



Security Awareness

การรับรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์



แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น

Cyber Hygiene



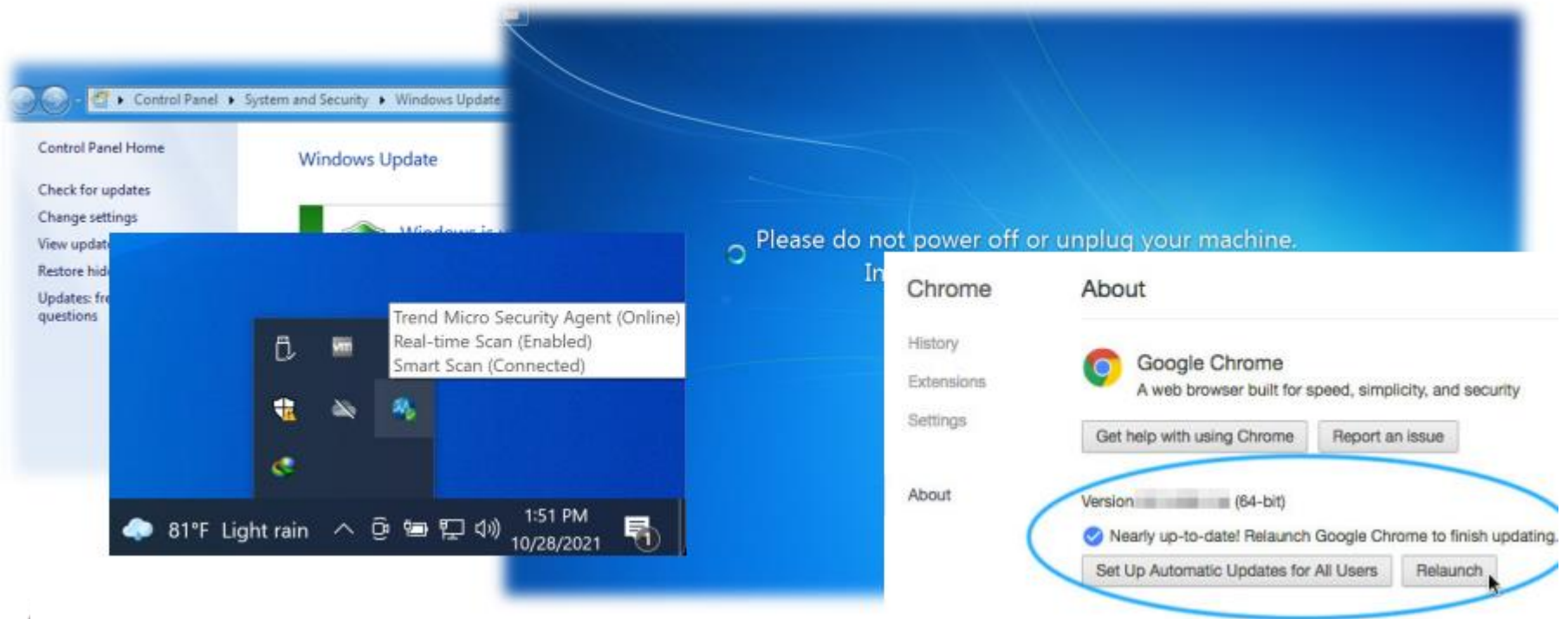
Security Checklist สำหรับการใช้เครื่องคอมพิวเตอร์

1. ควร Logout ทุกครั้งเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
2. ทำการอัปเดตแพตช์บนระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ หรือตั้งค่าอัปเดตอัตโนมัติ
3. ทำการอัปเดตซอฟต์แวร์ / โปรแกรมบนเครื่องอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ในเวอร์ชันก่อนหน้า
4. ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสบนเครื่องคอมพิวเตอร์และตั้งค่าการอัปเดตอัตโนมัติเพื่อรับข้อมูลการป้องกันใหม่ล่าสุด
5. เปิด Windows Firewall บน OS
6. ไม่ดาวน์โหลดโปรแกรมมาจากแหล่งที่ไม่น่าเชื่อถือ และหมั่นลบโปรแกรมที่ไม่จำเป็นออก



