1393

investigations were
conducted in 2022

720

open and closed registers
around the world

74

employees

molfar

Cyber security

Phishing

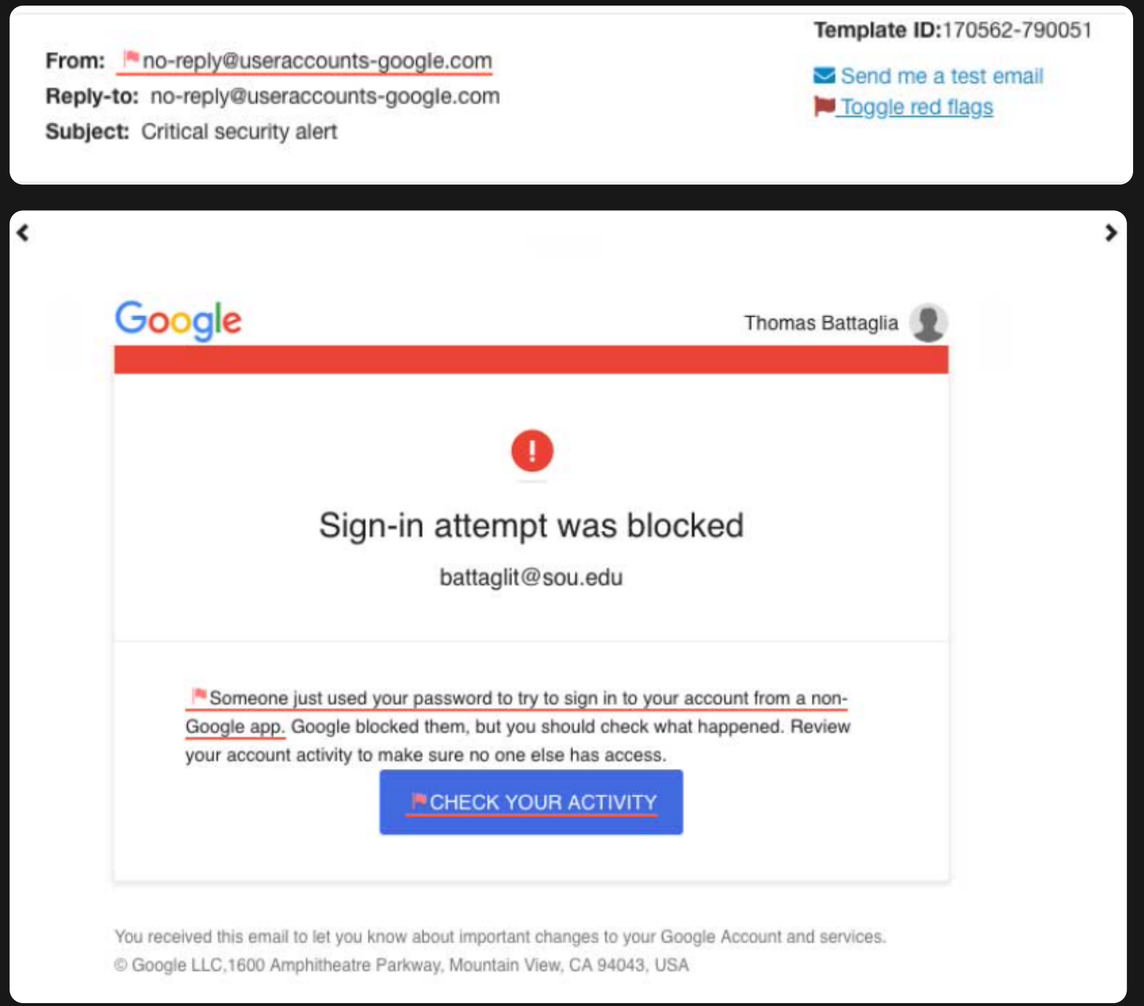
Online fraud where they attempt to trick you into revealing your:

