Security Tips

Sherolex
March 22, 2020

Table of Contents

1. Security Tips

In order to achieve greater security of your Sherolex account, please remember to implement and follow the four major security principles listed below:

- DO NOT give your password to anyone!
- DO NOT call any phone number of someone claiming to be Sherolex employee or from Support team!
- DO NOT send any money to anyone claiming to be a member of Sherolex.
- Enable Two Factor Authentication! (Google Authenticator)

2. Securing Your Trading Account

Our security team has prepared a list of 8 recommendations for how to improve the security of your Sherolex account. See our list below:

1). Use a unique email address and password for your account

You can use a secure password manager like LastPass or KeePass to easily keep track of your passwords and create more complex, secure passwords.

2). Enable 2FA on your Sherolex account

2FA adds an extra layer of protection to your account in case your password is compromised.

3). Always make sure to check the domain address you are visiting: https://sherolex.com/

Many phishing sites mimic Sherolex's domain or website to trick you into telling them your personal details. Make sure you're visiting the real site.

4). Don't click links or open unknown attachments in emails

Unless you are absolutely sure the email was sent by Sherolex.

5). Secure your email account and phone, and use PGP

Enable fingerprint or passcode lock on your phone, use a secure email provider, and use 2FA for your email account. Whenever possible use PGP.

6). Secure your computer

Don't install unnecessary software on your computer, or software from untrusted developers. If possible, consider using a dedicated computer or partition for Sherolex and trading. We recommend installing Linux, Chrome, a password manager plugin and nothing else.

7). Subscribe to good antivirus software, and keep it updated

8). Secure your internet connection

Always use a wired connection if possible. If you must use WiFi, consider routing your traffic through a VPN.

Please note: these tips are not exhaustive. On top of the above, please exercise vigilance and educate yourself further about general online security.

3. How to Prevent Phishing Attacks

1). What is a phishing attack?

Phishing is a type of social engineering attack; a fraudulent attempt to obtain sensitive information such as username, password, 2FA code, etc by disguising as Sherolex in electronic communication. Users are often deceived by trusted parties such as:

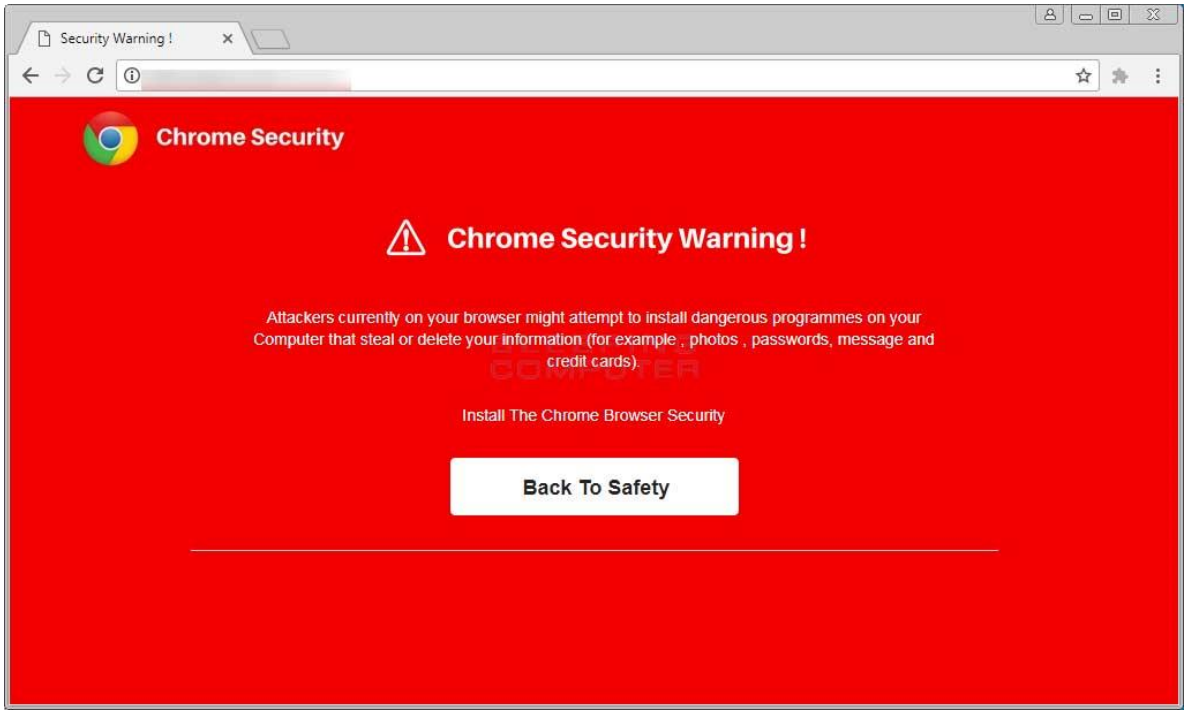
- Email spoofing.
- Fake Sherolex site.
- Instant message with a malicious link.
- Social websites with manipulated Sherolex link.
- Chat with impersonated Sherolex support.
- Fake Sherolex hotline or support in the search engine, etc.
- Social Media Fake Account.
- Malware downloaded from the internet.
- Free WIFI Phishing.

