

Cynch Security Case Study

Cyber security in practice: Google Ads used for phishing attacks

Cybercriminals are using Google Ads to carry out phishing attacks that are hard to detect. This type of cyberattack is becoming more frequent and widespread.

What is happening

Cybercriminals are creating fake advertisements for popular software programs, including Microsoft, Adobe and Amazon Web Services software. The fake advertisements are a type of phishing attack that appear on Google search results along with legitimate ads.

The fake ads direct users to websites that replicate legitimate websites or login portals, prompting users to enter their credentials or to download malware. Once cybercriminals have access to user credentials or their malware has been installed, they are able to infiltrate personal and/or corporate networks. From there, cybercriminals can steal valuable data, launch ransomware attacks and halt companies' business-critical operations.

Cybercriminals are also implementing phishing attacks using the Google Ads platform to send email invitations that contain malicious links in the email message. The invitations are sent from Google's servers, which enable them to bypass spam filters. The invitations direct people to spam websites, including dating sites that are designed to collect personal information.

Google's response

Google has strict policies in place for Google Ads that prohibit misrepresentation. Google is actively removing fake ads and websites as they are reported and detected, and is encouraging users to report any malicious activity so it can take appropriate action.

Key takeaways

Phishing attacks are common and new, sophisticated scams, including those using Google Ads, can be difficult to identify. Here are some tips to protect yourself:

- Be cautious of fake ads: fake advertisements are designed to closely resemble authentic Google Ads. The accompanying websites will often use similar fonts,

colours and wording to the organisation's legitimate website. Be wary of clicking on Google Ads that promote popular software programs.

- Verify the authenticity of the website: before downloading software or entering your credentials into a website you accessed via a Google Ad, check the authenticity of the website. If you are unsure, navigate directly to the website via its official URL or go back to your Google search and look for a link in the organic search results, rather than an ad.
- Look out for suspicious signs: avoid ads or websites with vague content, poor spelling or grammar and offers that are too good to be true. When in doubt, do not click, download or input credentials or personal information.
- Keep your software up-to-date: update your software as soon as a new version is available to ensure you have the most recent security patches and are protected from vulnerabilities.
- Use multi-factor authentication: multi-factor authentication provides an extra layer of security for your accounts. Where possible, use [stronger forms of multi-factor authentication](#) such as physical keys or app-based authentication, rather than email or text authentication.
- Report suspicious Google Ads and emails to Google: this allows Google take appropriate action against the accounts involved and helps keep the broader community protected.

More information

For regular updates and insights on topics including cyber security, consider joining the [.au membership program](#). .au members have access to a range of [benefits](#) including a partnership offer with [Cynch Security](#), to help small businesses strengthen their cyber defences.