THE TIMES OF INDIA

Research company warns of WhatsApp message scam; here's simple tip to check if the message you received is fake

The landscape of WhatsApp scams is changing swiftly, especially for business users. Cybercriminals are now infiltrating accounts to distribute harmful files, masquerading as urgent financial documents. By exploiting trusted contacts, these scams create a false sense of security around attachments. Sophisticated malware can even disable antivirus software using weak drivers prior to its attack. The safest way to combat these threats is by confirming messages through alternative channels.

WhatsApp scams are on a rise and recently cybersecurity firm Quick Heal Technologies also issued a warning about the same. Quick Heal warned that WhatsApp-based malware and scams are evolving rapidly. The company highlighted that scammers are mainly targeting finance teams, senior executives, chartered accountants and business users across the country. Unlike the regular scam messages, these messages come from unknown numbers and the WhatsApp scam campaign mainly depends on something far more dangerous: your own trust in the people already in your contact list. The company Once a WhatsApp account is compromised, attackers use it to forward malicious files to the account holder's existing contacts. Because the messages appear to come from a known colleague, client, friend or business associate, recipients may be more likely to open the attachment without independently verifying it.

WhatsApp scam: Why it is harder to spot

Many of us are trained to be suspicious of messages from strangers. However, this campaign flips that logic entirely. Once an attacker manages to compromise someone's WhatsApp account, then they don't send messages from a random number instead they use the compromised connection to forward the malicious files directly into the contact list of the victim. So, the message when appears to come from a genuine colleague, client, friend, or business associate, the recipients are more likely to open it and click on the attachment without any second thoughts.

In order to further worsen the situation, the attackers rely heavily on finance and compliance-themed filenames which are made to create a sense of urgency. The attackers disguise the malicious files under the names like "Financial Report," "Account Statement," "Outstanding Payment List," and "Debt Confirmation." In some cases they move a head further and try to impersonate urgent communications from institutions like the Reserve Bank of India or the Ministry of Corporate Affairs, pressuring recipients into opening the file immediately out of fear of missing something important or official.

How the WhatsApp scam attack actually works

The campaign has evolved through several stages. It initially spread through malicious Visual Basic Script files, or .vbs files, sent directly over WhatsApp.

Attackers later shifted to ZIP archives containing an executable file paired with a supporting malicious component, using a technique called DLL sideloading to trick a legitimate-looking program into secretly loading harmful code instead.

One particularly sneaky detail involves .img and .vhd file types, which most people would never think to be suspicious of. These aren't ordinary photos or documents when double-clicked, Windows treats them like a newly connected disk drive, which can quietly expose an executable file and other hidden malicious components. In short, an unexpected .img or .vhd attachment deserves exactly the same caution you'd give an unfamiliar .exe file.

In its most advanced form, the malware also uses a technique known as Bring Your Own Vulnerable Driver, or BYOVD, which involves installing legitimate, digitally signed drivers that happen to contain known security flaws. Attackers exploit those flaws to quietly disable or weaken antivirus protection before deploying their actual payload.

Once defenses are down, the campaign installs remote monitoring tools configured with password protection and self-defense mechanisms of their own, making them notably difficult for victims or IT teams to spot and remove. From there, attackers can gain hands-on, persistent access to the infected system running commands, moving files, and monitoring activity as if they were sitting at the keyboard themselves.

Perhaps most concerning is the campaign's ability to self-propagate: an infected system can use an active WhatsApp Web session to automatically forward the malicious file to the victim's own contacts, turning a single compromised account into a chain reaction that spreads through entire professional and social networks.

The simple tip to check if a WhatsApp message is fake

Given how convincing these messages can look, the single most reliable way to verify whether an unexpected file is genuine is refreshingly simple: don't reply in the same chat. Instead, contact the sender through a completely separate channel such as a phone call, a text message, or an in-person conversation and ask them directly whether they actually sent it. A genuine contact will be able to confirm or deny it instantly, while a compromised account obviously can't answer for itself.

Beyond that, it's worth periodically checking WhatsApp's Linked Devices setting under Settings, logging out of any web or desktop sessions you don't recognise or no longer use, and treating any unsolicited file even from a known contact with a healthy dose of suspicion before opening it. If you ever suspect your

own account has been compromised, log out of all linked devices immediately, disconnect the affected device from the internet, and warn your contacts not to open anything sent from your number until the issue is resolved.

A few other simple habits worth building

* Always be careful before accessing unexpected attachments. Be suspicious before clicking on attachments that even come from the known contacts especially if the file name try to create some kind of urgency.

* Keep an often check on WhatsApp Linked Devices and log out of any session you don't remember or recognise.

* Also avoid clicking and downloading the unfamiliar files that you were not expecting.

* If you think your own account may be compromised, log out of all linked devices right away, disconnect your device from the internet, and give your contacts a heads-up not to open anything sent from your number until things are sorted out.