Dear Jefit user,

We are writing to notify you about a cyber-incident that may have exposed some of your personal information (No financial data involved). We take the protection and proper use of your information very seriously, and contact you now to explain what happened and the steps that you can take to protect yourself against cyber crime.

What happened?

In early last month, we became aware of this data breach from a few users' reports and immediately investigated. Soon after we took a series of actions to make sure our system is safe and to further protect your account.

Upon discovering this breach, we took immediate action to secure our servers and the impacted accounts. We also began an investigation to understand the scope of the incident. We were able to identify the root cause of the data incident and confirmed that other Jefit systems were unaffected, and contacted law enforcement.

At this time, there is no sensitive financial data involved since we never stored customer's payment information. All the payment process was directly handled by Google Play Store, Apple App Store, or directly processed by the payment gateway company if customers purchase products on our website. Nevertheless, we are providing this notice out of an abundance of caution because some other part of your private information was accessed by the perpetrator of the cyber-incident.

What type of information was involved?

The personal and private information that the perpetrator gained access to some or possibly all of the following:

- Jefit account username.
- Email address (associated with the account).
- Encrypted password (hashed with unique salt to each account).
- IP address when creating the account.

What we are doing to prevent any future breach of data?

Upon discovery of the cyber attack, we immediately secured and patched the bug.
We also conducted a forensic investigation to confirm that no other systems were impacted. We have taken security measures to strengthen our network against similar incidents in the future. We also have implemented a stronger password policy on our product to further protect user's accounts in the future.

What can you do?

We want to make sure you are aware of steps you may take to guard against potential phishing email attacks or other forms of fraud. Although all the passwords have been hashed with unique salt (meaning passwords were encrypted) before saving to our system, it is still possible for the perpetrator to decrypt some of them if the passwords were too simple. We encourage you to change your password as soon as you can.

We take the privacy and security of your information seriously, and sincerely regret any concerns or inconvenience that the incident may have caused you.

Sincerely,

Ying Lin
CEO