BIZCOMMUNITY

# Cryptoscams target MetaMask users for seed phrases

With the use of digital currency becoming more mainstream, so cryptocurrency-related phishing scams are on the increase.

Image source: © welcomia – 123RF.com

Kaspersky reported its products detected and prevented over 460,000 crypto-related phishing attacks in 2021 overall, the company's researchers reported over 100,000 such attacks just in two and a half months of 2022.

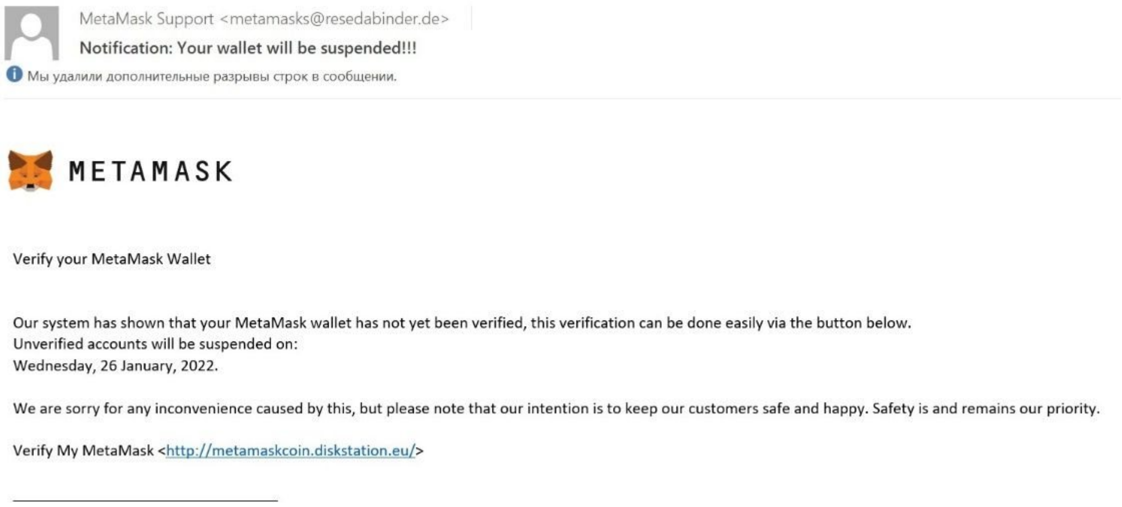
Kaspersky experts are currently seeing intensified scamming activity targeting MetaMask crypto wallet users, with more than 4,000 MetaMask-related phishing attacks detected in 2022 so far. By distributing phishing pages that show a warning of a potential account block, fraudsters can collect crypto investors' secret seed phrases and gain access to the victim's wallet, credentials and savings.

3 key reasons cybersecurity will never be fully automated

Amir Kanaan 14 Feb 2022

With the rise of NFTs throughout the past year, MetaMask gained users' attention since it allows users to authorise their Ethereum accounts by interacting with NFT marketplaces. In the fraud campaign spotted by Kaspersky, victims received an email with a warning that their account will be blocked. Users are asked to verify their account by clicking on the phishing link to prevent that from happening.

## An example of fake email from MetaMask:



MetaMask Support <metamasks@resedabinder.de>
Notification: Your wallet will be suspended!!!
Мы удалили дополнительные разрывы строк в сообщении.

METAMASK

Verify your MetaMask Wallet

Our system has shown that your MetaMask wallet has not yet been verified, this verification can be done easily via the button below.
Unverified accounts will be suspended on:
Wednesday, 26 January, 2022.

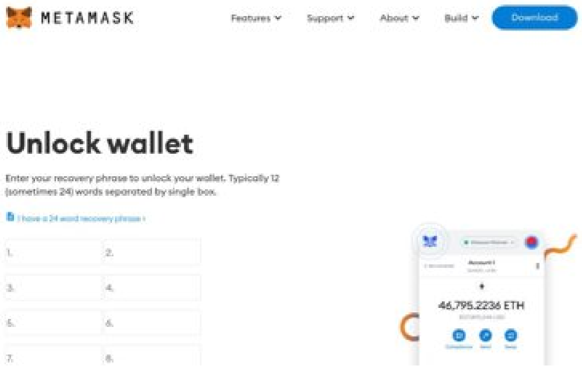
We are sorry for any inconvenience caused by this, but please note that our intention is to keep our customers safe and happy. Safety is and remains our priority.

Verify My MetaMask <http://metamaskcoin.diskstation.eu/>

click to enlarge

The phishing page mimics the original MetaMask design, using its logo and a domain that not only includes the “MetaMask” name, but also the names of other brands. To unblock the wallet, fraudsters ask for the victim’s personal seed-phrase (a secret phrase of 12, or 24 words) which ensures the security of the wallet, along with a password and private key. Once the user shares this secret phrase, they’re redirected to the real MetaMask website, however, by then, their account and all of their savings will be in the scammer’s hands.

## An example of a phishing page mimicking the MetaMask ‘Unlock wallet’ page:



Unlock wallet

Enter your recovery phrase to unlock your wallet. Typically 12 (sometimes 24) words separated by single box.

I have a 24 word recovery phrase ›

1. 2.
3. 4.
5. 6.
7. 8.

“While most crypto investors value the safety of their wallet’s password, some, especially those new to the world of cryptocurrencies, underestimate the importance of protecting their seed phrase. Overly trusting users might end up losing access to their wallets and, as a result, lose their cryptocurrency. Scammers have learned how to craft phishing pages allowing them to get access to a victims’ savings, but it is possible to recognise these pages. The MetaMask seed phrase theft campaign has all the common signs of fraudulent schemes, which can be spotted. Grammar, spelling mistakes and wrong domains always give the scammers away,” comments Roman Dedenok, security expert at Kaspersky.

Kaspersky records over 2m phishing attacks in SA in H1 2021
14 Sep 2021

## To guard yourself against cryptoscams, Kaspersky experts also recommend:

- **Being vigilant.** Unexpected messages about the loss of money and accounts, or transfers, gifts, and winnings are almost always a trick.
- **Always check links carefully.** It’s best not to click on any links in messages from internet service providers at all — instead, type the address of the service into your browser.

- **Install a reliable antivirus solution** to protect yourself against phishing. For example, Kaspersky Internet Security‘s built-in antiphishing and antifraud modules warn users about potentially dangerous sites before it’s too late.