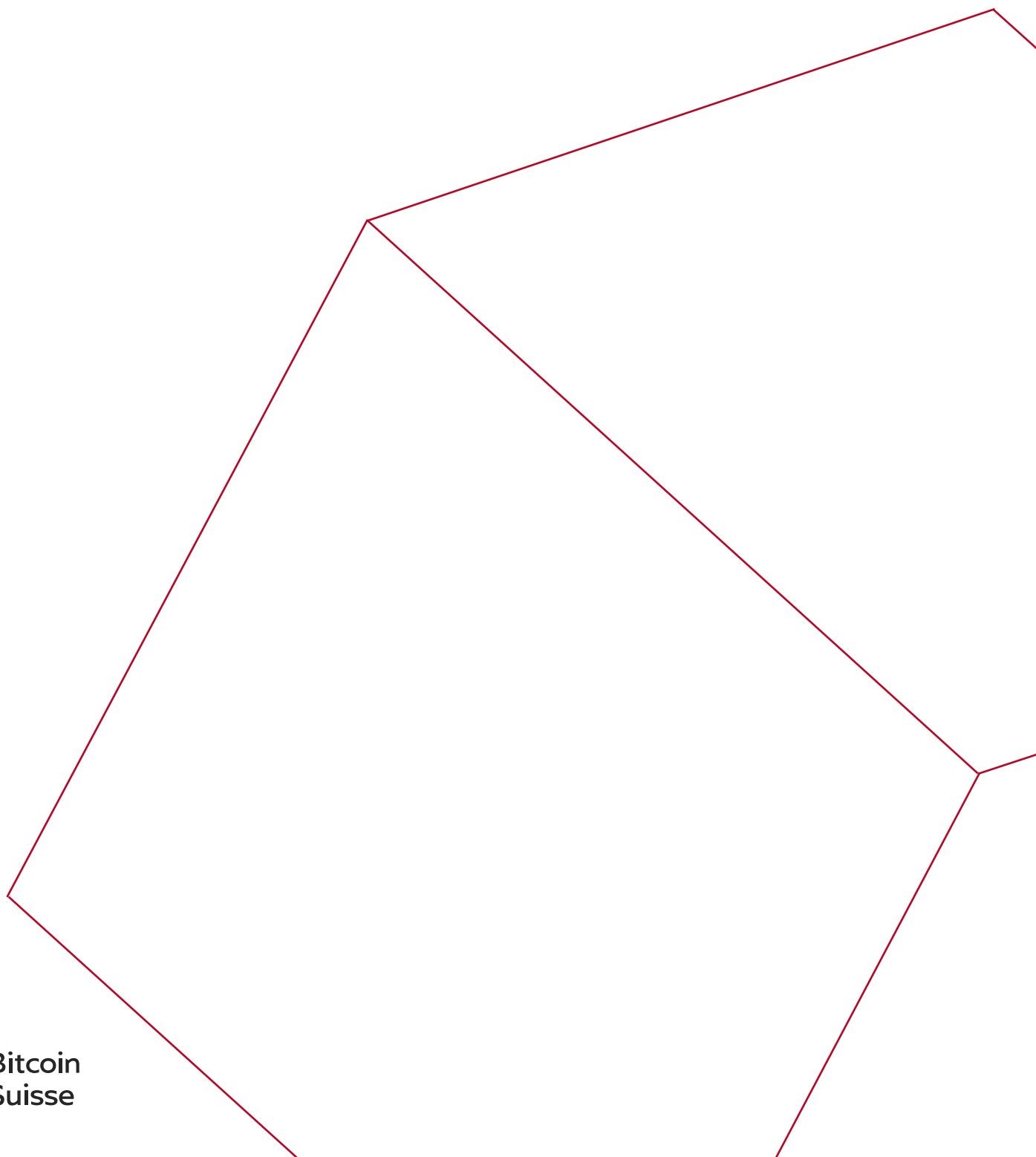


**V.1.0** July 2023

# Online Security



## General Online Safety

**Maintain vigilance in all online communications.**

- Be skeptical of suspicious emails, text messages or phone calls
- Verify senders of communications to ensure their authenticity
- Avoid opening emails, texts, or links from unknown or suspicious sources
- Never use contacts that were provided in suspicious communication
- Never share sensitive data like passwords, financial details etc.

