

1393

investigations were
conducted in 2022

moljar

720

open and closed registers
around the world

74

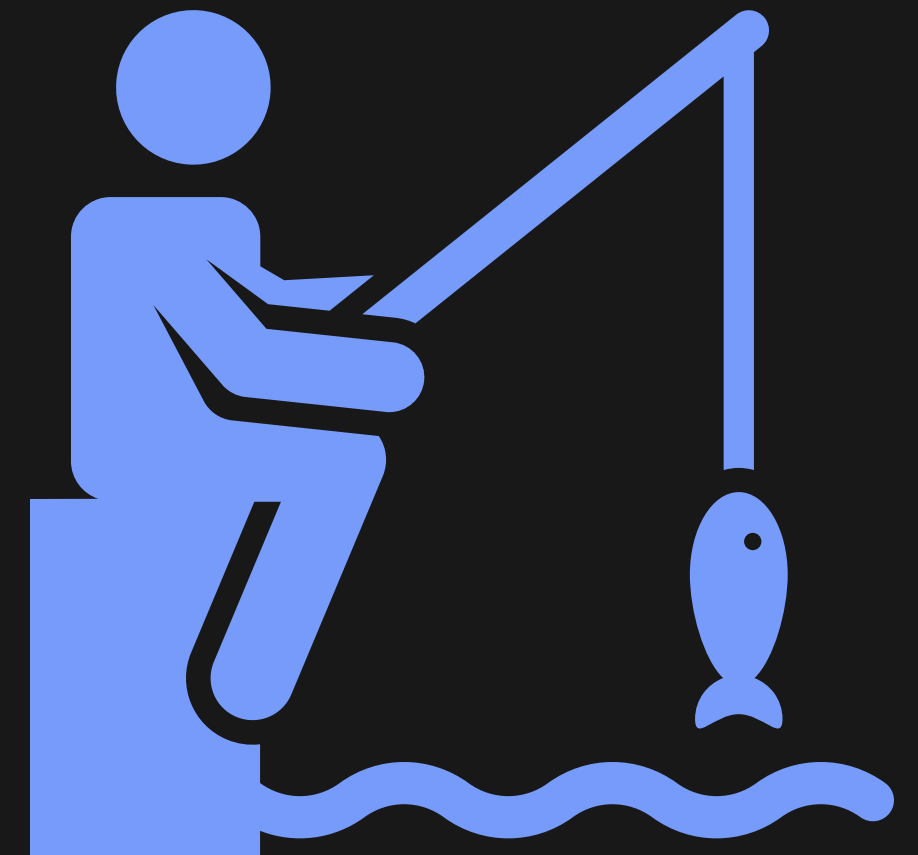
employees

Cyber security

Phishing

Online fraud where they attempt to trick you into revealing your:

- Social media accounts;
- Work and personal online storage;
- Banking information.



Phishing

- urgency
- noreply.ssupport@gamil.com (typo in the domain; should be gmail.com)
- viewing the email in a browser
- lack of https before the address
- google.fuuuuu90.tk

From: no-reply@useraccounts-google.com
Reply-to: no-reply@useraccounts-google.com
Subject: Critical security alert

Template ID:170562-790051

[Send me a test email](#)
[Toggle red flags](#)

