

CYBER HYGIENE



CYBER HYGIENE

- ขั้นตอนที่ผู้ใช้คอมพิวเตอร์และอุปกรณ์อื่นๆ สามารถปฏิบัติได้ เพื่อปรับปรุงความปลอดภัยออนไลน์และรักษาความพร้อมใช้งานของระบบ
- การใช้ความคิดและพฤติกรรมที่เน้นความปลอดภัยเป็นหลัก ซึ่งช่วยในการรักษาอุปกรณ์ที่ทำงานอย่างถูกต้องโดยปกป้องอุปกรณ์จากการโจมตีภายนอก เช่น มัลแวร์ ซึ่งอาจขัดขวางการทำงาน



CYBER HYGIENE

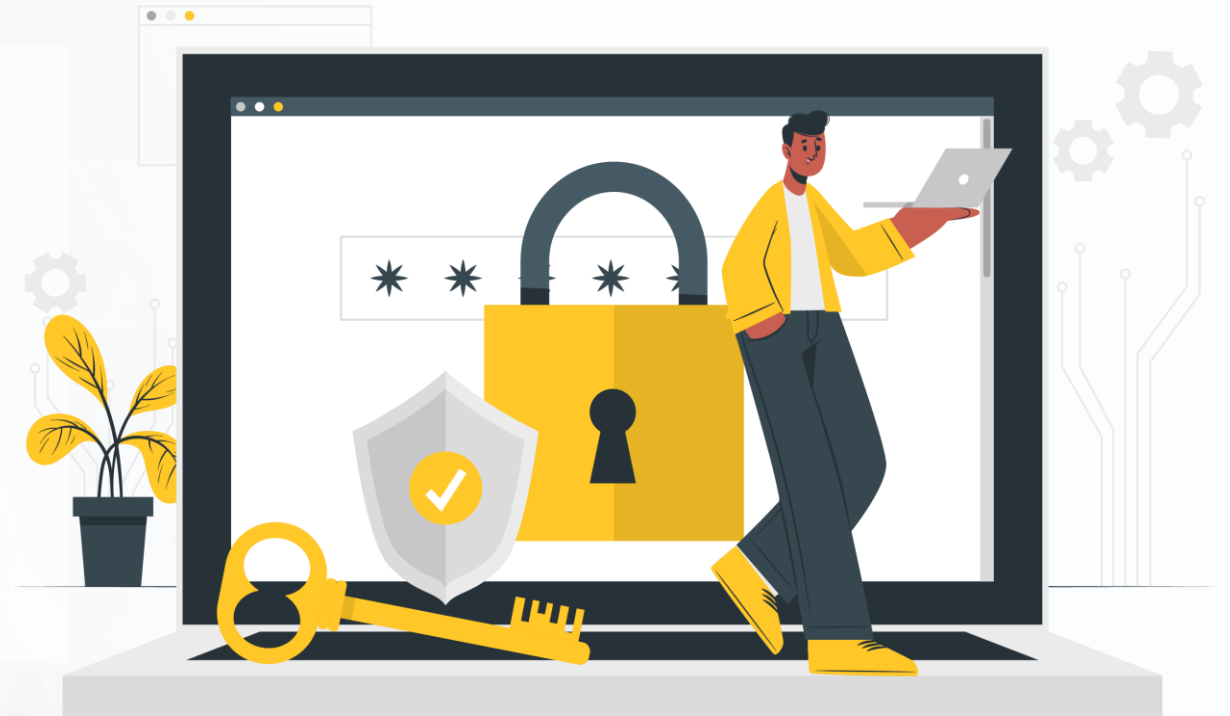
- Cyber Hygiene เกี่ยวข้องกับแนวทางปฏิบัติและข้อควรระวังที่ผู้ใช้ดำเนินการ โดยมีจุดประสงค์เพื่อจัดระเบียบข้อมูลที่สำคัญ ปลอดภัย และปลอดภัยจากการโจรกรรมและการโจมตีจากภายนอก
- ช่วยให้ผู้บุคคลและองค์กรสามารถบรรเทาการบุกรุกที่เกิดจากภัยคุกคามอาจเกิดขึ้นได้