2). Phishing attack protection

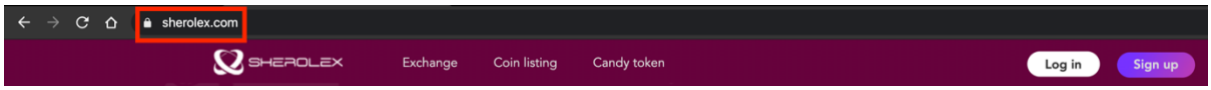
The most important and weakest aspect of a security system is people. Hence, For users, **vigilance** is the key:

A spoofed message often contains subtle mistakes such as spelling mistakes, strange syntax, unsmooth words, misspelled domain names, for instance, www.sherolex-co.com, etc.
In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, an email could threaten account expiration and shall be verified within a timeline; A message instructed users to move assets to a secure wallet to avoid loss as soon as possible.
Phishing attack protection requires steps to be taken by both users and Sherolex.

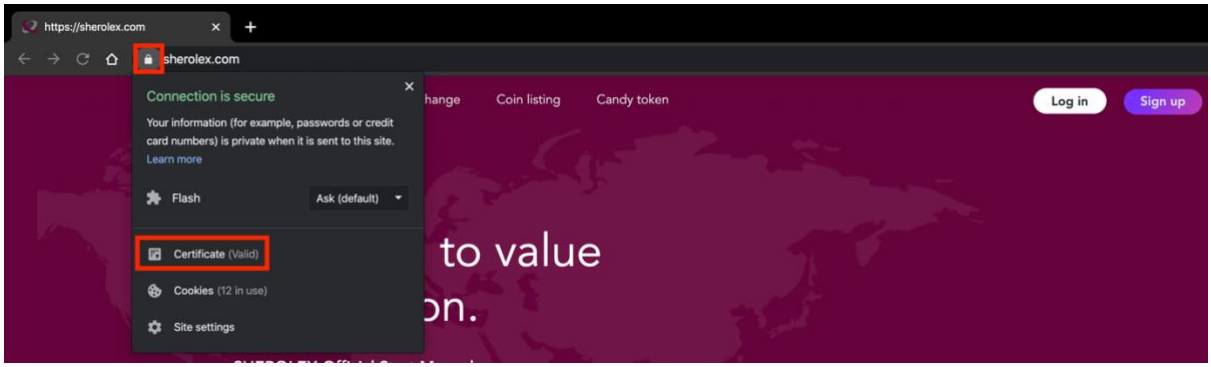
Always upgrade Google Chrome or Mozilla Firefox to the latest version. Google Chrome or Mozilla Firefox will warn users of phishing or unsafe high-risk website. For examples:



The safest way to login to Sherolex is through the website https://www.sherolex.com

