Distinguishing phishing messages warning of technical problems from legitimate technical issues

10/25/2024 12:33 am EDT

A common tactic used by phishing attackers is warn users of an urgent technical issue with their wallet or exchange account that purportedly requires the users' quick action to avoid a loss of funds.

In almost all cases, this warning is bogus and designed to spur quick action from a user, without giving them adequate time to think critically about whether the message is legitimate. The actions the user performs as a result of following directions from the phishing message lead to a loss of funds. The phishing message itself is harmless **if users ignore it or do nothing.**

There never going to be an instance where you need to take action quickly to avoid your wallet or account being compromised. It is safe, if you do nothing, and take time to closely vet the authenticity of any message received.

This includes taking time to assess whether or not you're on the real website of the exchange or web wallet you are using, whether or not you downloaded a fake or malicious wallet application, assessing whether you are actually speaking to 'customer support' or assessing whether the email you just received from 'Ledger' warning about technical issue is actually from Ledger or not (hint: it's not).

Carefully vet any email messages by checking the email headers. Verify you have an authentic version of any wallet software you downloaded from your computer and that it came from the real website, and you can further verify the checksum . Don't search for metamask in google, and especially don't click on a metamask ad you see. Instead, manually type metamask.com into your browser (if that's the website you want to navigate to) or better yet, use a bookmark.