Google Thomas Battaglia

Sign-in attempt was blocked
battaglit@sou.edu

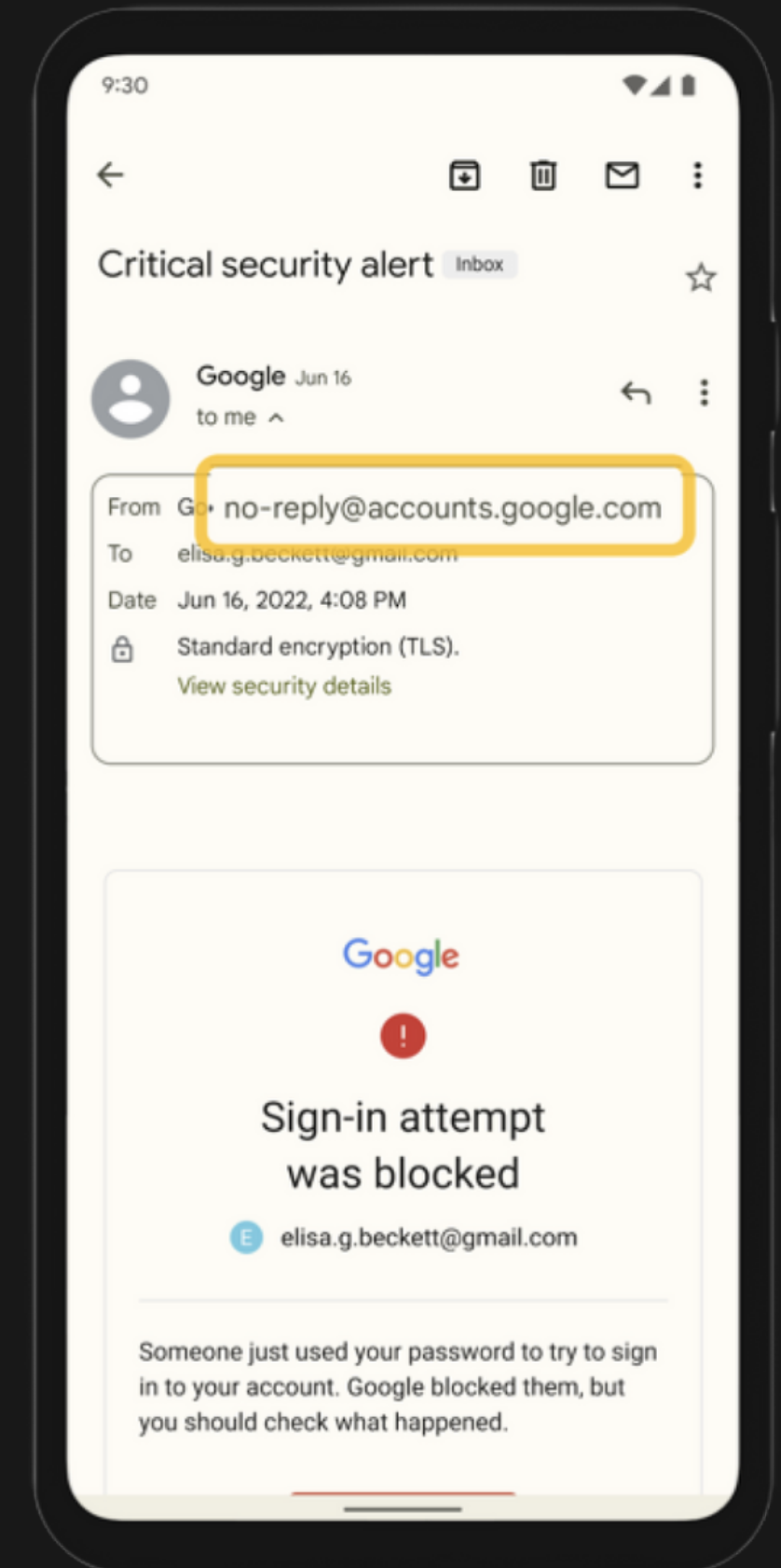
Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

[CHECK YOUR ACTIVITY](#)

You received this email to let you know about important changes to your Google Account and services.
© Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

How it ought to be

- Email from accounts.google.com
- Copies of emails sent to your backup accounts
- Duplicate of the correct address in the link
- https



Phishing

- Avoid using corporate email;
- Do not respond to unfamiliar and suspicious emails;
- Do not open files in suspicious emails;
- Canary tokens.



Phishing

Provocative messages

"You have been added to the blacklist, urgent identity confirmation required."

