New phishing campaign targets Monzo online-banking customers

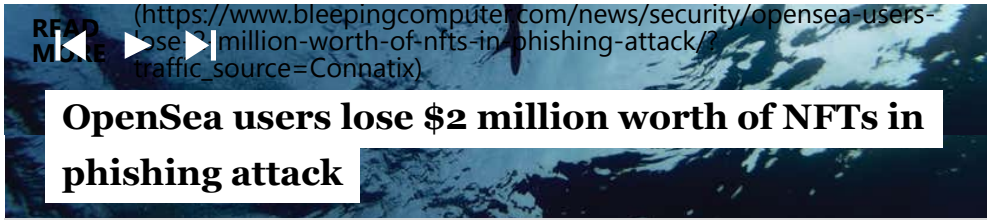
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

February 20, 2022 10:09 AM **0**

Users of Monzo, one of the UK's most popular digital-only banking platforms, are being targeted by phishing messages supported by a growing network of malicious websites.

Monzo is a 100% online banking platform with over four million customers and among the first to challenge the traditional financial managing system.

The mobile-only platform offers a feature-rich app, debit Mastercards, and a comprehensive yet not completely flawless (https://www.bleepingcomputer.com/news/security/monzo-asks-clients-to-reset-pins-after-exposure-to-employees/) fraud-detection system.



According to a report by security researcher William Thomas, there's an ongoing phishing campaign targeting users of Monzo and attempting to steal their accounts.

The banking platform also posted on Twitter to warn its customers about the signs of fraud and what not to do when receiving a message that appears suspicious.

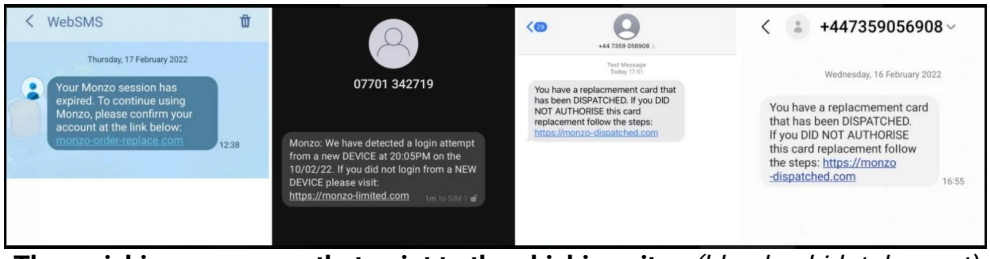
5:39 PM · Feb 16, 2022

Read the full conversation on Twitter

42 Reply Share

Read 10 replies

In a new report (http://blog.bushidotoken.net/2022/02/mobile-banking-phishing-campaign.html), Thomas explains that the phishing process begins with the arrival of an SMS text showing Monzo as the sender's name, asking the recipient to tap the provided link to reactivate their session or verify their account.



The smishing messages that point to the phishing sites *(blog.bushidotoken.net)*

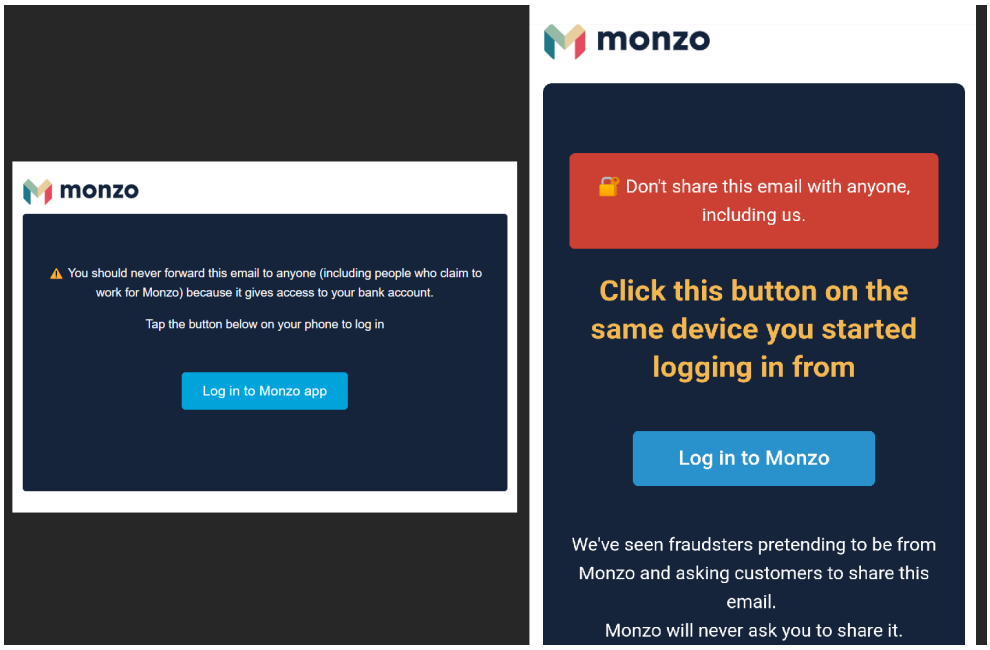
The users are taken to a phishing site that displays a fake email login form and then requests information about their Monzo account, including full name, phone number, and the Monzo PIN.

If these details are provided, the threat actors now have everything needed to begin taking over victims' Monzo accounts.

When installing the Monzo app on a new device, like the threat actor's smartphone, the service sends a device verification link for the first login to the user's email address.

As the threat actors now have access to victims' email accounts, they can click on this "golden link" and verify their device, giving full access to the Monzo account.

The severity of gaining access to this link is illustrated in the emails sent by Monzo, who warn that the link should never be shared with other people.



If the email account is protected by 2FA, Thomas believes the adversaries can likely overcome it with additional social engineering steps or by employing OTP stealing bots.

Setting up phishing sites

Thomas says the threat actors are using the Cazanova Morphine kit to create the Monzo phishing landing page, with some examples domains listed below:

- monzo-notice[.]com
- monzo-online-support[.]com
- monzo-check[.]com
- monzo-card-support[.]com
- monzo-replacement[.]com
- alert-monzo[.]com

Examples of Monzo phishing pages
Source: blog.bushidotoken.net

In addition to the above, the researcher also noticed four domains on the same ASN, which targeted users of Revolut, a popular online payments service.

- revolut-cancel-support[.]com
- revolut-cancellation[.]com
- revolut-cancel-online[.]com
- login-revolut-resolve[.]com

"Research into the domain itself via URLscan.io uncovered 33 other identical sites, dating back to 11 November 2021," details Thomas in his blog post.

"All 34 domains were hosted on the same three CIDRs in Russian IP space with NForce Entertainment (AS43350). Interestingly, the Monzo-themed domains also used two Guangdong-based Registrars (Eranet and NiceNic)."

Number of phishing domains *(blog.bushidotoken.net)*

Mixing Chinese registrars and Russian IP addresses makes attribution hard and complicate take-down actions, extending the uptime of the phishing sites.

Don't tap any links

When Monzo wants to inform users about anything, it uses built-in app notifications or the account portal on the official website.

Monzo doesn't use SMS to send notifications, and the platform would never urge users to follow any links from outside the app.

If you've tapped on these links and provided any login details to the actors, reset your account passwords immediately and activate MFA on both your email and Monzo accounts.