can cost them money, reputation and livelihoods.

“An email that knows you’ve just been vaccinated but preys on your fears around travel, or perhaps around side-effects, may ask you to use your healthcare insurance details to log into a fake website trying to capture more of your details,” says Collard.

Roll out of digital vaccination certificates imminent

10 Sep 2021





There are smart algorithms and intelligent tools designed to pick up on the information that's important in your life and use it against you. It's important to be aware of this risk and to mitigate it by blacking out personal information on your vaccination card before posting it on public platforms. Identity theft has increased by 337% according to the Southern African Fraud Prevention Service (SAFPS). People are at risk across the board, and identity theft is one of the most complex attack vectors to manage and recover from. Many people have been blacklisted or lost vast sums of money because someone else is using their details to rack up debts.

"Identity theft is a pandemic on its own," says Collard. "It can change a person's life drastically, and leave them destitute, or constantly fighting to prove that the bills coming to their name are not theirs. Even with extensive proof, it's hard to minimise the impact of an identity theft scam. So, the best first line of defence is to minimise the amount of information about you on the internet."

"Phishing is a profitable business, which makes it a sophisticated one," concludes Collard. "From personalised phishing emails to social engineering to fake emails pretending to be from your company, or a service provider, scammers are smart in their approaches and succeeding in their attacks. With the information available on your vaccination card, someone can pretend to be from your HR department asking you to change your login details by following a link, and you'll trust it because who doesn't trust HR? It's a complex world, so keep your information close to your chest and off the internet."

For more, visit: <https://www.bizcommunity.com>