

# Ken's Study Journey Internet Security Proposal

## Ken's Study Journey Strives to Maintain Internet Security

### Let's Strengthen Security on State-of-the-art Technology

Dear students, teachers, and visitors,

Thanks for choosing and using Ken's Study Journey services!

In January 2023, **Twitter**, an Internet social media platform, **was breached affecting over 200 million users**, according to Firefox Monitor. **Ken's Study Journey** attaches **strong importance** to this incident.

In recent years, the Data Breach problem of Internet services is becoming severe. I **stayed alert to Internet security**.

I then use **telecommuting and remote management** to urgently make security updates on program codes in my free time during the Spring Festival.

The Website Data Breach mainly relies on website security and API weaknesses, according to my investigation. **Tor (The Onion Router, i.e. The Dark Web)** is **mainly used for such activities**.

**Ken's Study Journey** has its headquarters and main servers in **Guangzhou, China (CN-CAN)**. It is not only **the core server node** of the Ken's Study Journey network but also **the busiest server node with the most users**, serving hundreds of Chinese users daily like the city centre library.

As a **Chinese international school student and Internet service**, Ken's Study Journey not only **complies with China laws and regulations** but also **communicates with and services to student users worldwide and internationally**.

On 1 July 2023, I **finished upgrading** my server's security and logging systems, **further strengthening** the user study plan and data security.

While Ken's Study Journey uses its maximum effort to strengthen security on the systems, **there are also some steps you can do to strengthen it further**.

#### 1. Know the Importance of Internet Security

Internet Security is more important than studying, only with which can you ensure your study plan is not illegally changed or viewed, **study productively** and **be rest assured**.

Students may **forget classes and tasks, be late or absent from classes**, and even create negative impacts on future study journeys and disclose exam materials without it.

## 2. See something Unusual? Report it Immediately

If you **see something unusual** while using Internet services (see **Appendix 1 below**) (not only Ken's Study Journey services), you must **report them to the platforms immediately**.

For example, you can email to [ken@kenstudyjourney.cn](mailto:ken@kenstudyjourney.cn) for **Ken's Study Journey products and services** (e.g. Ken's Study Planner).

This **strengthens security for both you and other users**. By the way, you can report bugs as well.

Unfortunately, Ken's Study Journey is a **free (volunteering) and non-profit service**, so I am unable to offer rewards for such reports.

However, this is **always appreciated**.

### Real Example

At the end of June 2023, Ken's Study Journey received an email from a user reporting a bug on **Ken's Study Planner: Unable to set Schedule/Lessons**.

This bug was then fixed in 12 hours.

## 3. Stop Abusive Activities

If you see **something abusive (like scanning login pages and (D)DoS attack)** (see **Appendix 2 below**) from people beside you, please stop and supervise them together.

Please also report to the platform if it persists after warnings.

## 4. Enable 2FA/MFA and Login Reminders

The login pages **can be massively scanned** on a website without adequate protection. **Account security on other websites can also be degraded** if a website is hacked and breached with password leaking.

For this reason, Two-factors Authentication (2FA) or Multi-factor Authentication (MFA) should be used (e.g. with **text/email messages and/or authenticator apps**). Others **cannot even log in** with the correct password.

You should also enable **login reminders** using text or email messages.

## 5. Don't Maintain Security Only for Inspections

Ken's Study Journey **emphasised many times** in **Study Tips Sharing lectures** to not follow rules **ONLY for inspections**. This only **disrespects inspectors' hard work** which will not have true effects.

Knowing the importance of Internet security, let's **actively** improve security awareness, avoiding security incidents like account hacking and data breach.

## 6. Follow Website Rules, Laws and Regulations

Developing state-of-the-art (modern) technologies like 5G, IPv6, AI (Artificial Intelligence), Big Data and IoT (Internet of Things), security also plays a critical role.

Every section of rules (e.g. Terms of Service (ToS)), laws and regulations is gold.

For example, the China Internet Security Law stated that websites must keep logs for at least 6 months, along with some relevant local industrial standards.