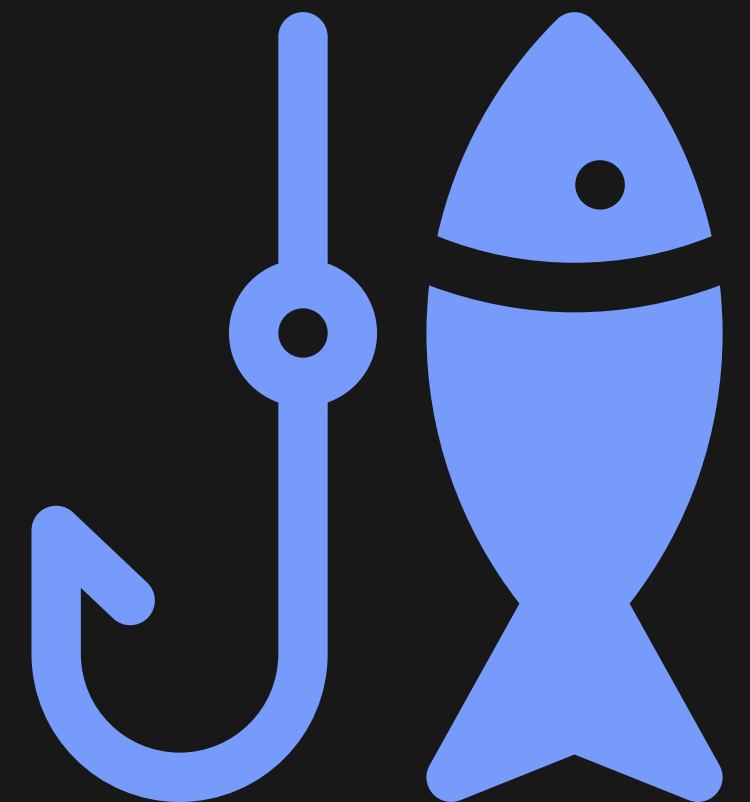
Blurred formulations in emails

"Dear account owner."

Messages from "friends"

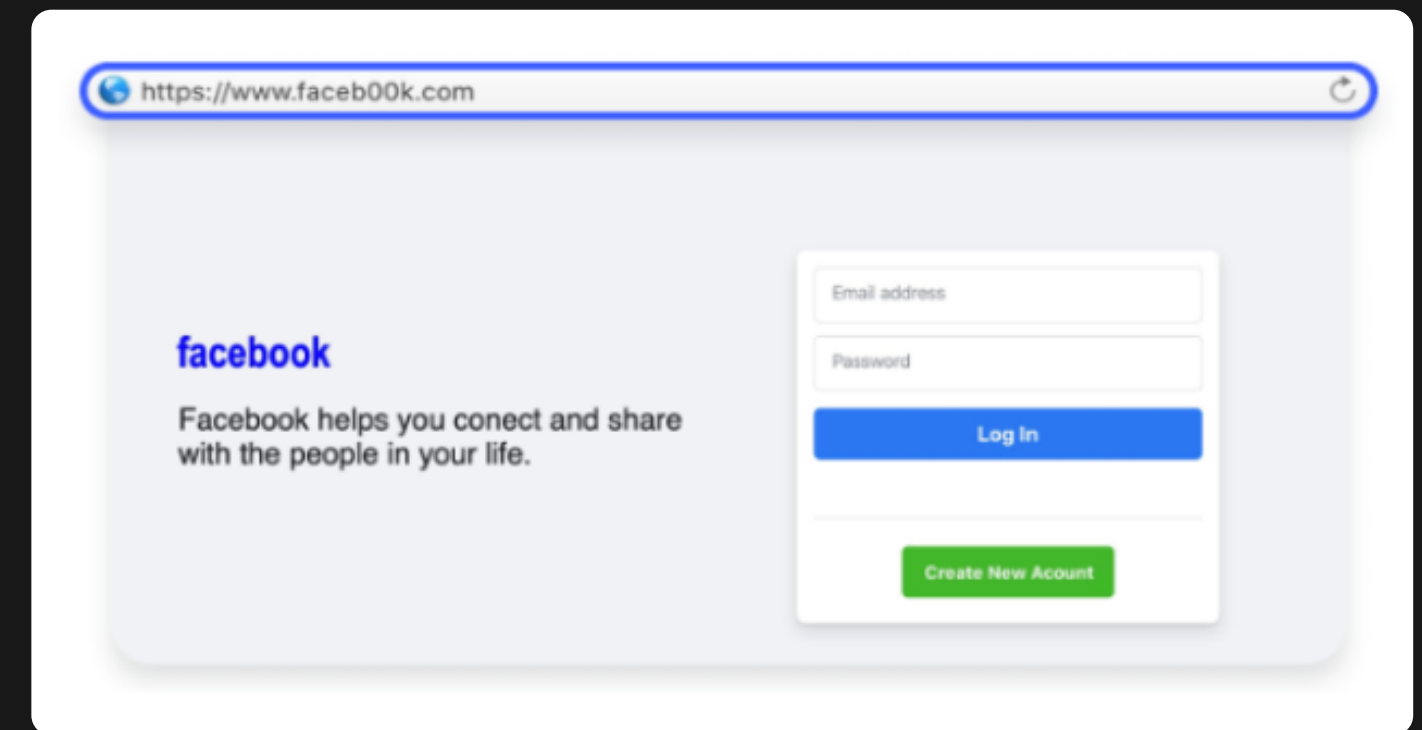
Request to provide or update personal information

