# Taking Action Against Malicious Accounts in Iran

By isolomons

Published: 2024-08-23 · Archived: 2026-04-06 00:31:10 UTC

As part of our regular updates on notable threat disruption efforts, we're sharing our most recent insights into a small cluster of likely social engineering activity on WhatsApp that our security teams blocked after investigating user reports. This malicious activity originated in Iran and attempted to target individuals in Israel, Palestine, Iran, the United States and the UK. This effort appeared to have focused on political and diplomatic officials, and other public figures, including some associated with administrations of President Biden and former President Trump.

Our investigation linked it to APT42 (also known as UNC788 and Mint Sandstorm), an Iranian threat actor known for its persistent adversarial campaigns using basic phishing tactics across the internet to steal credentials to people's online accounts. We have previously shared our threat research related to APT42 targeting people in the Middle East, including Saudi military, dissidents and human rights activists from Israel and Iran, politicians in the US, and Iran-focused academics, activists and journalists around the world.

These accounts posed as technical support for AOL, Google, Yahoo and Microsoft. Some of the people targeted by APT42 reported these suspicious messages to WhatsApp using our in-app reporting tools. Those reported messages enabled us to investigate this latest campaign and link it to the same hacking group responsible for similar attempts aimed at political, military, diplomatic and other officials, as reported by our industry peers at Microsoft and Google.

The vigilance of these users to report the messages to us suggests that these efforts were unsuccessful. We have not seen evidence that their accounts were compromised. We have encouraged those who reported to us to take steps to ensure their online accounts are safe across the internet. Out of an abundance of caution and given the heightened threat environment ahead of the US election, we also shared information about this malicious activity with law enforcement and with the presidential campaigns to encourage them to stay cautious against potential adversarial targeting.

We continue to monitor information coming from our industry peers, our own investigations and user reports and will take action if we detect further attempts by malicious actors to target people on our apps. We strongly encourage public figures, journalists, political candidates and campaigns to remain vigilant, take advantage of privacy and security settings, avoid engaging with messages from people they don't know and report suspicious activity to us.

As a reminder, cyber espionage actors typically target people across the internet to collect intelligence, manipulate them into revealing information and compromise their devices and accounts. When we disrupt these operations, we take down their accounts, block their domains from being shared on our platform and notify people who we believe were targeted by these malicious groups. Learn more about our threat disruption efforts.

Source: https://about.fb.com/news/2024/08/taking-action-against-malicious-accounts-in-iran/