From: threat-notifications@apple.com
Date: April 10, 2024 at 12:00:00PM PT
To: xxx
Subject: ALERT: Apple detected a targeted mercenary spyware attack against your iPhone

ALERT: Apple detected a targeted mercenary spyware attack against your iPhone

Apple detected that you are being targeted by a mercenary spyware attack that is trying to remotely compromise the iPhone associated with your Apple ID -xxx-. This attack is likely targeting you specifically because of who you are or what you do. Although it's never possible to achieve absolute certainty when detecting such attacks, Apple has high confidence in this warning — please take it seriously.

Mercenary spyware attacks, such as those using Pegasus from the NSO Group, are exceptionally rare and vastly more sophisticated than regular cybercriminal activity or consumer malware. These attacks cost millions of dollars and are individually deployed against a very small number of people, but the targeting is ongoing and global. Since 2021, we have sent Apple threat notifications like this one multiple times a year as we detect mercenary spyware attacks. Today's notification is being sent to targeted users in 92 countries, and to date we have notified users in over 150 countries in total. The extreme cost, sophistication, and worldwide nature makes mercenary spyware attacks some of the most advanced digital threats in existence today. As a result, Apple does not attribute the attacks or the notice you're receiving to any specific attackers or geographical regions.

Apple recommends that you immediately take these actions:

- **Enable Lockdown Mode right now** on your iPhone in Settings > Privacy & Security > Lockdown Mode. This feature takes only a moment to turn on and offers the **strongest protection for users like you** who are individually targeted by the most sophisticated digital threats.
- **Update your iPhone to the latest software version, iOS 17.4.1**, if you haven't already. We urge you to always update to the latest software as soon as it's available, as it

contains the latest security protections. To update, go to Settings > General > Software Update.

- **Update any other Apple devices you use** to the latest software. Enable Lockdown Mode on each Mac and iPad you use. You will only need to do this once for each device.
- **Update your messaging and cloud apps** to the latest available versions, as they contain the most up-to-date security improvements.
- **Enlist expert help,** such as the nonprofit, rapid-response emergency security assistance provided by the Digital Security Helpline, which is available 24 hours a day, seven days a week. For contact information, please see support . apple . com / 102174

Public reporting and research has shown that mercenary spyware attacks target users across modern computing platforms, including iOS and Safari as well as Google Android, Google Chrome, and Microsoft Windows, as well as a variety of messaging and cloud apps including iMessage and WhatsApp. These attacks are very well funded and are constantly evolving. If your device is compromised by a targeted mercenary spyware attack, the attacker may be able to remotely access your sensitive data, communications, or even the camera and microphone.

Some mercenary spyware attacks require no interaction from you, and others rely on tricking you into clicking a malicious link or opening an attachment in an email, SMS, or other message. These attempts can be quite convincing, ranging from fake package-tracking updates to custom-crafted, emotional appeals claiming a named family member is in danger. **Be cautious with all links you receive, and don’t open any links or attachments from unexpected or unknown senders.**

Mercenary spyware attackers are often persistent and will likely also try to target you through other channels, devices, and accounts not associated with Apple. Experts can provide the best advice for your specific circumstance, but if you are unable to reach an expert, as an additional precaution, **change your passwords for any sensitive websites and services** that you have accessed from your iPhone. If these attacks were successful in compromising your iPhone, they may have stolen your credentials for other services.

We are unable to provide more information about what caused us to send you this notification, as that may help mercenary spyware attackers adapt their behavior to evade detection in the future. Apple threat notifications like this one will never ask you to click any links, install an app or profile, or provide your Apple ID password or verification code by email or over the phone.

To verify that an Apple threat notification is genuine, sign in to appleid . apple . com. If Apple sent you a threat notification, it will be clearly visible at the top of the page after you sign in.

Please do not reply to this notification. We are unable to monitor responses to this message.

*Spaces inserted into all URLs to avoid creation of links. Please retype without spaces into a browser.

Copyright © 2024 Apple Inc.

All rights reserved.