

## New Mac phishing attack causes fake freezes to nab your Apple ID password

The attack attempts to get a user to enter their username and password by making them think their Mac is compromised.

By Roman Loyola Senior Editor, Macworld MAR 19, 2025 11:50 am PDT

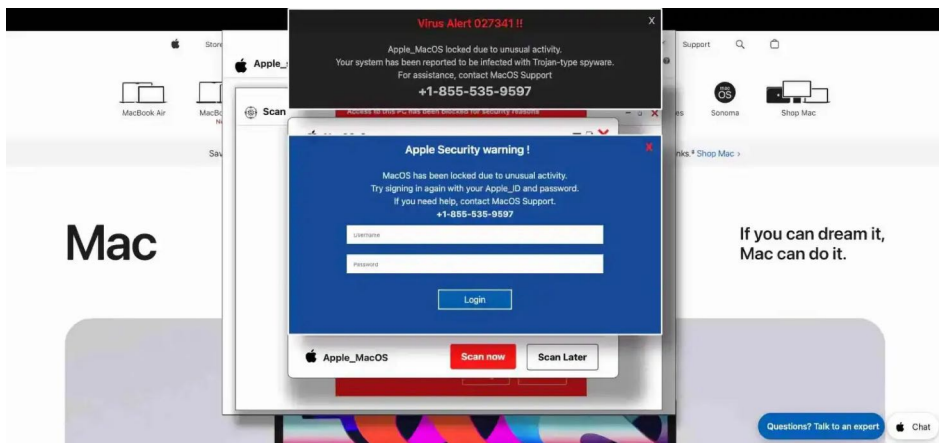


Image: IDG

LayerX Labs on Tuesday [posted](#) its finding on a new phishing attack that originally targeted Windows users, but now can be found on Macs. The phishing attack attempts to get a user’s username and password by making the user think their Mac is compromised.

The attack involves fake security warnings that appear while browsing the web. Alerts

appear stating that the Mac has been “compromised” and “locked” and the webpage appears frozen to heighten the sense of a compromise. A window appears prompting the user to enter their Mac’s username and password, along with a phone number to contact for “support.”



LayerX Labs

LayerX Labs provided a screenshot of the phishing attempt, though the attackers may modify the alert to make it more convincing. It has several telltale signs that it is fake, such as the design that doesn’t conform to Apple’s

style and the incorrect styling of the name “macOS.” Macworld called the phone number in the screenshot at 11 a.m. Pacific and got a message stating that they were not available and to call back between 8 a.m. and 5 p.m., so it’s a fake number that no one answers.

LayX Labs states that users run into these attacks inadvertently by making typos in the URLs entered into the browser. These mistyped URLs led users to compromised domain parking pages with the phishing attack.

The phishing attack initially focused on Windows users but Microsoft, Google, and Mozilla implemented new security features in their browsers that effectively blocked the attack. This caused the attackers to turn to Mac users.

## **How to protect yourself from web phishing attacks**

The easiest way to protect yourself from this attack is to verify the URL you have typed into your browser. Bookmark the sites you visit frequently so you don't have to type in the URL every time. In some instances, you can use a search engine, type the name of the place you want to visit, and then click on the link after looking at the URL it goes to. For example, type "Macworld" into the search engine you use, and then click on the link that's designated at [www.macworld.com](http://www.macworld.com). This way isn't as efficient but if you make a typo, you'll see it in the search and Google will steer you in the right direction.

Apple releases security patches through OS updates, so installing them as soon as possible is important. If you use a third-party browser, Macworld has several guides to help, including a guide on [whether or not you need antivirus software](#), a [list of Mac viruses, malware, and trojans](#), and a [comparison of Mac security software](#).

### **Author: Roman Loyola, Senior Editor, Macworld**

Roman is a Macworld Senior Editor with over 30 years of experience covering the tech industry, focusing on the Mac and other products in the Apple ecosystem. He is also the host of the Macworld Podcast. His career started at MacUser, where he received Apple certification as a repair technician (when Apple did that kind of thing). He's also worked for MacAddict, MacLife, and TechTV.