Gmail and Outlook users issued urgent warning over new login attack

metro.co.uk/2025/02/21/gmail-outlook-users-issued-urgent-warning-new-login-attack-22603205

Noora Mykkanen 21 February 2025

Noora Mykkanen

Published February 21, 2025 4:10pm **Updated** February 21, 2025 4:21pm

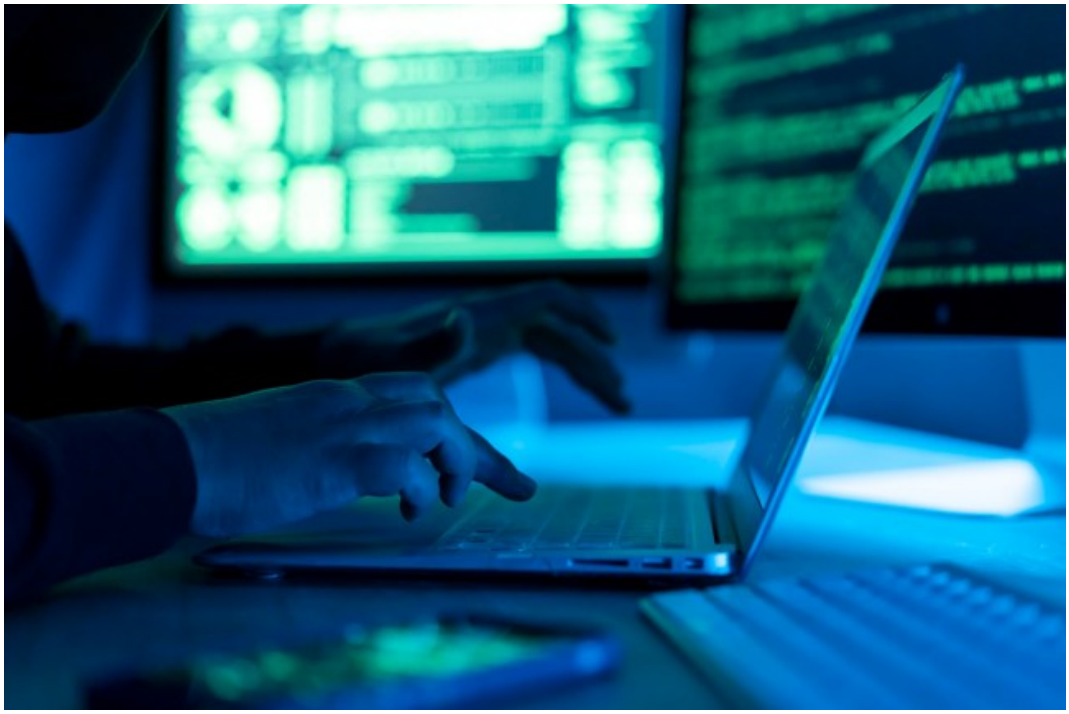
Cyber fraudsters have their eyes set on Gmail and Outlook accounts (Picture: NurPhoto/Getty Images)

Hackers are now targeting Gmail and Outlook accounts with an attack that can bypass even extra security layers.

Most of us check our emails regularly without paying much attention to them, so it is too easy to forget that they can be a convenient entry point for cybercriminals.

Now, a new sophisticated phishing attack that can even work around two-factor authentication (2FA) has been revealed by security experts, with Gmail, Yahoo and Microsoft accounts at particular risk.

Astaroth, the ominously named tool, can get around two-factor authentication through ‘session hijacking and real-time credential interception,’ SlashNext discovered.



