

Cybersecurity Awareness

- [Use strong password to prevent from password theft -
ໃຊ້ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງເພື່ອປ້ອງກັນຈາກການລັກລະຫັດຜ່ານ](#)
- [How to prevent from Phishing attacks - ວິທີການປ້ອງກັນຈາກການໂຈມຕີ Phishing](#)
- [Lock your computer when you leave - ລັອກຄອມພິວເຕີຂອງທ່ານເມື່ອທ່ານອອກ](#)
- [Is this Website Safe? How to Check - ເວັບໄຊນີ້ປອດໄພບໍ່? ວິທີການກວດສອບ](#)
 - [How to Check Website Safety - 2025](#)

Use strong password to
prevent from password theft

-

ໃຊ້ລະຫັດຜ່ານທີ່ແຂ້ງແຂງເພື່ອປ້ອງກັນ
ຈາກການລັກລະຫັດຜ່ານ

u\$3_\$TRonG P@55W0rDs



Step up your password game by
using a phrase and incorporating
lookalike characters.

All passwords should be:

Length: At least 8 characters long.

Unique: Never reuse passwords

Random: Use a random string of mixed-case letters, numbers and symbols, like: PxH1#n!8.

Keep your passwords safe by keeping in a safe place or use a password manager, like Lasspass.

Below is an example:



Figure 1: Example for a secure password

ໃຊ້ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງເພື່ອປ້ອງກັນຈາກການລັກລະຫັດຜ່ານ

ລະຫັດຜ່ານທັງໝົດຄວນຈະເປັນ:

ຄວາມຍາວ: ຢ່າງໜ້ອຍ 8 ຕົວອັກສອນຍາວ.

ເປັນເອກະລັກ: ຢ່າໃຊ້ລະຫັດຜ່ານຄືນໃໝ່

ສຸມ: ໃຊ້ສະຕຣິງສຸມຂອງຕົວພິມນ້ອຍ, ຕົວເລກ ແລະ ສັນຍາລັກ, ເຊັ່ນ: PxH1#n!8.

ຮັກສາລະຫັດຜ່ານຂອງທ່ານໃຫ້ປອດໄພໂດຍການເກັບຮັກສາໄວ້ໃນບ່ອນທີ່ປອດໄພ
ທີ່ໃຊ້ຕົວຈິດການລະຫັດຜ່ານ ເຊັ່ນ: Lasspass.