## Password and Authentication Practices

**Create unique and secure passwords.**

- Use at least 12 characters (mix of upper- and lower-case letters, numbers, and special characters)
- Avoid common words and regular password repetition
- Change your password regularly
- Implement multifactor authentication (MFA) where available
- Be cautious of e-mails, messages, calls or websites that are asking for credentials or to do something urgently
- Update your systems, apps and devices whenever an update is available
- Avoid using public WiFi

## Interactions with Service Providers

**If contacted by a service provider and uncertain of their legitimacy, reach out to them through their official communication channels.**

- Always verify the identity of any service provider contacting you
- Remember that legitimate service providers will typically not ask for sensitive information via e-mail or call
- If something feels off, report the interaction to the service provider's official customer support
- Trust your instincts – if something feels off or too good to be true, it most probably is

## Dealing with Bitcoin Suisse

**Bitcoin Suisse will never contact you to ask for sensitive information.**

- Bitcoin Suisse will never ask for your passwords or transferring funds over a call or e-mail
- If you're unsure about a caller claiming to be from Bitcoin Suisse, terminate the call and dial back on the official phone line +41 (0)800 800 008
- If you receive a suspicious request purportedly from Bitcoin Suisse, report it to our official customer support

## Social Engineering Defense

**Be aware that criminals may trick your service providers into granting them access to your information. Such stolen documents can be used to gain unauthorized access to your data or accounts.**

- Ask and confirm: Enquire your service providers about the password reset process they have in place
- Trust but verify: Insist on strong identification measures before resetting passwords, such as video calls
- Less is more: Limit the amount of personal information you share online, including social media, social engineers often gather information from these platforms
- Stay updated: Regular updates of your operating system and application include security patches
- Backup for safety: Regularly backup important data to mitigate the effects of potential attacks

- Be cautious offline: Be skeptical on unscheduled calls and overcurious people beside you in bars, restaurants, or public transportation
- Use anti-malware protection: Enable anti-malware security solutions to prevent malware infection on your computer

**Ensure you have strong prevention measures in place to avoid falling victim to social engineering attempts.**

## Understanding Blackmailing

**Blackmailing is threatening to expose potentially harmful or private information unless demands, typically monetary, are met.**

- Don't Make Hasty Decisions: Avoid making decisions while under pressure or panicking. Take time to understand the situation before deciding on any action
- Document Everything: Keep a record of all communications from the blackmailer. This will serve as valuable evidence if you decide to report the issue
- Contact Authorities: Report the incident to your local law enforcement agency. They can provide guidance and assistance in investigating the matter
- Avoid Paying the Ransom: Paying the blackmailers often doesn't solve the problem and might even encourage further blackmailing attempts

**Remember, in times of distress, maintaining a clear mind and taking appropriate steps can help manage and possibly resolve blackmailing attempts.**

**Disclaimer**

The information provided in this document pertaining to Bitcoin Suisse AG and its Group Companies (together "Bitcoin Suisse") is for general informational purposes only and should not be considered exhaustive and does not imply any elements of a precontractual or contractual relationship nor any offering. This document does not take into account, nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information is believed to be accurate and reliable, Bitcoin Suisse and its agents, advisors, directors, officers, employees, and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information, and Bitcoin Suisse expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Bitcoin Suisse reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient hereof. The information provided is not intended for use by or distribution to any individual or legal entity in any jurisdiction or country where such distribution, publication or use would be contrary to the law or regulatory provisions or in which Bitcoin Suisse does not hold the necessary registration, approval, authorization or license, in particular in the United States of America including its territories and possessions. Except as otherwise provided by Bitcoin Suisse, it is not allowed to modify, copy, distribute, transmit, display, reproduce, publish, license, or otherwise use any content for resale, distribution, marketing of products or services, or other commercial uses. Bitcoin Suisse 2023.

---

Bitcoin Suisse AG  
Grafenauweg 12  
6300 Zug  
Switzerland

[bitcoinsuisse.com](https://bitcoinsuisse.com)