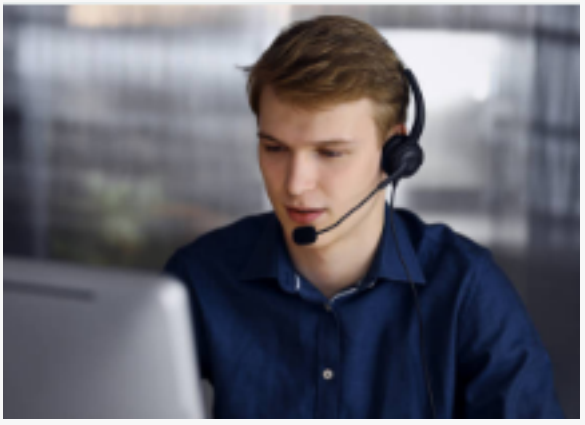
Scammers posting fake customer care service numbers on Google Ads: Cyber-Forensics.net explains ways to spot red flags

Scammers are tricking victims into calling fake bank hotlines found in advertisements on Google searches. The emerging cases have resulted in millions of losses

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, March 8, 2022 /EINPresswire.com/ -- Singapore Police were left stunned when at least 15 people fell prey to a relatively advanced type of scam. This new variant has come to notice since December 2021.

According to the local police, “scammers are using Google ads to create fake customer care helpline numbers of banks and demand money.” The latest updates reveal Singapore police are working closely with the search engine giant to take the fake advertisements down.

For the time, authorities are joining hands with the state government and federal government to alert bank account holders. Cyber-Forensics.net, a cyber forensics service for online scam victims, followed the emerging cases that led the firm to present insightful facts.

How Does The Scam Work?

> scammers are using Google ads to create fake customer care helpline numbers of banks and demand money.”
>
> *Timothy Benson*

Bitcoin fraud recovery explain that the plot begins with fraudsters posting fake ads on Google searches which show up as consumers search for their bank's contact number to resolve a dispute. The displayed ads provide fake phone numbers and email ids.

The potential targets call these numbers to speak to a bank representative only to meet the scammer impersonating the bank's staff. The tricksters

may even create fake scenarios to lure potential targets.

As a result, believing these fake ads, customers share their personal information, bank account details, and other information like credit/debit card or loan amounts-informed the investigating authorities.

The victims follow the instructions of the imposters and temporarily transfer the funds to bank accounts provided by the scammers under the pretext of resolving the banking-related issues. In reality, it is nothing but a refined version of identity theft.

The same pretext became a nightmare for Mrs. Wong- a resident of Singapore who lost nearly S$ 20,000 in a sophisticated ploy.

What happened?

Mrs. Wong's Grab app notified that her app's top-up functions were facing some issues. The notifications said that she had insufficient funds in her bank account. Her wallet was linked to her bank. So, she checked the account and confirmed she had enough money.

So, to settle the matter once and for all, she searched her bank's customer service on Google and talked to a so-called professional.

Finally, because "it was exactly how an employee would sound," Mrs. Wong gave the scammer her name, address, birth date, email, and account details.

Fund recovery expert Timothy Benson says, "In many cases, victims receive an SMS with headers spoofing the bank to appear more authentic, claiming the bank is facilitating a reset account as part of 'Let's Fight Scam' campaign." But the victims wouldn't realize the scam until it's too late. This is precisely what Mrs. Wong faced.

In response to these emerging cases, Cyber-Forensics.net lays out some tips to avoid becoming victims of such scams:

Tips to avoid becoming victims of bank spoofing scams

 Keep contact information up to date: Customers can quickly check the suspicious activities in their accounts. Log in to review and update the contact information or directly visit a bank.

 Create strong passwords for login: A scammer's easy targets are especially those accounts that have remained passive for over 3-5 months. Therefore, a strong password offers a strong defence against hackers looking to penetrate systems. To do this, login into the bank's user page, sign in and check the settings.

 Allow push alerts on the mobile banking app: Banks can directly send suspicious activities in the user's accounts to the bank account holders, against which they can take quick actions and prevent the financial loss from happening. Log in to the mobile banking app, select alerts from the menu, and review the settings to receive security alerts to the mobile device.

 Protect Devices: Keeping mobiles, laptops, desktops, pads up to date with the latest browsers and operating systems helps clean off any bugs in the old version and protects against vulnerabilities that hackers may exploit later on.

 Enable Biometrics: These days, smartphones require mobile users' fingerprints to lock or unlock the phone screen. Similarly, the mobile apps where payment details are stored can also be locked using biometric or facial recognition systems. So, when someone unknown gains access to customers' personal information, they won't access vital information like balance in the account.

 Know the red flags that signal a scam: Understand how scammers work and how fund recovery companies can pressure them to return the stolen funds.

 Know which parties have access to account information: This piece of information increases the chances of third-party money management apps and websites. Review the policies of third-party apps. Sometimes a mediator doesn't need the information being asked.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit https://cyber-forensics.net/.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter