What is Online Account Hijacking?

Instances of account hijacking date back to 2014. During this time, the instant messaging software LINE had a system vulnerability that exposed users’ accounts to hackers. These hackers were then able to deceive the victim's family and friends in their contact list into purchasing prepaid cards. The situation continued until around 2016, when the vulnerability was eventually resolved. In 2017, scammers began hijacking users’ WhatsApp accounts to trick people into purchasing prepaid cards using similar deception methods. Later, WhatsApp introduced the “two-step verification” (now known as “two-factor authentication”) feature. This feature has gradually improved the situation and made it harder for scammers to hijack accounts.

In August 2023, a new account hijacking method involving phishing messages emerged and later transformed into "search engine optimisation poisoning" attacks—these attacks primarily target WhatsApp accounts, with a few cases involving Telegram and other online platforms.

Trick 1: Phishing text messages

- Scammers send phishing text messages with links to fake websites
- The fake websites obtain the user’s phone number and request the platform to issue a registration code to the user
- Scammers then get the registration code from the user
- Scammers then use another device to log into the user’s account Scammers exploit excuses like bank transfers and loans to defraud users' family and friends

Trick 2: Search engine optimisation poisoning attack

- Scammers create fake WhatsApp web login page
- Scammers advertise using the keyword “WhatsApp” on search engines
- When users enter the keyword “WhatsApp” in a search engine, the fake website will appear as the top ad
- When users click on the top ad, they are taken to the fake website, where they scan a malicious QR code, allowing scammers to obtain their connection information
- Scammers simultaneously log into users’ accounts through the online version of WhatsApp to deceive the users’ family and friends for money

Online account intrusions can have different causes. For instance, one may forget to log out of web-based messaging software after using a public computer, use malicious multi-account login tools, or have their electronic devices compromised by malicious software.

Scammers often use the excuse that online bank transfers exceed the limit and request contacts in the address book to help transfer money. They promise to repay the amount the following day, and the requested amount can vary from thousands to tens of thousands of dollars. Occasionally, there are also requests for large transfers.

Tips for avoiding online account hijacking:

Enable two-factor authentication

Regularly review the devices linked to your account and log out any unknown connected devices

Avoid disclosing passwords and verification codes casually or scanning QR codes without verifying

Set a strong password for your voicemail to prevent theft of voice one-time password

Avoid connecting to public Wi-Fi or logging into online accounts on public computers

Bookmark frequently used websites instead of relying solely on search engines for trustworthy results

Beware of any abnormalities in text messages and websites, such as misspelled domains or a mixture of traditional and simplified Chinese characters

If you receive a message from family or friend requesting help with bank transfers or remittances, always call to verify their identity and relevant request

If in doubt, use Scameter to assess for URLs, payment accounts, etc., or call 18222 for enquiries