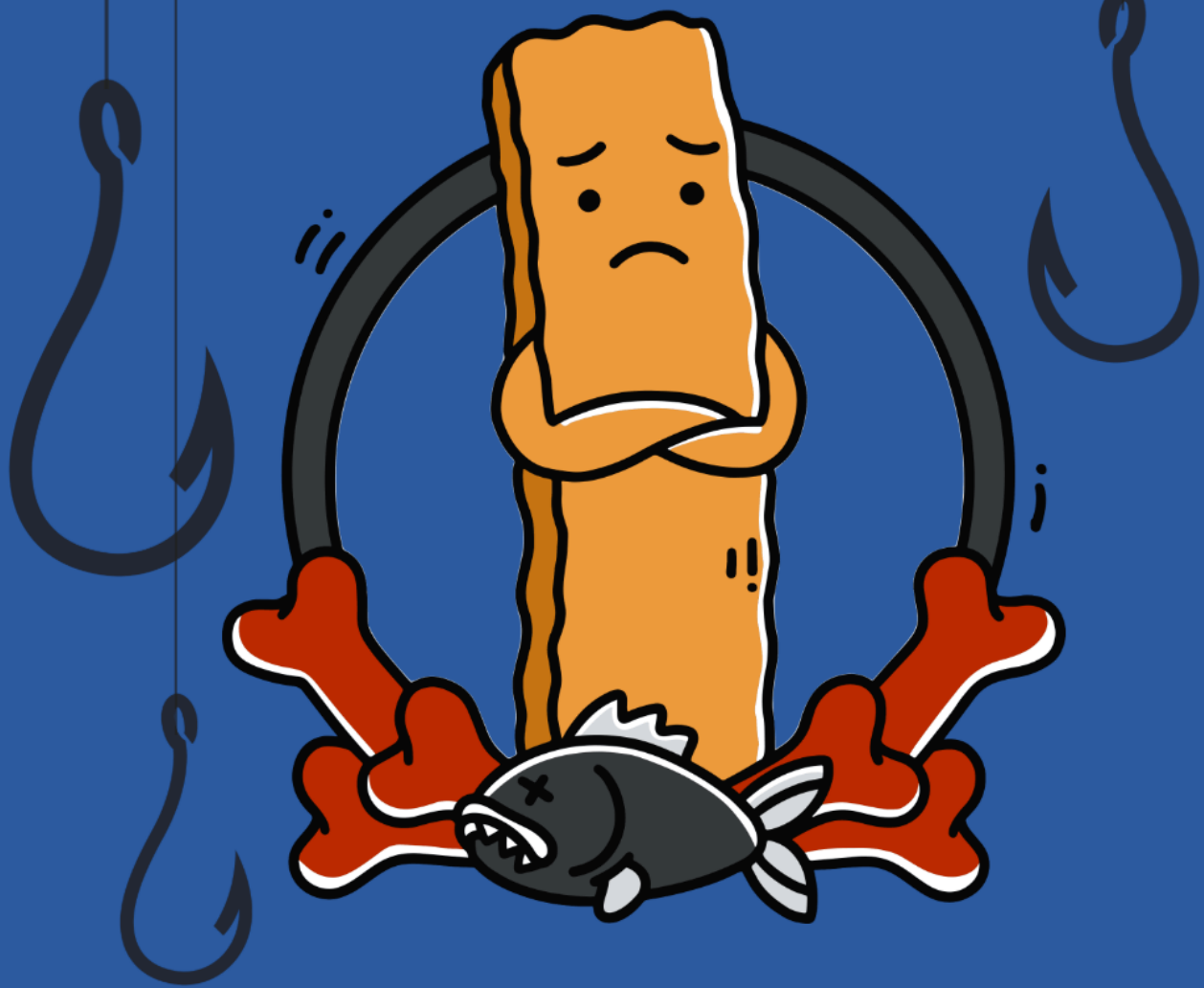
How to prevent from

Phishing attacks -

ວິທີການປ້ອງກັນຈາກການໂຈມຕີ

Phishing

Don't Be the Office Phish Fingers!



Avoid phishing by watching for urgent tones, unfamiliar senders, poor grammar and suspicious links.

Prevent Phishing attacks by avoiding suspicious links, verifying sender identities, enabling multi-factor authentication, updating software, and educating users regularly.

ປ້ອງກັນການໂຈມຕີ Phishing ໂດຍການຫຼີກເວັ້ນການເຊື່ອມຕໍ່ທີ່ໜ້າສົງໄສ, ຢັ້ງຢືນຕົວຕົນຂອງຜູ້ສົ່ງ, ເປີດໃຊ້ການກວດສອບຄວາມຖືກຕ້ອງຫຼາຍປັດໃຈ, ຮັບເດດຊອບແວ ແລະໃຫ້ການສຶກສາຜູ້ໃຊ້ເປັນປົກກະຕິ.

rnicrosoft.co.uk

support@rnicrosoft.co.uk

16/01/2023 11:44

FAKE

From: support@rnicrosoft.co.uk

Sent: 16/01/2023 11:44

To: Bob Smith <Bob.Smith@company.com>

Subject: Urgent Action Needed!

Urgent



Microsoft Account

email account?

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

space

calander

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.live.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

REAL?

From: support@microsoft.co.uk

Sent: 16/01/2023 11:44

To: Bob Smith <Bob.Smith@company.com>

Subject: Unusual Sign In Activity



Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account [bo*****@company.com](#). you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

Thanks,
The Microsoft Team

context

Lock your computer when
you leave -

ລັອກຄອມພິວເຕີຂອງທ່ານເມື່ອທ່ານອອກ

Secure Your Workspace



If you're leaving it, lock it!

Is this Website Safe? How to Check - ເວັບໄຊທີ່ນີ້ປອດໄພບໍ?

ວິທີການກວດສອບ

In this digital world, **Check a website is safe** is the most critical concern since there are countless [malicious websites](#) available everywhere over the Internet

ໃນໂລກດິຈິຕອລນີ້,

ການກວດສອບເວັບໄຊທີ່ແມ່ນປອດໄພແມ່ນຄວາມກັງວົນທີ່ມີຄວາມສໍາຄັນທີ່ສຸດນັບຕັ້ງແຕ່ມີເວັບໄຊທີ່ອັນຕະລາຍນັບບໍ່ຖ້ວນທີ່ມີຢູ່ໃນຫົວທຸກແຫ່ງໃນອິນເຕີເນັດ.

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