New Phishing Attack Disables iPhone Security: How to Protect Yourself?

A dangerous smishing campaign is targeting Apple iMessage users, using social engineering to disable the messaging service's built-in anti-phishing protection.

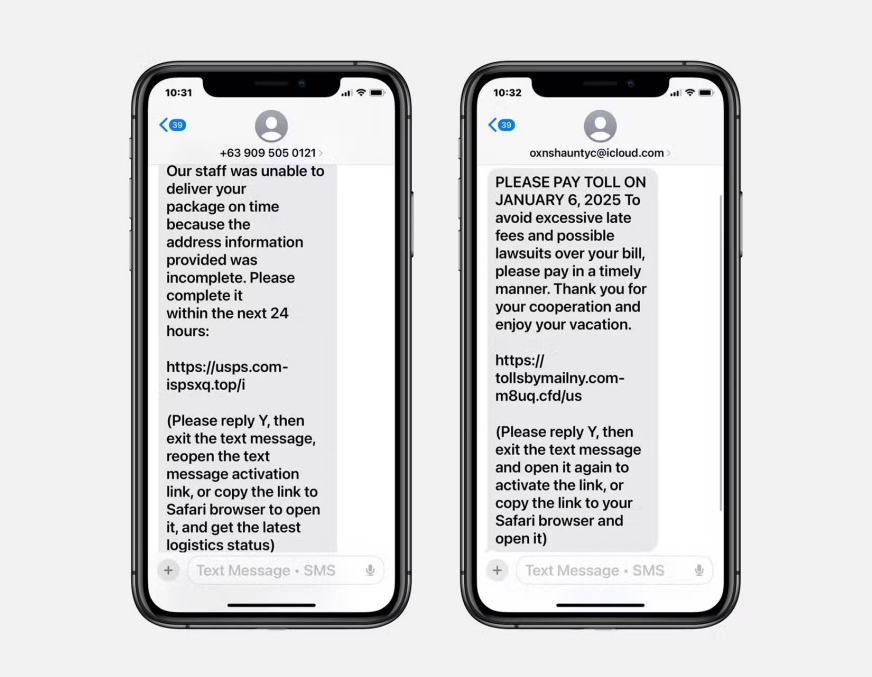
A dangerous smishing campaign is targeting Apple iMessage users, using social engineering to bypass the messaging service's built-in anti-phishing protections. The attack could expose millions of users, but you can stay safe by changing one security feature.

How this smishing attack disables iMessage security

Apple's built-in security protections block links sent via iMessage if the message comes from an unknown sender. This is to protect users from being exposed to malicious links. Cybercriminals have found a way to bypass this feature by tricking you into disabling this anti-phishing protection.

Attackers are sending fake alerts asking iMessage users to respond. These alerts take the form of fake shipping alerts or fake unpaid phone bills messages. The messages ask users to reply with 'Y' (yes) or 'N' (no) to accept or decline the delivery. Replying tells iMessage that you know the number, which enables the links.

Bleeping Computer reports that the message also includes instructions to *'Exit the text message, re-open the text message activation link, or copy the link into Safari'* to get the latest shipping status or pay tolls. The link takes users to a phishing site where their personal and financial information is stolen and then used for identity theft, credit card fraud, and other attacks.



Since people are used to replying STOP, YES, or NO to confirm or cancel valid appointments or alerts via text messages, attackers exploit this to trick users into thinking that replying is harmless. Even if you don't click on the link, replying tells the attacker that you are replying to a smishing message, making you a target for future attacks.

How to protect yourself

Don't respond to text messages from numbers you don't recognize, as this will disable Apple's built-in security protections, especially if you receive a text about an unexpected package or a fine you don't know about. Always treat links sent from unknown sources as malicious and don't click them. There are other ways to spot smishing messages, too.

If you're not sure if you have a package or fines and fees due but still want to check, close iMessage and open the company's official website in your browser. Contact their customer service to verify the information. You can also log into your account through their website or app. Don't access the website using a link from a message.

Be wary of messages that pressure you to act 'now,' offer a 'limited time offer,' or threaten you with negative consequences if you don't respond immediately. Most phishing scams are designed to get you to act before you think. This causes you to give them your information before you realize you've been scammed.

What to do if I have already sent a feedback?

If you responded or followed the attacker's instructions before realizing it was a scam, there are still ways to mitigate this.

First, block the phone number immediately to prevent them from sending you any more messages. Then, change your account password and enable multi-factor authentication (MFA).

If you have provided your financial information, call your bank immediately. The bank may freeze your account, cancel your credit card, and issue a new one.

If you have provided your personally identifiable information (PII) to a hacker that could be used for identity theft, you can contact TransUnion, Equifax, and Experian to freeze your credit. Doing so will prevent scammers from using your information to get loans or apply for new credit cards in your name.

Monitor your credit card and bank statements for suspicious transactions. You can also use identity theft protection services, including credit and PII monitoring. Advanced services include social media monitoring to find profiles created in your name and other services such as stolen data recovery assistance or ID recovery processes.

Also, be sure to download the latest software updates or patches for your device as soon as they become available, as they can help patch security holes and prevent future attacks.