CYBER HYGIENE

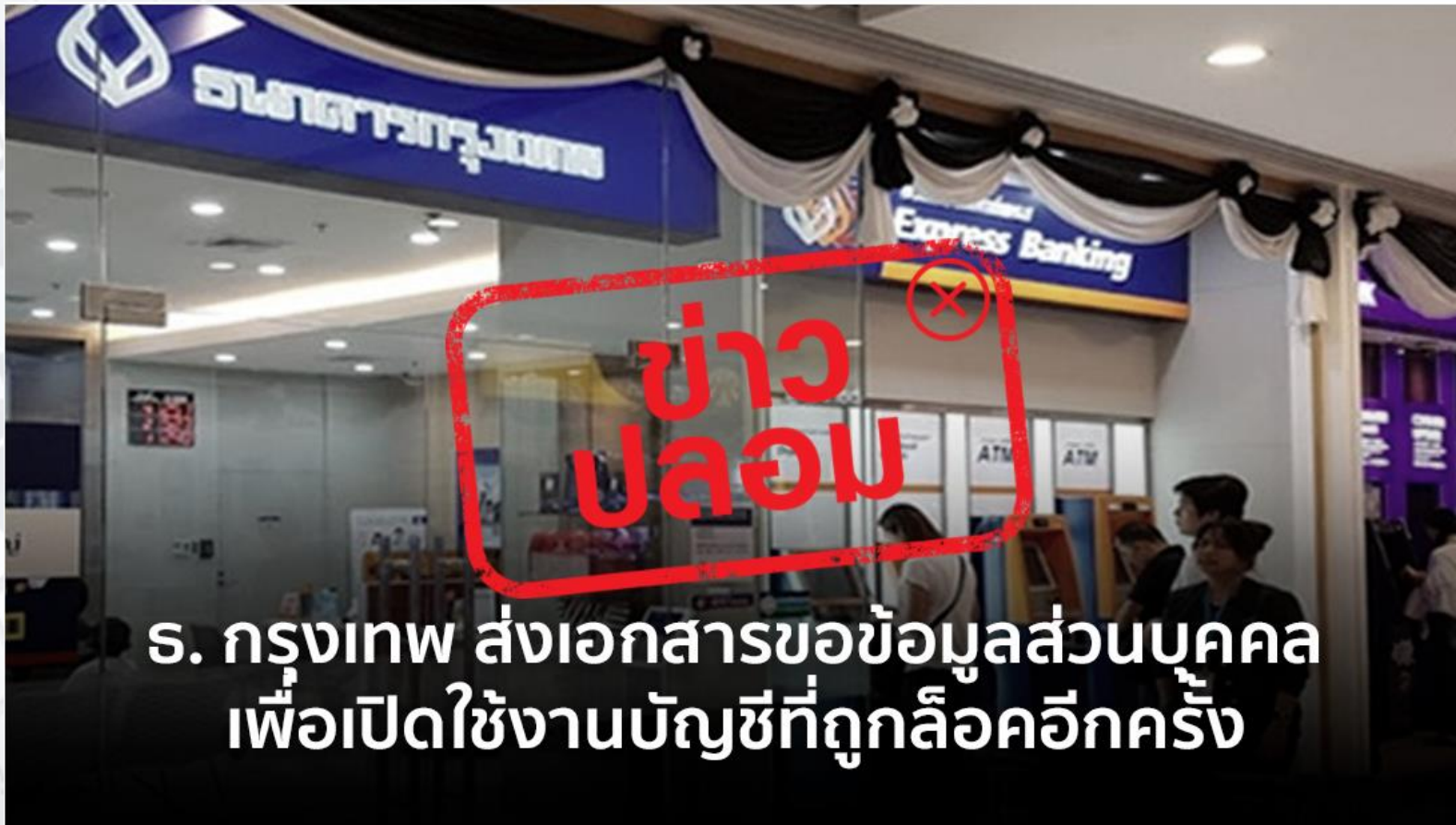
➤ เก็บข้อมูลส่วนบุคคลเป็นความลับ

- ข้อมูลส่วนบุคคล เช่น วันเกิด หมายเลขบัตรประชาชน และข้อมูลที่ระบุถึงตัวตนของเราได้ (Personally Identifiable Information: PII) เพื่อป้องกันการปลอมแปลงตัวตน