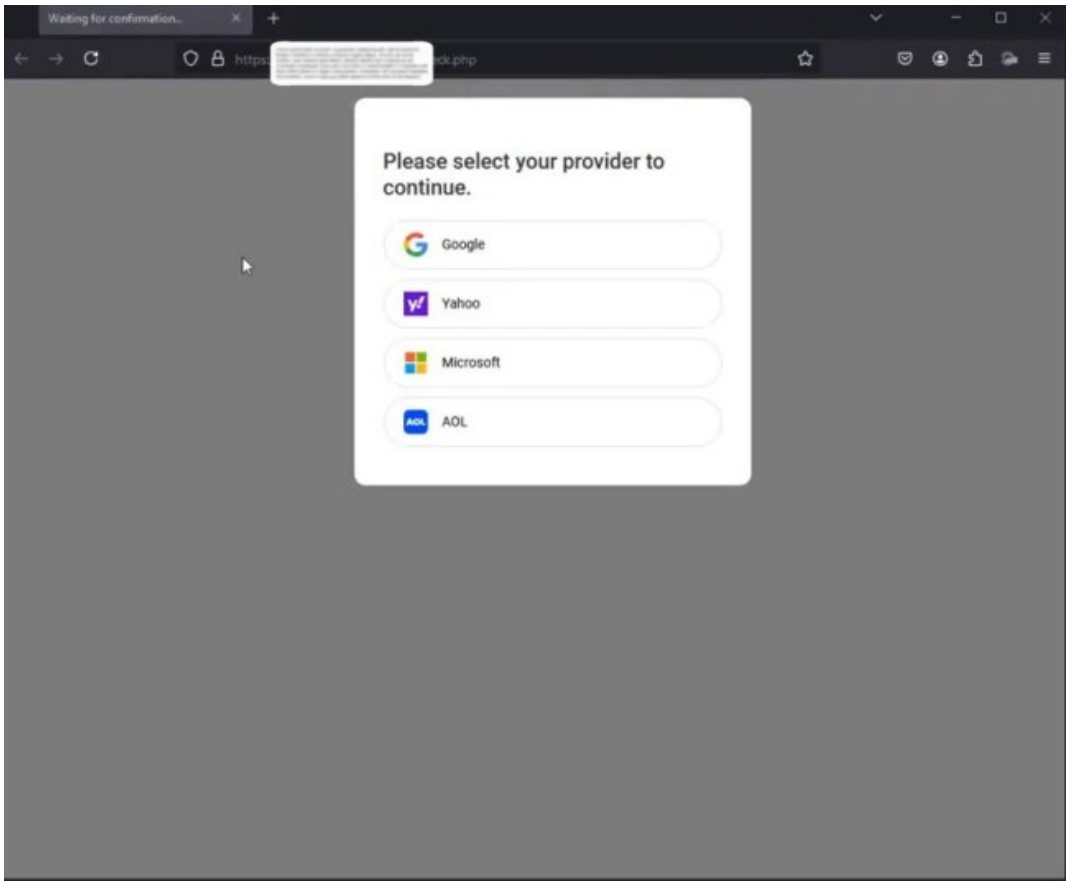
Even two-step authentication has nothing on the new phishing tool, Astaroth, that is being sold for $£1,580 in the dark web (Picture: Getty Images)

Here is how it works so you can avoid falling victim to the latest phishing attack as new tools are being developed.

How the Gmail and Outlook cyber attack works

With the new attack, hackers will first send a URL link to email users.

It will then redirect them to a malign server where a fake sign-in page will appear.