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

molfar

Phishing

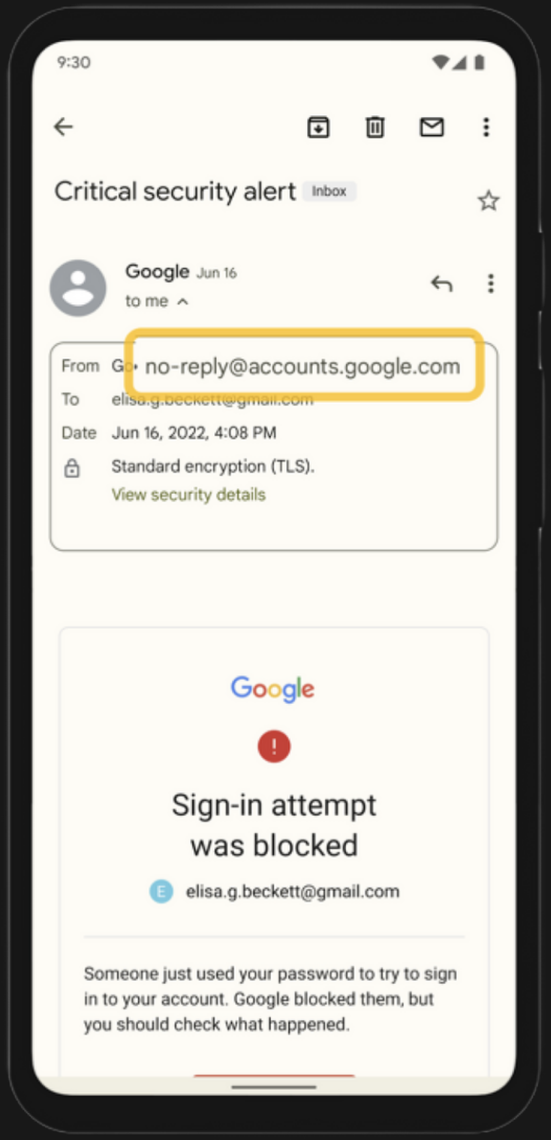
— urgency
— noreply.ssupport@gamil.com (typo in the domain; should be gmail.com)
— viewing the email in a browser
— lack of https before the address
— google.fuuuuu90.tk



molfar

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



molfar

Phishing

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

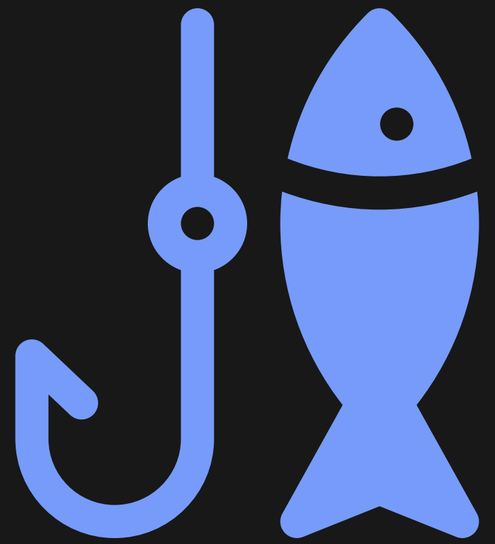
Phishing

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

Blurred formulations in emails
"Dear account owner."

Messages from "friends"

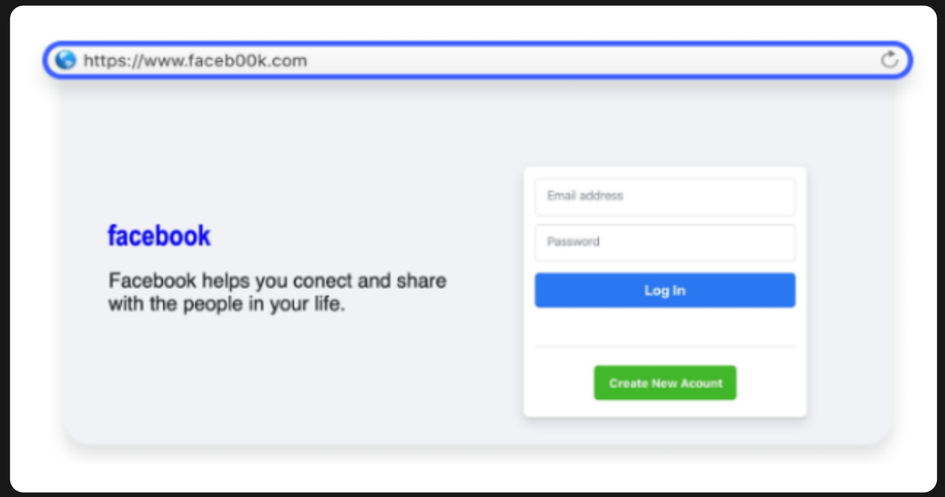
Request to provide or update personal information



molfar

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.