CYBER HYGIENE

➤ เก็บข้อมูลส่วนบุคคลเป็นความลับ



CYBER HYGIENE

➤ เก็บข้อมูลส่วนบุคคลเป็นความลับ



CYBER HYGIENE

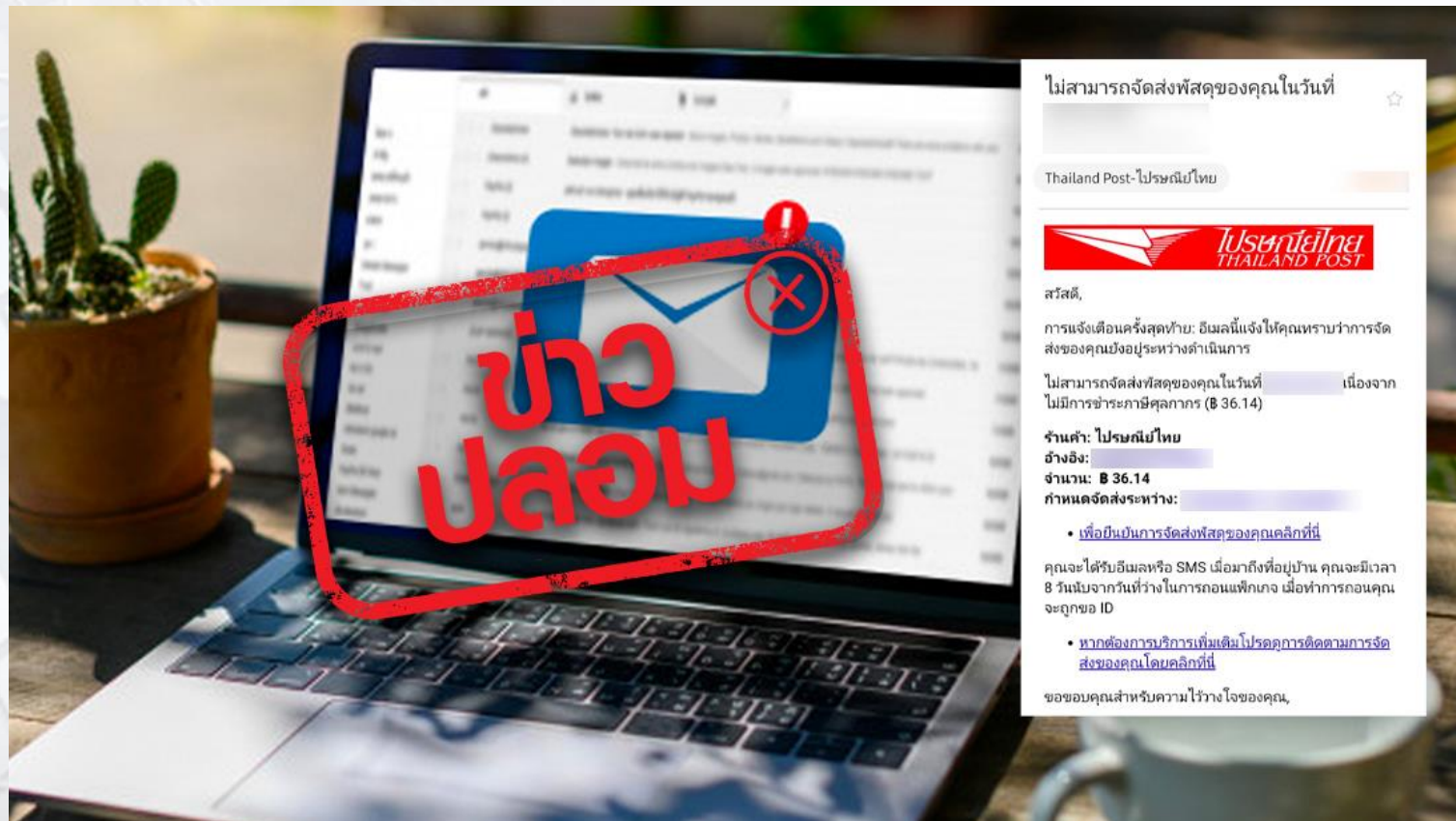
➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์

- ระมัดระวังการเปิดอีเมลที่มาจากผู้ไม่ประสงค์ดี แม้ว่าอีเมลเหล่านั้นจะดูเหมือนว่ามาจากบุคคลหรือองค์กรที่ไว้ใจได้ สามารถสังเกตได้จากการใช้ **ไวยกรณ์ผิดๆ** **การร้องขอแบบเร่งด่วน** รวมไปถึงการขอรหัสผ่านหรือข้อมูลส่วนบุคคล