Knowing the importance of keeping logs, Ken's Study Journey servers logged and blocked many scanning attempts on Ken's Study Planner APIs and website WordPress modules from May to June 2023 (see Appendix 3 below). Having all unsuccessful scanning attempts, no security incidents occurred.

I usually say: "Let's Strengthen Security on State-of-the-art Technology", curbing abuse using high-tech products.

### Real Example

Discovering malicious scanning attempts, the bottom of the reminder notice includes a law content, in English, reminding users that Chinese Internet services keep activity logs.

## 7. Say "No" to Massive Website Scanning

Website Scanning is an essential attacking stage. Every successful scan means the beginning of an attack process.

This includes scanning login pages and APIs, where single-call APIs are more vulnerable to attacks since no CAPTCHAs are allowed on them.

Ken's Study Journey turned off APIs by default for new users, which should be enabled only when necessary, installing anti-crawl systems on login pages and logging all login and API call attempts.

Preventing scans means preventing attacks so let's stop massive website scanning.

## 8. Be Civilised and Avoid Abuse, being an Internet Security "Volunteer"

The Internet is also regulated by laws and regulations. Let's be civilised and avoid abuse, immediately reporting any suspicious activities.

Ken's Study Journey not only manages itself strictly but also is friendly to users, organising reminders and education, pointing out mistakes and improving awarenesses instead of banning accounts and/or IP addresses for the first time.

Some Internet services may ban accounts and/or IP addresses or add CAPTCHAs for abuse like scanning to maintain security. Don't be negatively impacted by threatening Internet security.

Please supervise together and be an Internet security "Volunteer".

Ken's Study Journey strives to maintain Internet security.

Ken's Study Journey

14 July 2023

Guangzhou, China

[www.kenstudyjourney.cn](http://www.kenstudyjourney.cn), [ken@kenstudyjourney.cn](mailto:ken@kenstudyjourney.cn)

## Appendix 1: Common Unusual Situations on Internet Platforms

1. Unusual **logins and login reminders** on your account.
2. Unusual actions displaying on Activity Logs in Settings.
3. **Automatically redirecting to other websites** or displaying other website content.  
(Login pages on Public WiFis excepted)
4. Private data changed without your permission/operation.
5. Can view/edit **other's** data on your account.

## Appendix 2: Common Abusive Activities on Internet Platforms

Note: This **also violates the Terms of Service** on many websites.

1. Massively scanning **usernames and passwords** on a website's login page,  
Note: Some websites have anti-crawl systems (e.g. CAPTCHA) installed.
2. Massively scanning **website API** links and keys, etc.,
3. Massively scanning **server hidden ports** (e.g. scan from Port 1 to 65535; TCP/80, TCP/443 and ICMP Ping are excepted),
4. Scanning **website admin panel** entrance and open-source modules (e.g. WordPress: "/wp-admin", "/wp-comments-post.php", "admin.\*\*\*.com").
5. Sending **massive useless requests** in a short time ((D)DoS or CC attacks).

### Appendix 3: Examples of Suspicious Access Logs (from Tor)

All were recorded and reported by GB-LHR-01 (London, UK) server:

IP Address	Date & Time (GMT+8, CST)	URL Accessed/Scanned	Browser/Device Type
185.130.**.** (Tor)	2023-06-12 14:36:**	https:// www.kenstudyjourney.cn/ wp-comments-post.php	Chrome, Windows
104.244.**.** (Tor)	2023-06-26 from 04:22:00 to 04:23:00	https:// www.kenstudyjourney.cn/ wp-admin/admin-ajax.php	Chrome, Android
23.154.**.** (Tor)			
192.42.**.** (Tor)	2023-06-26 from 04:24:15 to 04:25:00	https:// www.kenstudyjourney.cn/ wp-content/plugins/**/ download.php	
107.189.**.** (Tor)			
199.195.**.** (Tor)	2023-06-26 from 04:28:15 to 04:28:30	https:// www.kenstudyjourney.cn/ wp-content/themes/**/ view-pdf.php	
185.243.**.** (Tor)			
23.137.**.** (Tor)	2023-06-26 from 04:28:00 to 04:33:00	https:// www.kenstudyjourney.cn/ wp-content/themes/**/ download.php	
91.203.**.** (Tor)			