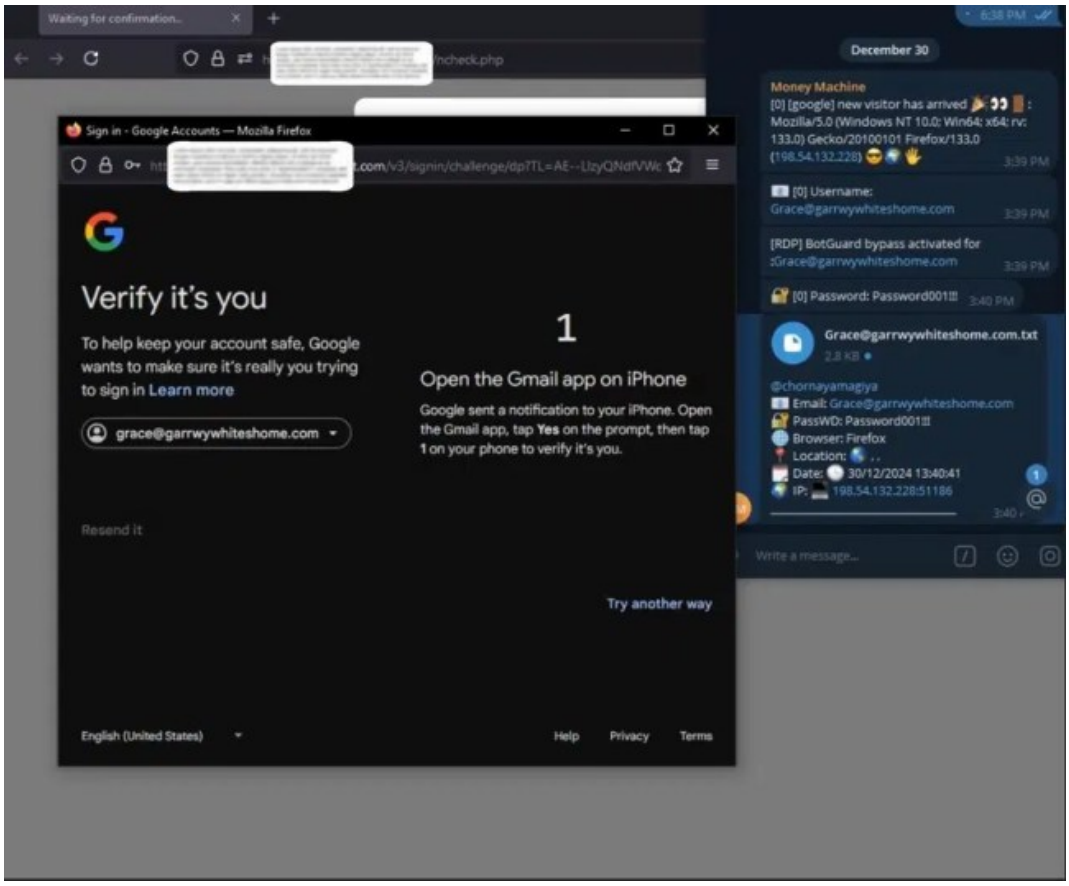


What the oblivious email users will see when login in using the malicious link (Picture: SlashNext)

To make matters worse, the fake page does not activate security warnings on the device.

Then the phishing tool becomes like a malign middleman between the user and the legitimate website. It captures sensitive data like username, password and IP address when the unaware victim enters their login credentials before forwarding them to the legitimate website server.

These details ‘allow attackers to replicate the victim’s session environment and reduce detection risks during login,’ SlasNext experts said.

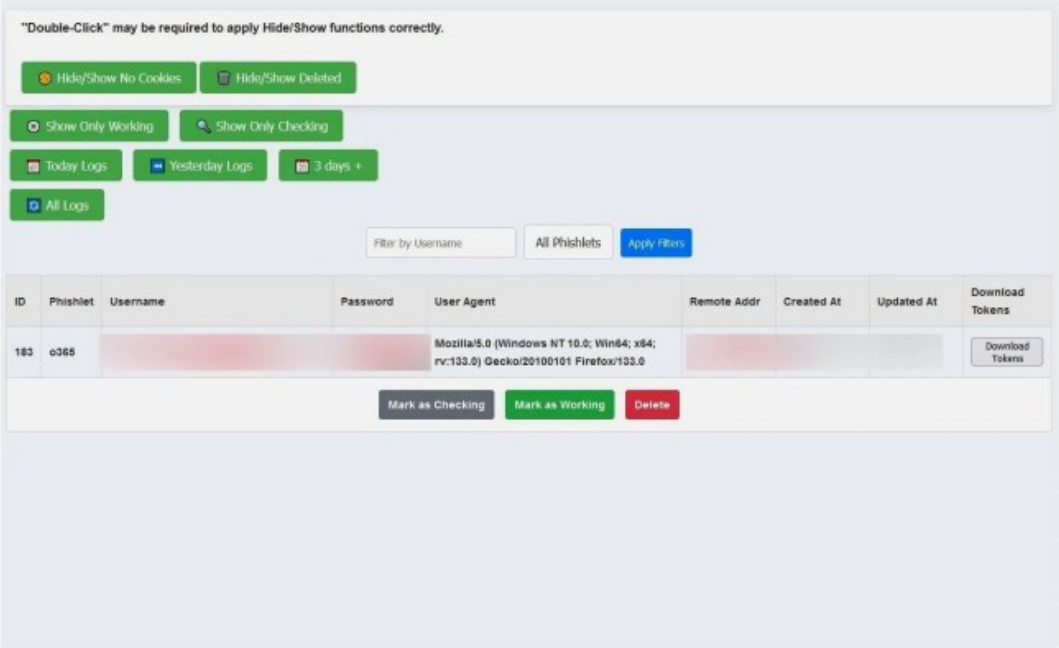


Gmail and Outlook users will see a seemingly legitimate window asking them to use two-step verification (Picture: SlashNext)

Can two-step authentication stop the attack?

Unfortunately, the worm will automatically get hold of the 2FA token in real time as it intercepts the details immediately when entered by the oblivious user.

This means that even the text message verification codes that appear stealthy cannot protect from this type of attack.



The hacker will get a notification when the login details and credentials have been entered (Picture: SlashNext)