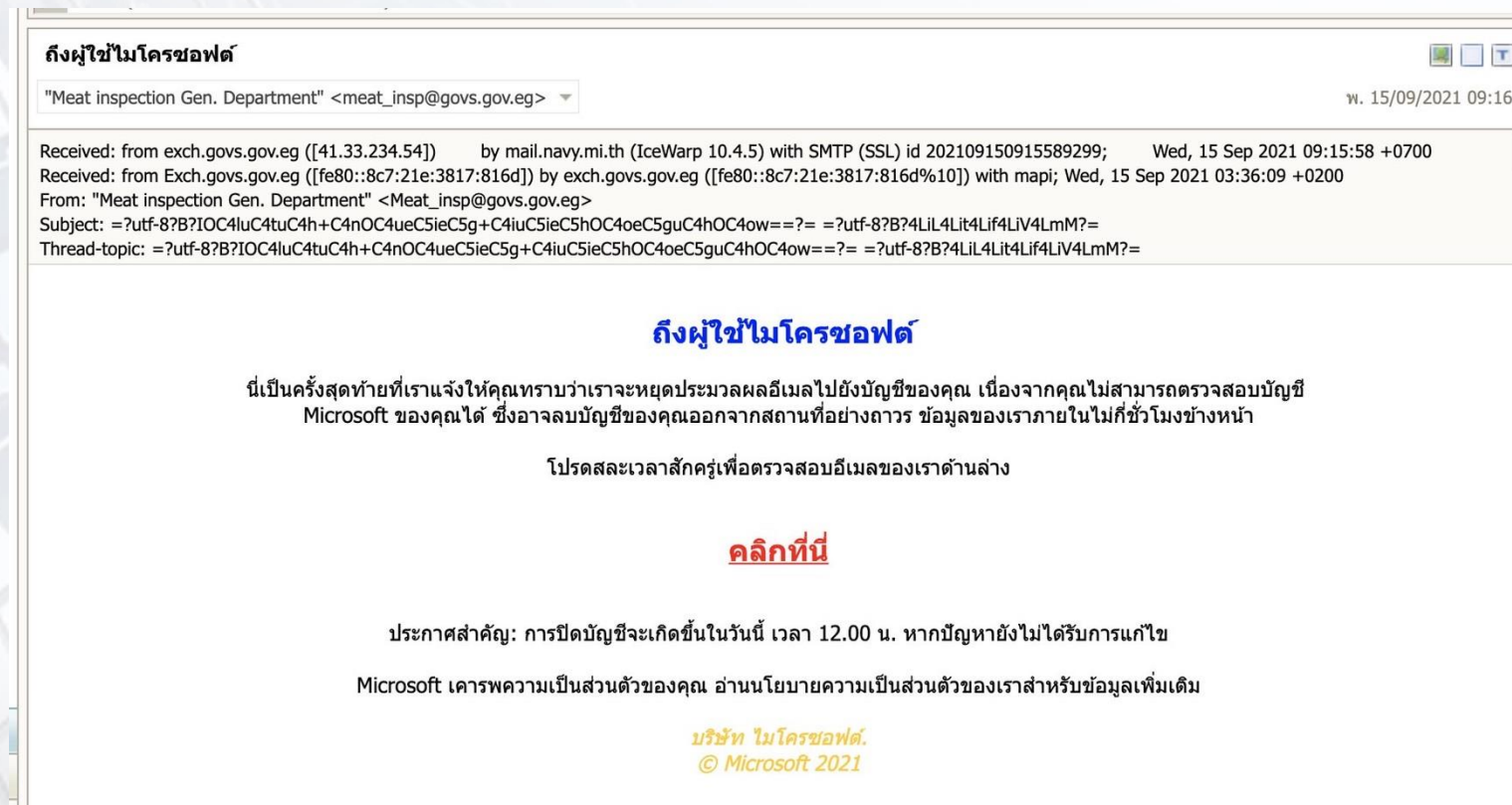
CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์



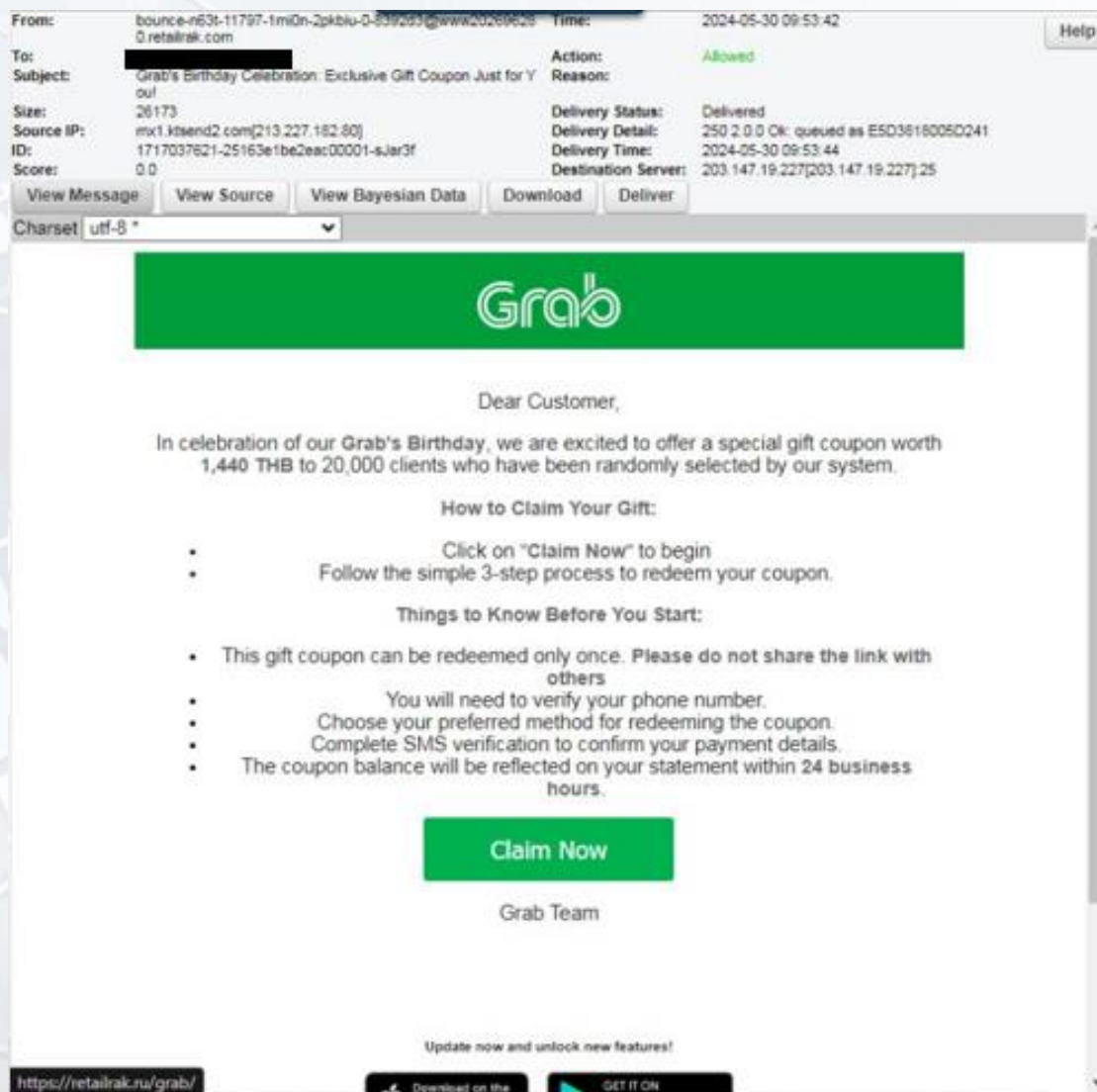
CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์



CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์



CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์

✖ ไม่ปลอดภัย https://203.147.19.148/cgi-mod/view_message_log_detail.cgi?cgi_type=view_message_log_detail&bess_recip...

From:	clients@thedreamiseverything.com	Time:	2024-05-27 14:24:18	Help
To:	[REDACTED]	Action:	Allowed	
Subject:	Account Blocked	Reason:		
Size:	9442	Delivery Status:	Delivered	
Source IP:	v111202.serveradd.com[43.245.111.202]	Delivery Detail:	250 2.0.0 Ok: queued as 4FCD218006652D	
ID:	1716794658-25163e1be1ddd60001-dCs589	Delivery Time:	2024-05-27 14:24:18	
Score:	2.9	Destination Server:	203.147.19.227[203.147.19.227]:25	

[View Message](#) [View Source](#) [View Bayesian Data](#) [Download](#) [Deliver](#)

Charset [iso-8859-1 *](#)

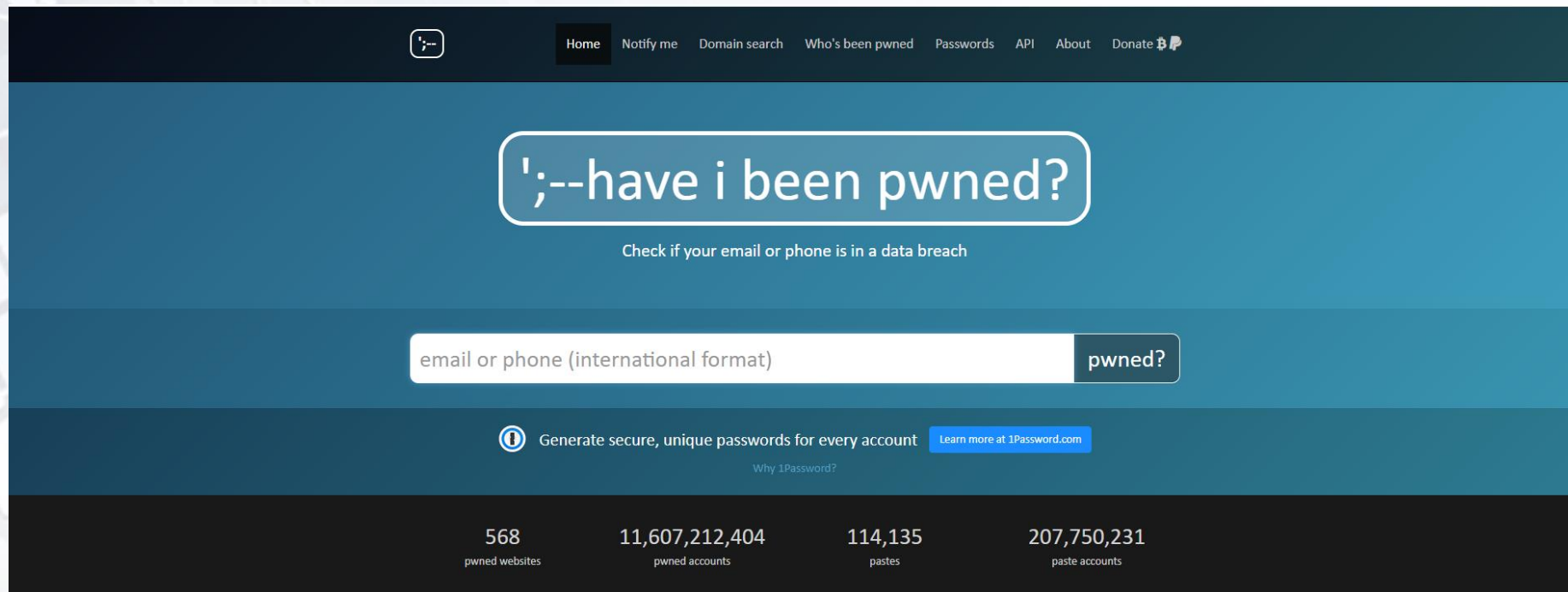
Dear zimbra user,

To enable you to use the new zimbra system, we are currently upgrading our email server to zimbra 2.0. To activate your account [click here](#)

Administration
All rights reserved.
©2024

CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์



The screenshot shows the homepage of the 'have i been pwned' website. The header is dark blue with a navigation menu including 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'Passwords', 'API', 'About', and 'Donate'. The main content area has a large blue background with a white rounded rectangle containing the text '';--have i been pwned?'. Below this is a smaller text 'Check if your email or phone is in a data breach'. A search bar with the placeholder 'email or phone (international format)' and a 'pwned?' button is present. A banner for 1Password is also visible, with the text 'Generate secure, unique passwords for every account' and a link 'Learn more at 1Password.com'. The footer is dark blue and displays statistics: 568 pwned websites, 11,607,212,404 pwned accounts, 114,135 pastes, and 207,750,231 paste accounts.

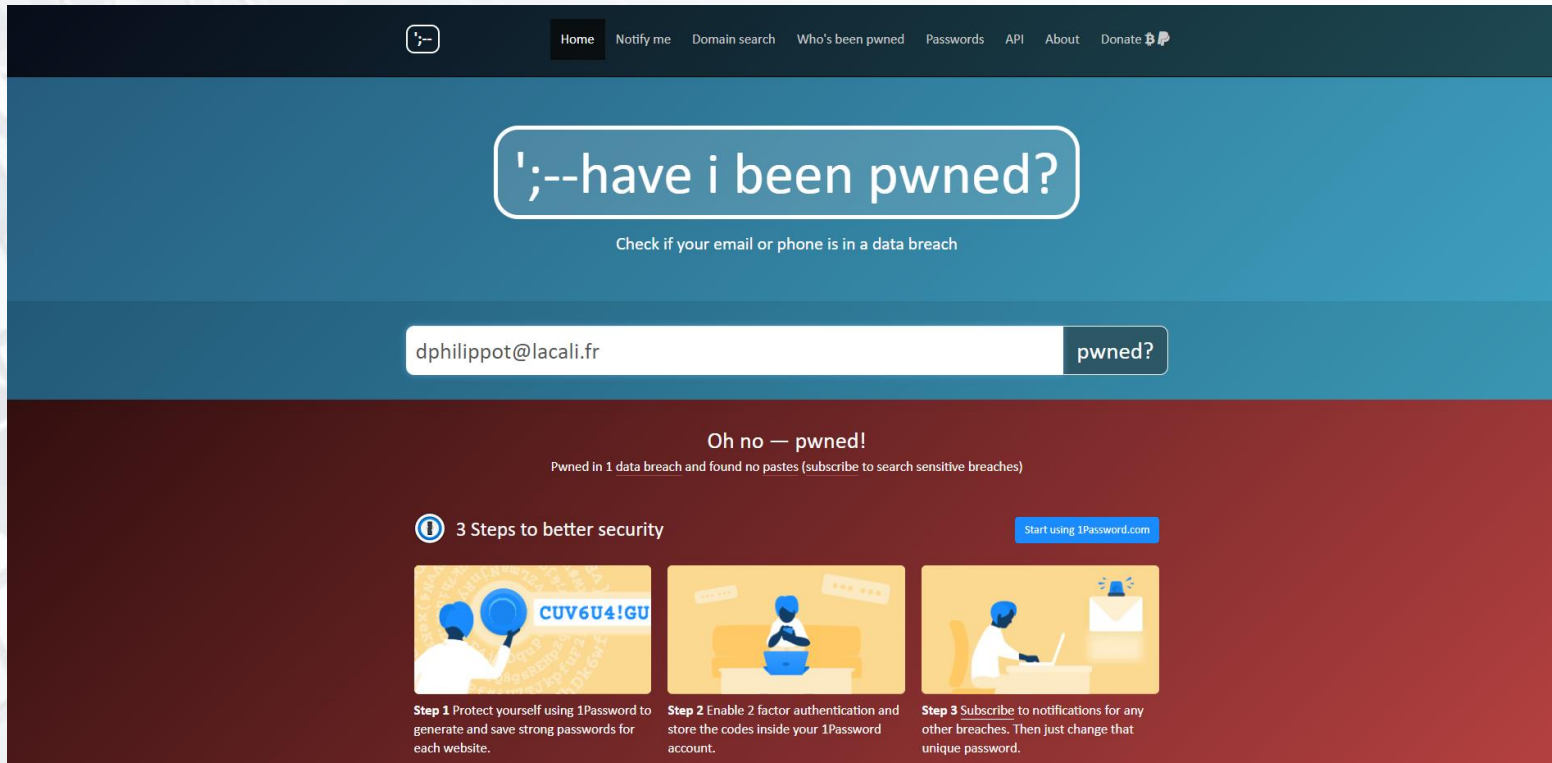
Category	Count
pwned websites	568
pwned accounts	11,607,212,404
pastes	114,135
paste accounts	207,750,231