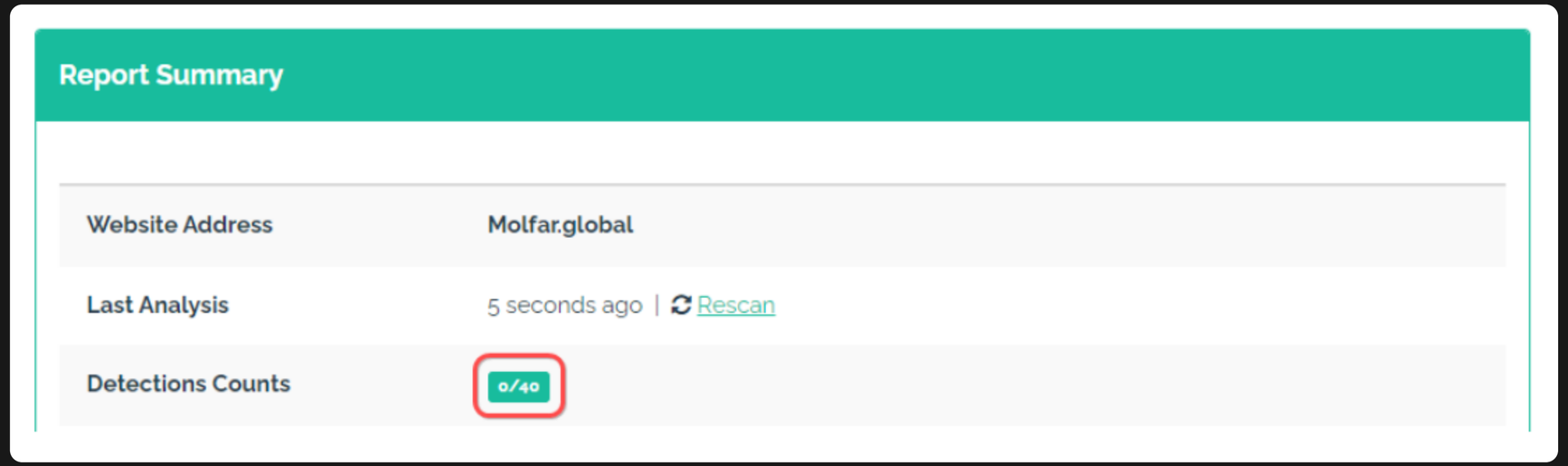


"google" - "google." In the original domain, it's a lowercase English "l," and in the fake one, it's a capital "I."

molfar

Checking the link address

— checkshorturl.com — checking for link shortening;
— urlvoid.com, safeweb.norton.com, transparencyreport.google.com — checking for reliability.



molfar

Anonymity

molfar

Messengers

— Signal
— Dust
— Wire
— Threema

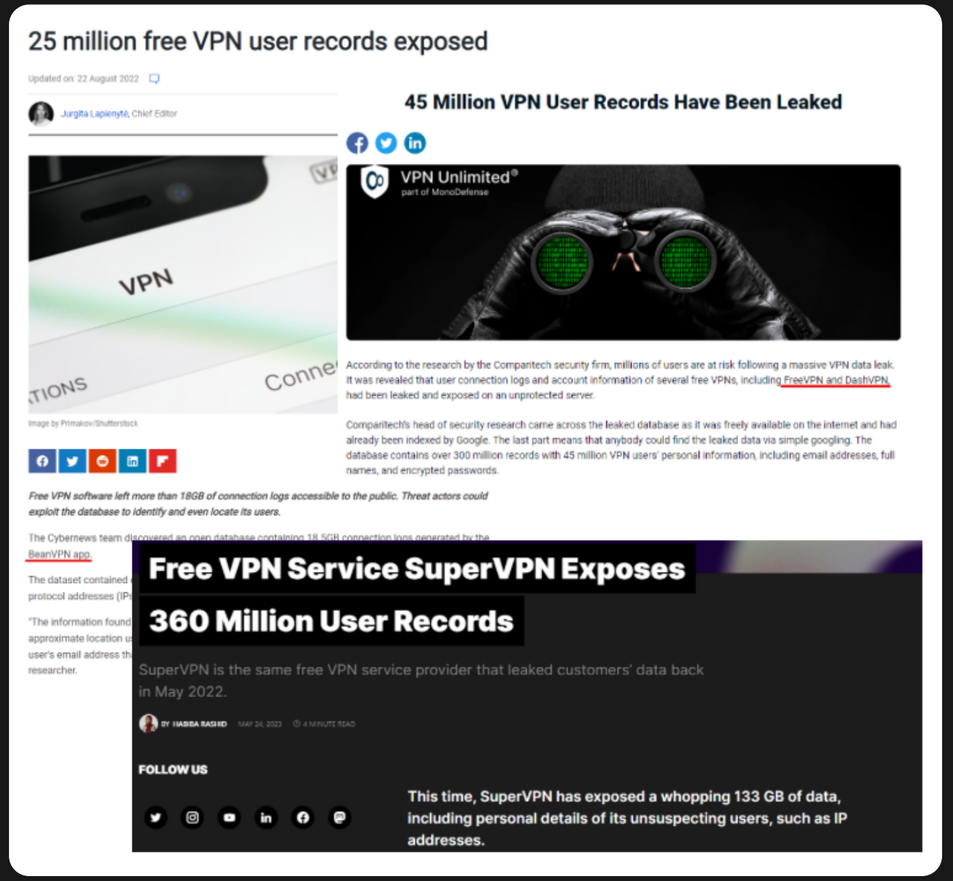
molfar

VPN

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

— DotVPN
— ZenMate
— Ghostery
— Hotspot Shield

Using two or more VPNs is not advisable.



molfar

VPN

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

— NordVPN
— Windscribe
— Surfshark

molfar

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

molfar

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

molfar