Bank Zero
mutual bank
be the change

29 March 2023

Bank Zero has Zero phishing victims

Hot on the heels of its announcement that its customers have experienced Zero card fraud, Bank Zero is today announcing a second "Zero milestone". In the 18 months since its launch, not one of its customers has fallen prey to the phishing scams that are taking in people and businesses all around the world.

Kaspersky, a leading security software company, says that phishing attempts more than doubled to over 500 million in 2022, as compared with 2021. According to Fortinet, South Africa was one of the top 20 countries in terms of phishing attacks in 2022. This figure is supported by Surfshark research, which indicates that South Africa has the sixth highest cybercrime density in the world.

Michael Jordaan, chair of Bank Zero, says that the stakes have been raised significantly since the Banking Ombud recently ruled that customers are responsible for losses if they divulge sensitive authentication details.

"This is a big wake-up call for consumers. Many consumers assume they have chargeback rights, but this ruling means they are in fact liable for the full loss if they act carelessly," Jordaan says. The losses referred to are the result of phished secure card transactions, or transactions after a customer's banking profile was compromised.

Jordaan explains that while they are not technologically complex, phishing attacks are highly effective because they use the most sophisticated social engineering techniques, backed up by slick and well-resourced teams. The aim is to earn customers' trust and then get them to reveal login details and/ or one-time passwords, followed by the rapid emptying of all accounts.

Yatin Narsai, CEO of Bank Zero, says: "We all know somebody who has fallen prey to phishing—these criminal networks are extremely devious and effective. With that in mind, when we designed Bank Zero we assumed that the customer will indeed reveal all their personal information, and we worked out a way to still protect them. I am delighted to say that we are succeeding—and that's something which not many other banks in the world can claim."

Bank Zero protects its customers from phishing by applying two highly effective principles. The first principle is to ensure that the correct person is transacting. Banking is only permitted via the Bank Zero app on a mobile device—Internet banking, which can easily fall prey to keyloggers, is not supported. When registering on the app, the customer uploads their facial biometrics. At the same time, the app registers the mobile device, and will only permit access to that specific profile from this device—anyone attempting to access that profile from an unregistered device will have to be authenticated using the biometrics previously provided.

"It's all about double checking that the person transacting is the authorised person for that account," Narsai says. "Businesses small or large enjoy the same protection: staff acting on behalf of the business as Authorisers, Mandated Officials or Relationship Bankers do so under the same rules of biometrics and safe pairing. This means businesses are also protected against phishing, and are no longer exposed to 'unknowns' working on PCs and laptops that are vulnerable to key loggers and prone to failures from clumsy digital certificates."

The second principle is to provide comprehensive notifications of all actions and/or transactions. These notifications are provided via the app and e-mail, with geolocation included for every sensitive action, such as the addition of a new beneficiary to a business account or the pairing of a new device.

"This comprehensive notification of all actions and transactions, including geolocation when they are risky, provides a high level of security. When it's combined with the rigorous confirmation of the customer's identity via facial biometrics, you get a system that is well defended, even if the log-in details and so on have been divulged," Narsai explains. "And, best of all, it's not a technologically complex solution, the perfect antidote to the social engineering that phishers use. It's deceptively simple but highly effective.

"Security is critical always, but it's especially vital in tough economic times when fraud rises dramatically, and customers are more vulnerable to scams."