<https://haveibeenpwned.com/>

CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ

อาชญากรไซเบอร์



The screenshot shows the homepage of the 'have i been pwned' website. The header is dark blue with a navigation menu: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a blue background with the text 'have i been pwned?' in a white box. Below this is a search bar containing the email 'dphilippot@lacali.fr' and a button labeled 'pwned?'. The results section has a red background and shows 'Oh no — pwned!' with a subtext 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Below this is a section titled '3 Steps to better security' with a 'Start using 1Password.com' button. The steps are: Step 1: Protect yourself using 1Password to generate and save strong passwords for each website. Step 2: Enable 2 factor authentication and store the codes inside your 1Password account. Step 3: Subscribe to notifications for any other breaches. Then just change that unique password.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

dphilippot@lacali.fr pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

<https://haveibeenpwned.com/>

CYBER HYGIENE

➤ ระมัดระวังไม่ให้ตกเป็นเหยื่อ
อาชญากรไซเบอร์



<https://www.virustotal.com>

CYBER HYGIENE

➤ หมั่นอัปเดตซอฟต์แวร์สม่ำเสมอ

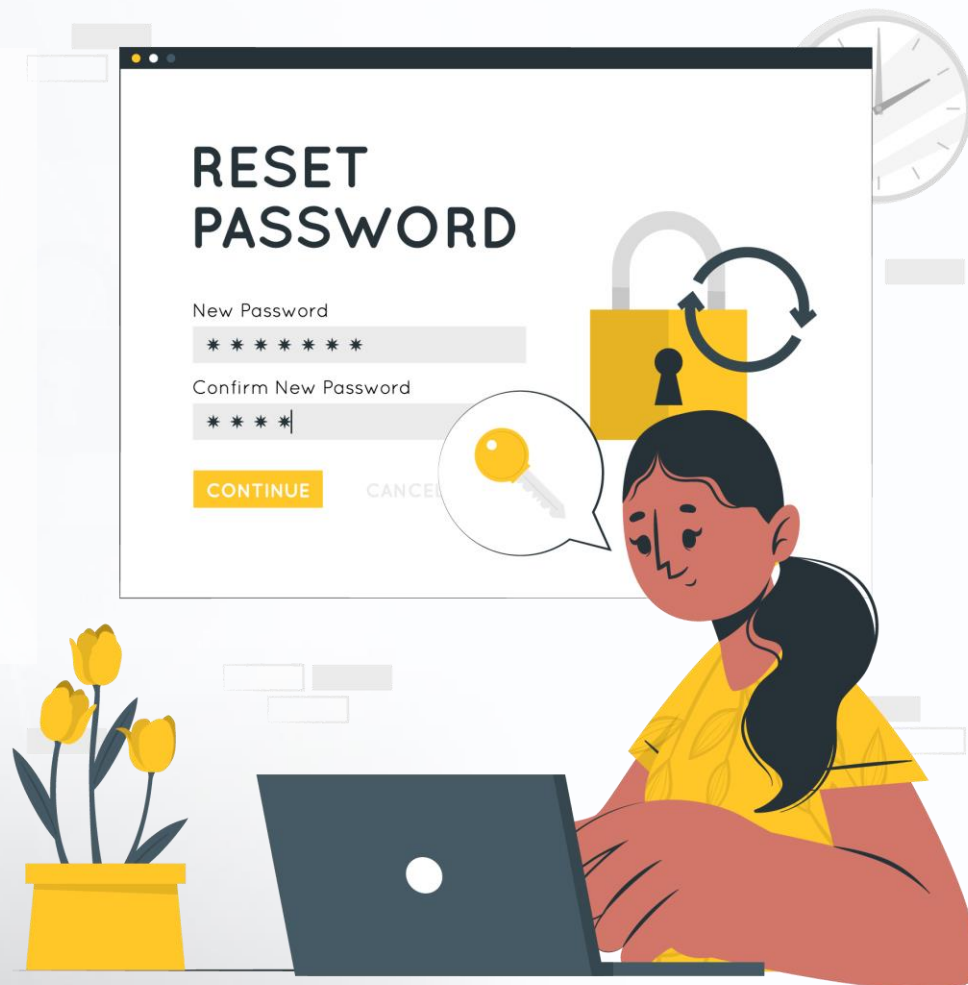
- อาชญากรไซเบอร์มักใช้ประโยชน์จากช่องโหว่บนซอฟต์แวร์ที่ยังไม่ได้รับการแพตช์ การหมั่นอัปเดตซอฟต์แวร์ให้ใหม่ล่าสุดอยู่เสมอจึงเป็นหนึ่งในวิธีที่ดีที่สุดในการสร้างความมั่นคงปลอดภัย