moljar



Checking the link address

- link shortening;
- removing unnecessary characters, phrases, and numbers;
- URL encoding: the letter "M" becomes "%6D";
- discrepancy in the link from what is specified in the email;
- substituting letters with visually similar ones without changing the appearance.



"google" - "google." In the original domain, it's a lowercase English "l," and in the fake one, it's a capital "I."

Checking the link address

— checkshorturl.com — checking for link shortening;

— urlvoid.com, safeweb.norton.com, transparencyreport.google.com — checking for reliability.

Report Summary

Website Address	Molfar.global
Last Analysis	5 seconds ago Rescan
Detections Counts	0/40

Anonymity

moljar

Messengers

- Signal
- Dust
- Wire
- Threema



VPN

Semi-free Chrome plugins. Quality of work is 50/50:

- DotVPN
- ZenMate
- Ghostery
- Hotspot Shield

Using two or more VPNs is not advisable.

25 million free VPN user records exposed

Updated on 22 August 2022

Jurgita Lapienytė, Chief Editor

45 Million VPN User Records Have Been Leaked

VPN Unlimited®
part of MonoDefense

According to the research by the Comparitech security firm, millions of users are at risk following a massive VPN data leak. It was revealed that user connection logs and account information of several free VPNs, including [FreeVPN](#) and [DashVPN](#), had been leaked and exposed on an unprotected server.

Comparitech's head of security research came across the leaked database as it was freely available on the internet and had already been indexed by Google. The last part means that anybody could find the leaked data via simple googling. The database contains over 300 million records with 45 million VPN users' personal information, including email addresses, full names, and encrypted passwords.

Free VPN software left more than 18GB of connection logs accessible to the public. Threat actors could exploit the database to identify and even locate its users.

The Cybernews team discovered an open database containing 18.5GB connection logs generated by the [BeanVPN](#) app.

The dataset contained protocol addresses (IPs).

The information found approximate location user's email address the researcher.

Free VPN Service SuperVPN Exposes 360 Million User Records

SuperVPN is the same free VPN service provider that leaked customers' data back in May 2022.

BY HABBA SAGHD MAY 24, 2023 4 MINUTE READ

FOLLOW US

This time, SuperVPN has exposed a whopping 133 GB of data, including personal details of its unsuspecting users, such as IP addresses.

VPN

Instead, we recommend using paid VPN services on a regular basis:

- NordVPN
- Windscribe
- Surfshark



moljar

VPN

Additionally, changing your IP address using VPN services is necessary in the following cases:

- If you're sending a fake email on behalf of an American client with a Ukrainian IP;
- Some foreign registries and news websites do not work with Ukrainian IPs;
- When resetting the password for someone else's account on their email, a message may be sent from your IP;
- Besides changing your IP, clearing cookies can also be helpful.

Confidential search engines

Search engines that do not store user IP addresses and do not collect information:

- DuckDuckGo
- Startpage
- Qwant
- SearchEncrypt



The researcher's primary task during the search is to ensure their own safety

For this purpose:

- Use a VPN for browsing;
- Implement two-factor authentication;
- Search through a fake email account not linked to personal social media;
- Create fake profiles on social networks;
- Whenever possible, use temporary email services for registration;
- Disable location services in applications where it's not necessary;
- Utilize third-party SIM cards.

Molfar's social media



Telegram



Youtube



Instagram