Keep Yourself Up to Date

Don't Forget to Spare Your Time Before Go Home



Security Checklist สำหรับโทรศัพท์มือถือและแท็บเล็ต

1. เปิดการใช้งาน Passcode, Face ID และ Fingerprint ในการเข้าใช้งานอุปกรณ์ต่างๆ
2. ทำการอัปเดตแพตช์บนระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ หรือตั้งค่าอัปเดตอัตโนมัติ
3. ทำการอัปเดตซอฟต์แวร์ / โปรแกรมบนเครื่องอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ในเวอร์ชันก่อนหน้า
4. ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสแบบ Mobile และตั้งค่าการอัปเดตอัตโนมัติเพื่อรับข้อมูลการป้องกันใหม่ล่าสุด
5. ไม่ติดตั้งแอปพลิเคชันที่น่าสงสัย หรือไม่ทราบผู้พัฒนาที่แน่ชัด
6. กำหนดสิทธิในการเข้าถึงแอปพลิเคชัน (permission) ให้เหมาะสม
7. ปิดการแจ้งเตือนเกี่ยวกับรหัสความปลอดภัยเช่น OTP บนหน้าจอ
8. เลี่ยงการเก็บข้อมูลสำคัญเอาไว้ในโทรศัพท์มือถือ



How to ยกระดับความปลอดภัย บัตรเดบิต/เครดิต ด้วยตัวคุณเอง

ทำได้ง่ายๆ ที่ SCB EASY App

- หากพบความผิดปกติ ระวังการใช้อ่านบัตรช้อคราว
 - 1. เช็กเมนู "บันชีงบอดิน"
 - 2. เช็กประวัติธุรกรรม
 - 3. เช็ก "บันชีงบอดิน" สาขา (เลือกรุ่นและสาขาให้ตรงกับสาขา)
 - 4. กด "แจ้งเตือน" เพื่อแจ้งเตือนหากมีการเปลี่ยนแปลง
 - 5. ติดต่อคอลเซ็นเตอร์
- หากต้องการเปลี่ยนแปลงวงเงินกดเงินสดและชำระสินค้า
 - 1. เช็กเมนู "บันชีงบอดิน"
 - 2. เช็ก "บัตรเดบิต/เครดิต" ที่เลือก
 - 3. เช็กเมนู "บันชีงบอดิน" สาขา (เลือกรุ่นและสาขาให้ตรงกับสาขา)
 - 4. กด "แจ้งเตือน" เพื่อแจ้งเตือนหากมีการเปลี่ยนแปลง
 - 5. ติดต่อคอลเซ็นเตอร์
- หากต้องการให้แจ้งเตือนธุรกรรมผ่าน SCB Connect
 - LINE Official Accounts @SCBCONNECT
 - หรือ QR Code
 - หรือ Line ID

ติดต่อขอความช่วยเหลือ โทร. 02-777-7777 หรือ visit scb.com

1. SCB Call Center 02-777-7777
2. Facebook Inbox SCB Thailand
3. E-mail : customer_service@scb.co.th

ลูกค้าสามารถปรับเปลี่ยนวงเงิน หรือปิดบัตรชั่วคราวด้วยตนเอง ผ่านหลายช่องทางของธนาคาร

- ปิดการใช้งานชั่วคราว หรือ การปรับเปลี่ยนวงเงิน สำหรับบัตรกรุงศรี เอบีซี จีดี ดี ทีเอ็มวี**
 - บัตรกรุงศรี เอบีซี จีดี ดี ทีเอ็มวี (วงเงิน) > บริการบัตรกรุงศรี > บริการปรับวงเงินบัตร > "ปิดการใช้งาน"
 - บัตร Krungsri Boarding Card ไม่ใช้บัตร Krungsri Boarding Card > บริการปรับวงเงินบัตร > "ปิดการใช้งาน"
- บัตรกรุงศรี เอบีซี จีดี ดี ทีเอ็มวี**
 - ไม่ใช้บัตรกรุงศรี เอบีซี จีดี ดี ทีเอ็มวี > บริการบัตรกรุงศรี > บริการปรับวงเงินบัตร > "ปิดการใช้งาน"
- บัตร Krungsri Boarding Card**
 - ไม่ใช้บัตร Krungsri Boarding Card > บริการปรับวงเงินบัตร > บริการปรับวงเงินบัตร > "ปิดการใช้งาน"
- การปรับเปลี่ยนวงเงิน สำหรับบัตรเดบิต ทุกรุ่น**
 - ATM (ตู้ที่ให้บริการ) > โฉลก > บัตรกรุงศรี > ปรับวงเงิน > บัตรเดบิต > บัตรกรุงศรี
 - Krungrsri online (www.krungrsri.com) > บัตร > verified by visa > ปรับวงเงินบัตร > เลือก "ปรับเปลี่ยนวงเงิน" > เลือกเงิน "0 บาท"