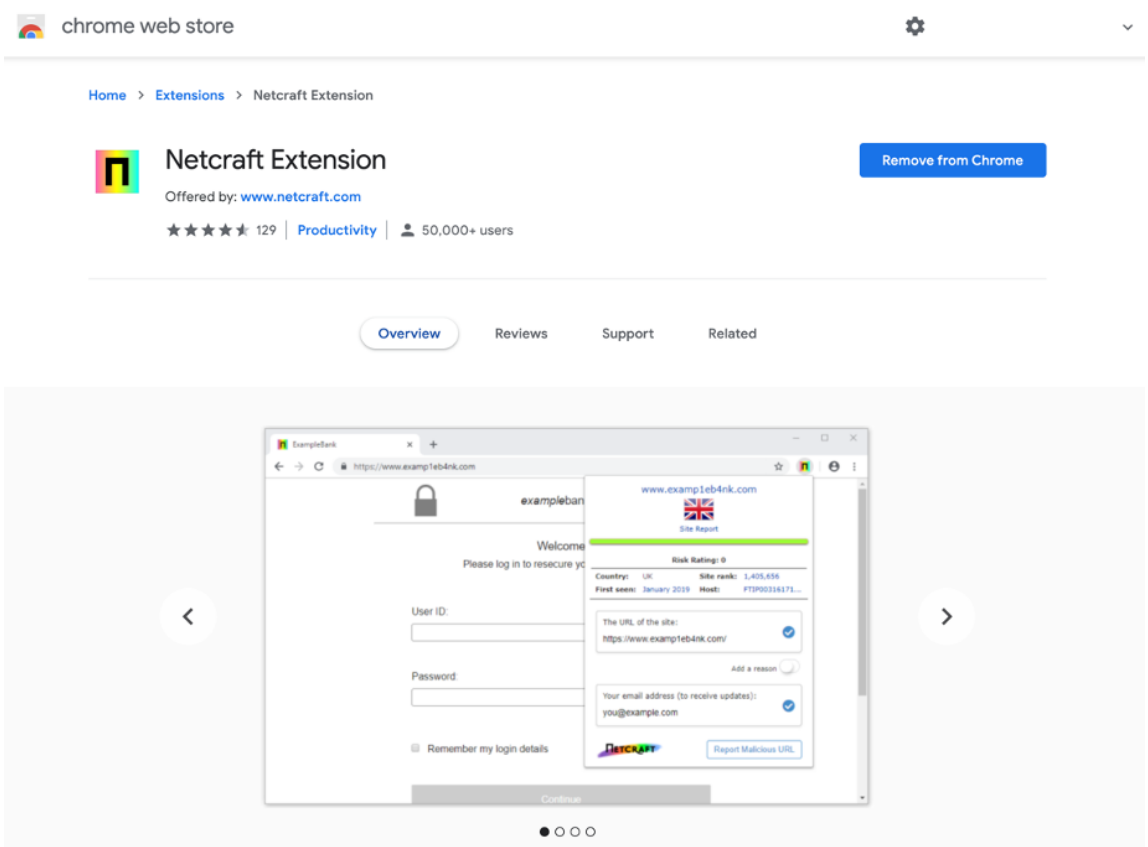


We also recommend you to check and verify whether SSL certificate is given for domain name *.sherolex.com.



Enable Two-Factor Authentication (2FA) by Google 2FA. Be cautious and don't disclose Google 2FA 16 digital backup keys to anyone or on any website. If username and password are compromised, 2FA prevents the use of compromised credentials, since these alone are insufficient to gain entry to the account or its funds.

1). Install Chrome Netcraft Extension (* If use Firefox, install Firefox Netcraft Anti-Phishing Extension).



Keep your systems/applications updated to avoid the security bugs. Install anti-virus software and keep it up to date.
Do not connect to an untrusted wireless network.

3). Reporting Phishing

Please report any Sherolex phishing sites you see to this form: Report Sherolex Phishing Sites.

4. Impersonators of Sherolex Support on Telegram

Sherolex support never ask you to send money to any address for any reason. If someone asks you to do this, he is trying to scam you and you should ignore him. Report these users to an administrator using private message function.

Sherolex Support representatives are not involved in chats with users using private messages. Our team will never ask you to reveal your sensitive information, such as account email address, password or 2FA backup key.

If you've experienced a problem or issue, either Sherolex Customer Support or a member of our security team might alert users via email or in a community such as telegram and suggest you to report the situation in detail to our support team.

5. Scammers on Telegram

There are NO official Sherolex Customer Support service being given in any of our official Telegram communities.

