ADVISORY ON

FALSE SEARCH ENGINE ADVERTISING

CyberPeace
Foundation

ADVISORY ON

FALSE SEARCH ENGINE ADVERTISING

Date : 28 December 2022

Cybercriminals are impersonating brands and directing customers to harmful websites that host ransomware and steal login credentials and other financial information by leveraging search engine ad services, FBI warns.

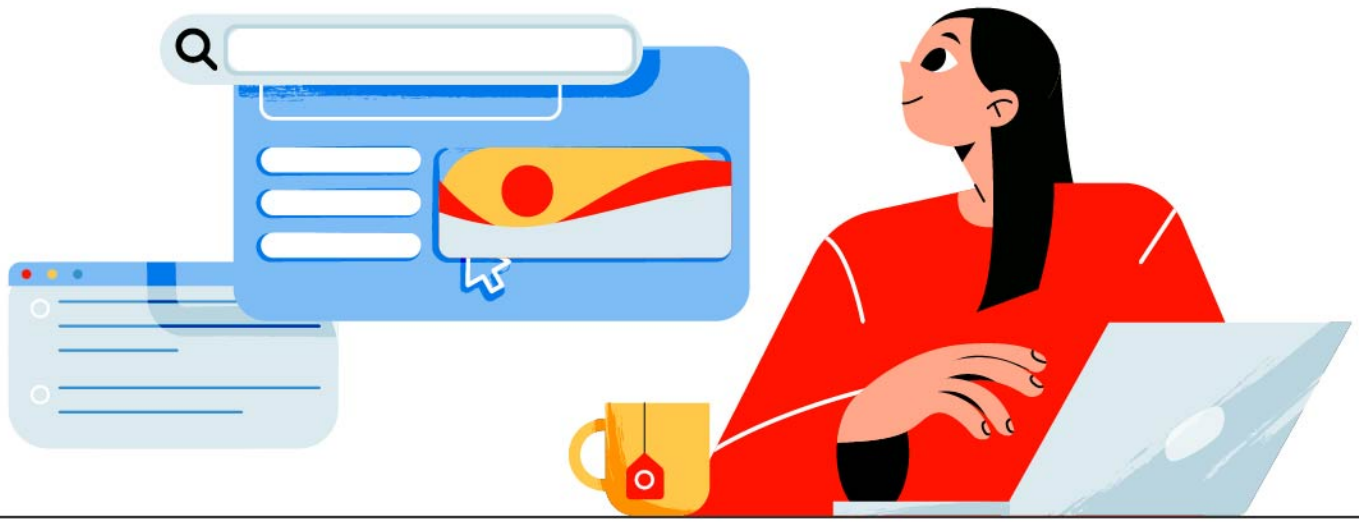
Modus Operandi

Cybercriminals buy adverts that show up in internet search results using a domain that resembles an actual company or service. These advertisements appear at the top of search results when a user searches for that company or service, hardly distinguishing them from legitimate search results. These adverts lead to a website that closely resembles the fake company's official website.

When a user is looking for a program to download, the fake website may contain a link to a malicious piece of software. The download is named after the program the user planned to download, and the download page appears natural.

Additionally, these adverts are being used to spoof financial websites, specifically exchange platforms for cryptocurrencies. These malicious websites pose as legitimate exchange platforms and request users to provide their login credentials and payment information, giving thieves access to the victims' money.

Although search engine adverts have no malicious intent, it is advisable to use caution when visiting a website via an advertisement.



Mitigation and Recommendation

Instead of searching for a company or financial institution, enter its URL into the address bar of your web browser to go straight to its website.

Check the URL of an advertisement to ensure the site is legitimate before clicking on it.

When searching the internet, use an ad-blocking plugin. Users can add extensions to most web browsers, including ones that block adverts.

To avoid domain spoofing, use domain protection services to alert businesses when comparable names are registered.

Inform visitors about fake websites and the value of ensuring destination URLs are accurate.

Inform users of where to locate trusted downloads of the company's software.

Never share financial information like bank account numbers, CVV, OTP, etc. with the impersonated website.

Reference

https://www.ic3.gov/Media/Y2022/PSA221221

Revision Note

Version No.	Description	Status	Date
1.0	Initial Public Release	Final	28-12-2022

Issued by

Research Wing, CyberPeace Foundation
Research Wing, Autobot Infosec Private Ltd.

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation