

[Click Here](#)































A new Ledger phishing campaign is underway that pretends to be a data breach notification asking you to verify your recovery phrase, which is then stolen and used to steal your cryptocurrency. Ledger is a hardware cryptocurrency wallet that allows you to store, manage, and sell cryptocurrency. The funds in these wallets are secured using 24-word recovery phrases or 12 and 18-word phrases generated by other wallets. Anyone who knows your Ledger recovery phrase can use it to access the funds within the wallet. Therefore, recovery phrases must always be kept offline and never shared with anyone to prevent cryptocurrency funds from being stolen. Fake data breach notifications Ledger has long been a target of phishing campaigns that attempt to steal users' recovery phrases or push fake Ledger Live software to steal information. These campaigns became significantly worse after Ledger suffered a data breach in 2020 that exposed its customers' names, addresses, phone numbers, and email addresses. However, over the past few days, multiple people have notified BleepingComputer or shared on X that they received a Ledger phishing email that pretends to be a new data breach notification. The phishing emails have the subject of "Security Alert: Data Breach May Expose Your Recovery Phrase" and appear to be from "Ledger