Coinhako Data Security Guide

Content

Password Basics

01 Do not share with others

It is never advisable to share your password(s) with anyone.
Do not share any password(s) related to Coinhako.

02 Do not repeat on different sites

It is never advisable to use the same passwords for different sites. Use a unique password for Coinhako.

03 Do not use Information that identifies with you

Never use anything synonymous with yourself:
- Birth date
- Name
- Phone number etc.

04 Keep your Password Long

We recommend having at least 13 characters. Longer passwords are harder to figure out.

Account Security Best Practices

05 Keep your 2FA enabled

2FAs give extra protection on top of your password. Enabling it greatly reduces the risk of your account being compromised.

06 Adopt external password managers

Password Managers provide secured platforms for password storage and management. They also help generate secured passwords.

07 Avoid unsecured and/or public wifis

Unsecured and public wifis increases your risk of data theft or breach of data. Only key in data in networks you can trust.

08 Watch where you share your personal data

Do not share information in places that you are unsure of. Always check with Coinhako before sharing any data related to us.

Protecting Your Online Data

Identify Fraudulent And Secured Sites

01 Check for discrepancies in spelling

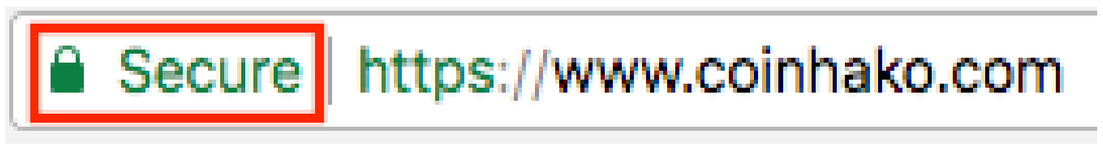
Coinhako's URL is
https://www.coinhako.com

Do not provide any information or try to avoid sites that that might bear a slight resemblance to Coinhako's URL and you are not entirely sure of. Contact us if you come across such sites.

02 Check for encrypted connections

Check if sites have encrypted connections before sharing information. Different Browsers have different indicators for encrypted connections.

Google Chrome Indicators:



1. "Https://: protocol in the address
2. A lock sign next to "Secure"
3. Indicators are Coloured Green

Fraudulent Activity and Applications

Fraudulent plug-ins have the ability to install malicious software(s) into your device. These might affect your device with viruses and/or online identity theft.
Always do some research on Plug-ins before installing them.

03 Check for credibility and legitimacy of browser plug-ins

It is common to encounter links, advertisements or messages that will lead you to Fraudulent sites.

Such sites could:
1) Be Phishing Sites
2) Install malicious software(s) into your device (ie. Malware).
These might result in your device being affected by viruses and/or online identity theft.

04 Avoid suspicious links and messages

Further Data Protection Tips

05 Handle your Information with Care

Never share data on places that you are uncertain of.

Coinhako would never ask you for your password. We will never send out any emails, pop-ups and/or SMSes requesting for such information. If you are unsure about any requests that might seem related to Coinhako, kindly check with our support team before carrying on.

06 Monitor your Online Data

We highly recommend that you check your online data at https://haveibeenpwned.com/ every once in awhile.

Any other recommended data protection programmes should also be considered to further ensure that your personal data is not compromised in any way.

Increasing Capabilities of Malicious Technlogy & Closing Statement

As Technology and Innovation continue to grow at an astounding rate, so does the threat from hackers and online data security breaches.

Eg. Malware programmes now have the ability to identify Bitcoin/Ethereum addresses when you “copy”, and replace them with their own just when you are about to click send – in addition to stealing online data. Hackers are also known to have capabilities to generate online information from data that they might have gathered on other sites.

It is highly advisable to take extra precautions to prevent such software and applications from infecting your devices.

Some basic security advice includes:

- Keeping all your device & online security measures up to date
- Regularly Scanning your devices

Knowledge is defense.

We also strongly recommend consulting with any relevant regulatory bodies before registering with any Cryptocurrency related and/or Online companies. You should be able to find valuable information about the risks online companies and digital products to help you better fend against online threats.

Best Regards,
Coinhako Team

For more information, permission to reprint or translate this work, and all other correspondence, kindly email us at hello@coinhako.com