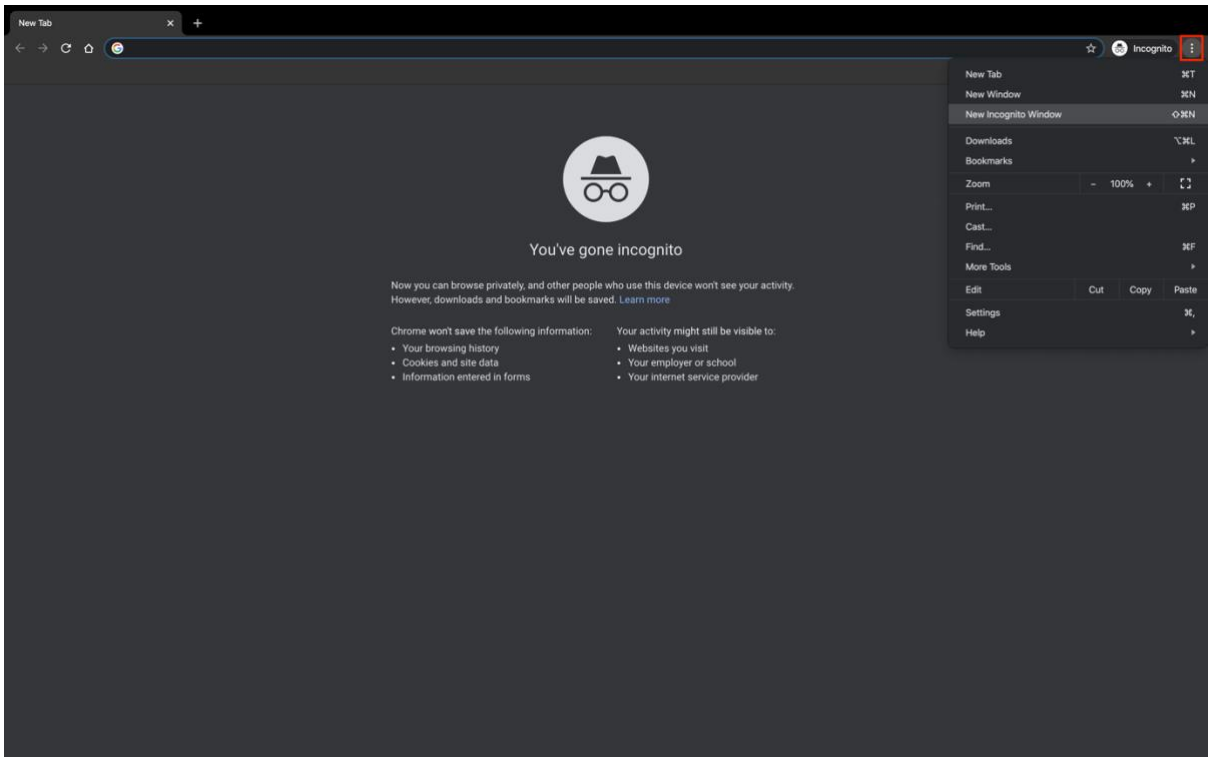
Anyone that claims to be Sherolex Customer Service and messages you first in a private message is a scammer. If anyone asks you to send money to any address, they are also trying to scam you and should be ignored.

If you find the above case and need to contact Sherolex Customer Support, please send an email to usersupport@sherolex.com and we will do our best to respond as soon as possible.

6. Antivirus & Trojan Guidelines

It is recommended that you perform a full security scan on your computer periodically.
We've listed two suggested methods below that will help to protect and secure your system:

1). Every time you browse Sherolex.com or log in to your account, we recommend using Security Mode or incognito/private tab without any browser plug-ins and extensions. Chrome: new incognito window shortcut Ctrl+Shift+N



(if you use Firefox: New private window shortcut Ctrl+Shift+P)

2). Double or even triple check the withdrawal/deposit address that you're going to use on your Sherolex account. Make sure to always put a valid withdrawal/deposit address in a safe place, such as notepad, then copy/paste it to the browser from there. Finally, check the consistency of the address between the one in notepad and the one that you've pasted in the browser window.

If you find any sort of inconsistencies between addresses, it is possible that the computer or mobile phone has been infected by a Trojan or virus(es) already. Below are some helpful suggestions for you:

- Install anti-virus software to scan/kill Trojans and viruses as soon as possible;
- Disable plug-in/extensions in the browser, uninstall unknown software from your computer;
- In extreme risk situations, you might need to format the disk and reinstall the OS on the computer to get rid of viruses;
- Seek help from information security experts;