SECURITY INFORMATION

General

The **GUILD SAGA with company name EHMO TECH INNOVATION LTD and Registration Number, HE. 407977, incorporated in the Republic of Cyprus (full member of the European Union) with registered address: 1 Driadon. 1st Floor, 101, 6041, Larnaca, Cyprus,** will announce any breaking security issues on this website. We suggest all users of **GUILD SAGA** wallets and services to read the below information.

Security of your Personal Information

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

What if GUILD SAGA gets Hacked?

In the event GUILD SAGA's website is down or hacked, please also check our Twitter or Discord channel. GUILD SAGA's protocol has an alert system and currently a small set of people working for GUILD SAGA's control the keys to issue alerts. These will be sent to all nodes.

What if GUILD SAGA Turns Evil?

If we are sufficiently hacked, or if we collectively turn evil, the above resources will not be sufficient to protect you. Luckily, the **GUILD SAGA** network is growing into a larger and more resilient community beyond the **GUILD SAGA** company itself. If you suspect that the company has been compromised, please also check other community resources **unrelated to GUILD SAGA.**

Phishing & Spam

A social engineering technique used by attackers aiming to receive the users' personal data. Phishing attacks can provide an attacker with access to the following personal data:

- Credentials for any electronic service (electronic wallets, mailboxes, payment services, social network and other accounts etc.);
- Personal data to be further used in other types of attacks;

Methods used by attackers:

- Personal e-mails (can have a particularly powerful psychological effect on a person);
- Bulk spam mail (a widespread, cheap technology that can reach a large target audience);

- Any online resources (efficiency stems from the carelessness of the visitors of web resources).

How to recognize phishing?

- Use of brands and well-known trademarks with a slight difference from the original;
- Similar links and copycat sites (use of similar interfaces or addresses);
- Incorrect domain name of the mail server or mailbox name of the sender.

Countermeasures:

- Careful handling of attachments and links in e-mails;
- Scanning downloadable files and resources with VirusTotal;
- Checking connection security.

DATA EXCHANGE VIA FILE-SHARING SITES AND FLASH DRIVES

Countermeasures:

- Using trusted sources;
- Scanning downloaded files (VirusTotal);
- When uploading files to a file-sharing site, use password-protected archives and asymmetric encryption.

About Email

- Account activity monitoring (IP address, time zone);
- Two-factor authentication;
- Creation of complicated passwords.

About the Browsers

- Account activity monitoring (IP address, time zone);
- Use of plugins;
- Disabling the browser’s password auto-fill functionality.

About the Social Networks

- Two-factor authentication;
- A complicated password;
- Responsibility for published posts