



Phishing attacks that impersonate Apple

'Do your part – be cyber smart'

Phishing is undoubtedly still the world's most common cyber threat as an estimated three billion fraudulent emails are sent out every day to compromise sensitive information.


According to the 2021 edition of the Phishing Benchmark Global Report, one in every five phishing email recipients is prone to clicking on the enclosed malicious link. A key component of strong cyber security is being able to consistently detect and avoid phishing email attempts that land in your inbox^[1].

Introduction

Phishing refers to fraudulent attempts to obtain personal information from internet users, usually by email. Scammers use any means they can to trick you into sharing information or giving them money, including:

- Fraudulent emails and other messages that appear to be from legitimate companies, including Apple
- Misleading pop-ups and ads warning you that your device has security problems
- Scam phone calls or voicemails that impersonate Apple
- Fake promotions that offer free products and prizes
- Unwanted calendar invitations and subscriptions

SEE MORE

-  [Recognise and avoid phishing messages and other scams](#)

READ MORE

-  [Spear Phishing: Top Threats and Trends](#)
- [Examples of Common Phishing Emails](#)

DO MORE

-  [Protect your Apple ID and password](#)

Why would someone phish for your Apple ID?

Your Apple ID account contains all your contact, payment and security information. If hackers figure out your ID and password, they can dig even deeper to gain access to private information, either for their own corrupt uses or to sell on the black market. They also have access to all the documents, photos and files stored on your iCloud drive.

How does phishing work?

Anyone who uses the internet and macOS devices can be targeted by phishing scammers. Phishing scams normally try to:

- Infect your device with malware
- Steal your private credentials to gain access to your money or identity
- Obtain control of your online accounts
- Convince you to willingly send money or valuables

What are the main Apple ID phishing scams to be aware of?

Hackers are continually inventing new scams. The most enduring ones include:

- Apple ID order receipt: In this type of scam, you will receive an email that appears to be from Apple, stating that your ID has been used to make a purchase.
- Apple ID locked: This scam works in tandem with the fake receipt scam. A spoofed email will take you to a fake Apple page, which will show an 'unlock' button that requires you to divulge personally identifying information.
- Calendar invitation: You might receive a spam iCloud calendar invitation to a meeting or event from an unknown individual or group, often with promises of easy money.

How to protect yourself from Apple ID phishing scams

The best way to avoid becoming the victim of a phishing attack is to never click on a link or attachment in an email, text message, or pop-up unless you are a 100 percent certain that the message is real.

Also adhere to the following best practices:

- Never share your Apple ID password with anyone.
- Keep your operating system updated to the latest version.
- Keep your browsers updated. Also consider using Chrome, which has built-in phishing protection.