

# How to Check Website Safety - 2025

## 1. Check for HTTPS in the URL

A secure website's URL begins with [https://](#) (not just [http://](#)). The "S" stands for "Secure" and means the site is encrypted using SSL/TLS, protecting data transmitted between you and the website.

- Look for a **padlock icon** in the address bar.
- Avoid sites with a message like "Not Secure" in your browser's address bar.

**Note:** Though HTTPS is a good starting point, it doesn't automatically make a website completely trustworthy; it only ensures data encryption.

## 2. Verify the Website's Reputation

Use online tools and services to check the website's credibility. The following tools analyze websites for safety:

- **Google Safe Browsing:** Visit [Google Transparency Report](#) and input the website URL to check if Google has flagged it as dangerous.
- **Web of Trust (WOT):** Install the WOT browser extension or use the [WOT website](#) to see user reviews and safety ratings.
- **VirusTotal:** Paste the URL into [VirusTotal](#) to scan for malware, phishing, or other threats.
- **Norton Safe Web:** Use Norton Safe Web to evaluate the site's security reputation.

## 3. Inspect the Website's Domain

- **Double-check the URL:** Cybercriminals often create fake websites with URLs that mimic legitimate sites (e.g., "[g00gle.com](#)" instead of "[google.com](#)").

## 4. Look for Contact Information

Legitimate websites usually include accessible and trustworthy contact details, such as:

- A physical address
- A customer support email or phone number
- Links to verified social media accounts

## 1. ກວດເບິ່ງ HTTPS ໃນ URL

URL ຂອງເວັບໄຊທ໌ທີ່ປອດໄພເລີ່ມຕົ້ນດ້ວຍ https:// (ບໍ່ພຽງແຕ່ http://). "S" ຫຍໍ້ມາຈາກ "Secure" ແລະຫມາຍຄວາມວ່າເວັບໄຊທ໌ໄດ້ຖືກເຂົ້າລະຫັດໂດຍໃຊ້ SSL / TLS, ປົກປ້ອງຂໍ້ມູນທີ່ສົ່ງຜ່ານລະຫວ່າງທ່ານກັບເວັບໄຊທ໌.

ຊອກຫາໂອກາດ locklock ໃນແຖບທີ່ຢູ່.

ຫຼັກວິທີເວັບໄຊທ໌ມີຂໍ້ຄວາມເຊັ່ນ "ປອດໄພ" ໃນແຖບທີ່ຢູ່ຂອງຕົວທ່ອງເວັບຂອງທ່ານ.

ຫມາຍເຫດ: ເຖິງແມ່ນວ່າ HTTPS ເປັນຈຸດເລີ່ມຕົ້ນທີ່ດີ, ມັນບໍ່ໄດ້ເຮັດໃຫ້ເວັບໄຊທ໌ທີ່ຫນ້າເຊື່ອຖືຢ່າງສົມບູນ; ມັນພຽງແຕ່ຮັບປະກັນການເຂົ້າລະຫັດຂໍ້ມູນ.

## 2. ຍົນຢັນຊື່ສຽງຂອງເວັບໄຊທ໌

ໃຊ້ເຄື່ອງມືແລະການບໍລິການອອນໄລນ໌ເພື່ອກວດສອບຄວາມຫນ້າເຊື່ອຖືຂອງເວັບໄຊທ໌.

ເຄື່ອງມືຕໍ່ໄປນີ້ວິເຄາະເວັບໄຊທ໌ເພື່ອຄວາມປອດໄພ:

Google Safe Browsing: ເຂົ້າໄປເບິ່ງບົດລາຍງານຄວາມໂປ່ງໃສຂອງ Google ແລະໃສ່ URL ເວັບໄຊທ໌ເພື່ອກວດເບິ່ງວ່າ Google ໄດ້ທຸງມັນເປັນອັນຕະລາຍຫຼືບໍ່.

Web of Trust (WOT): ຕິດຕັ້ງສ່ວນຂະຫຍາຍຂອງຕົວທ່ອງເວັບ WOT ຫຼືໃຊ້ເວັບໄຊທ໌ WOT

ເພື່ອເບິ່ງການທົບທວນຄືນຂອງຜູ້ໃຊ້ແລະການຈັດອັນດັບຄວາມປອດໄພ.

VirusTotal: ວາງ URL ໃສ່ VirusTotal ເພື່ອສະແດງການຫາ malware, phishing ຫຼືໄພຂົ່ມຂູ່ອື່ນໆ.

Norton Safe Web: ໃຊ້ Norton Safe Web ເພື່ອປະເມີນຊື່ສຽງດ້ານຄວາມປອດໄພຂອງເວັບໄຊທ໌.

## 3. ກວດກາໂດເມນຂອງເວັບໄຊທ໌

ກວດເບິ່ງ URL ສອງຄັ້ງ: ຄະດີອາຍາທາງອິນເຕີເນັດມັກຈະສ້າງເວັບໄຊທ໌ປອມທີ່ມີ URLs ທີ່ mimic ເວັບໄຊທ໌ທີ່ຖືກຕ້ອງ (ເຊັ່ນ: "g00gle.com" ແທນ "google.com").

## 4. ຊອກຫາຂໍ້ມູນຕິດຕໍ່

ເວັບໄຊທ໌ທີ່ຖືກຕ້ອງຕາມກົດໝາຍມັກຈະມີລາຍລະອຽດການຕິດຕໍ່ທີ່ສາມາດເຂົ້າເຖິງໄດ້ ແລະເຊື່ອຖືໄດ້, ເຊັ່ນ:

ທີ່ຢູ່ທາງກາຍ

ອີເມວ ຫຼືເບີໂທລະສັບຊ່ວຍເຫຼືອລູກຄ້າ

ລິງຫາບັນຊີສື່ສັງຄົມທີ່ຍືນຍັນແລ້ວ

---

Revision #1

Created 10 January 2025 06:02:26 by Admin

Updated 10 January 2025 06:03:48 by Admin