CYBER HYGIENE

➤ สร้างรหัสผ่านที่แข็งแกร่งและหมั่นเปลี่ยน
รหัสผ่านอย่างสม่ำเสมอ

- สร้างรหัสผ่านที่แข็งแกร่ง มีการใช้ตัวพิมพ์ใหญ่
ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ โดย
รหัสผ่านที่ดีควรมีความยาวมากกว่า 12
ตัวอักษร แยกใช้รหัสผ่านไม่ซ้ำกันในแต่ละบริการ
ออนไลน์



CYBER HYGIENE

➤ ใช้การพิสูจน์ตัวตนแบบ Multi-factor

- การเพิ่มอีกหนึ่งปัจจัยในการพิสูจน์ตัวตน นอกเหนือจาก Username และ Password
- ช่วยยกระดับความมั่นคงปลอดภัยให้แก่บัญชีออนไลน์ได้อย่างมหาศาล สามารถป้องกันการโจมตีแบบ Phishing, Social Engineering และ Password Brute Force Attacks ได้



CYBER HYGIENE

➤ ระวังการใช้ Wi-Fi สาธารณะ

- Wi-Fi ฟรีหรือ Wi-Fi สาธารณะเสี่ยงต่อการถูกโจมตีได้ง่าย **อาชญากรไซเบอร์สามารถดักฟังข้อมูล** เช่น ข้อมูลส่วนบุคคล ที่ส่งไปมาบนเครือข่ายไร้สายได้
- เมื่อมีความจำเป็นต้องใช้ Wi-Fi สาธารณะ ให้หลีกเลี่ยงเว็บไซต์ที่มีการใช้หรือจัดเก็บข้อมูลส่วนบุคคล เช่น ธนาคารออนไลน์ โซเชียลมีเดีย หรือช้อปปิ้งออนไลน์ เป็นต้น



CYBER HYGIENE

➤ อย่าหลือร่องรอยไซเบอร์ไว้บนอุปกรณ์
สาธารณะที่ใช้งานร่วมกัน

- การหลือข้อมูลหรือร่องรอยบางอย่างไว้บนอุปกรณ์อาจทำให้ผู้ใช้คนอื่นๆ สามารถเข้าถึงข้อมูลของเราได้ ดังนั้น ก่อนที่จะเลิกใช้งาน ควรยกเลิกการบันทึกรหัสผ่านบนอุปกรณ์หรือเบราว์เซอร์ ล็อกเอาต์ออกจากระบบต่างๆ รวมไปถึงการลบ Cookie รวมไปถึงประวัติการเข้าถึงเว็บทิ้งไปให้หมด



CYBER HYGIENE

➤ ตั้งค่าความเป็นส่วนบุคคลบนอุปกรณ์ต่างๆ

- การตั้งค่าความมั่นคงปลอดภัยและความเป็นส่วนบุคคลบนอุปกรณ์ บริการออนไลน์ และแอปพลิเคชันต่างๆ ช่วยเพิ่มความมั่นคงปลอดภัยให้แก่การดำเนินกิจกรรมบนโลกไซเบอร์มากยิ่งขึ้น



CYBER HYGIENE

➤ หมั่นตรวจสอบแอปพลิเคชันที่ได้ติดตั้งและใช้งานอยู่เสมอ

- ควรตรวจสอบ **Permission** ที่แอปพลิเคชันร้องขอ และเลือกอนุญาตเฉพาะสิ่งที่จำเป็นเท่านั้น โดยเฉพาะอย่างยิ่งเมื่อมีการร้องขอสิทธิ์การเข้าถึง Camera Roll, Microphone หรือ Keystrokes



CYBER HYGIENE

➤ เดินหน้ารักษาความมั่นคงปลอดภัยไปด้วยกัน

- แสร้งความรู้ด้านความมั่นคงปลอดภัยที่ได้เหล่านี้ไปยังเพื่อนๆ และญาติๆ ของตนเอง เพื่อยกระดับความตระหนักด้านภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์