เพิ่มความมั่นใจในการใช้งานบัตร ทีทีบี

ควบคุมการใช้งานบัตรด้วยตัวเองได้ง่ายๆ ผ่านแอป ttb touch

- เปิด/ปิด การใช้งาน**
 - ผ่านแอป ttb touch
 - ผ่านเว็บไซต์
 - ผ่านตู้ ATM
 - ผ่านสาขา
- ปรับ เพิ่ม/ลด วงเงินการใช้จ่าย**
 - ผ่านแอป ttb touch
 - ผ่านเว็บไซต์
 - ผ่านตู้ ATM
 - ผ่านสาขา
- เปิดการแจ้งเตือนผ่านแอป**
 - ผ่านแอป ttb touch
 - ผ่านเว็บไซต์
 - ผ่านตู้ ATM
 - ผ่านสาขา

พกบัตรอย่างมั่นใจ

เปลี่ยนแปลงวงเงินชำระค่าสินค้าและบริการ บัตรบีพีเอส สมาร์ท **ได้ง่ายๆ ด้วยตนเอง**

ผ่านมือถือ โทร. 1333

ผ่านเว็บไซต์ โทร. 1333

เมนูสำหรับเปลี่ยนแปลงวงเงินชำระค่าสินค้าและบริการด้วยตนเอง

- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333
- กดปุ่มวงเงิน โทร. 1333

วงเงินชำระค่าสินค้าและบริการ (บาท)	ค่าธรรมเนียม (บาท)
1	5,000
2	20,000
3	50,000
4	100,000
5	150,000
6	วงเงินเต็ม

หมายเหตุ: การเปลี่ยนแปลงวงเงินชำระค่าสินค้าและบริการด้วยตนเอง จะดำเนินการโดยอัตโนมัติในวันรุ่งขึ้น

บัตรเดบิตกรุงไทย

มั่นใจทุกการใช้จ่าย

เพิ่มความปลอดภัยด้วยวิธีง่ายๆ

- เลือกเปิด/ปิด การใช้งานชั่วคราว ผ่านแอป Krungthai NEXT
- ปรับลด/เพิ่มวงเงินในการใช้จ่ายชั่วคราว ผ่าน Krungthai Contact Center 02 111 1111 หรือ ธนาคารกรุงไทย ทุกสาขา
- แจ้งเตือนเงินเข้า-เงินออก ผ่าน LINE Krungthai Connex

กรุณาลูกค้าพบรายการชำระเงินออนไลน์ ผ่านบัตรเดบิตกรุงไทย โดยไม่ได้ทำธุรกรรมด้วยตนเอง กรุณาแจ้งธนาคารเพื่อตรวจสอบทันทีที่ Krungthai Contact Center 02-111-1111 หรือ ธนาคารกรุงไทย ทุกสาขา

Security Checklist สำหรับการใช้งาน

1. เปลี่ยนรหัสผ่านของอุปกรณ์ Wi-Fi router ที่บ้าน ไม่ใช่ค่าตั้งต้นที่กำหนดมาจากโรงงานผู้ผลิต (Default)
2. เปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดจากผู้ให้บริการและซ่อน SSID หากเป็นไปได้
3. กำหนดผู้ที่สามารถเชื่อมต่อ Wi-Fi ที่บ้านของเราได้ เช่น การล็อกให้เฉพาะเครื่องที่มี Mac address ที่กำหนดไว้ เข้าใช้งานได้เท่านั้น
4. ไม่เชื่อมต่อ Public Wi-Fi หรือ Free hotspot ที่เปิดให้ใช้งานได้ฟรีแบบไม่มีรหัสผ่าน
5. หลีกเลี่ยงการใช้งาน Public Wi-Fi ที่ไม่ทราบแหล่งที่มาในการเปิดให้บริการ
6. เมื่อออกจากบ้านควรปิดสัญญาณ Wi-Fi เพื่อป้องกันการเชื่อมต่อ Public Wi-Fi อัตโนมัติ



Security Checklist สำหรับการเข้าถึงเว็บไซต์

1. ใช้ Browser ที่ได้มาตรฐานและมีการอัปเดตเวอร์ชันของ Web Browser เสมอ
2. ไม่ทำการจดจำหรือบันทึกรหัสผ่าน (Password) ในการเข้าถึงเว็บไซต์ต่างๆ บน Browser
3. ไม่มีอะไรได้มาฟรีๆ ไม่ตื่นตระหนก ไม่หลงเชื่ออะไรง่ายๆ
4. ไม่เข้าใช้งานเว็บไซต์ที่ได้รับการแชร์จากช่องทางที่ไม่แน่ชัด เช่น จากโซเชียลมีเดีย เป็นต้น
5. สังเกต HTTPS เสมอ เมื่อต้องการเข้าใช้งานเว็บไซต์ที่เกี่ยวข้องกับการทำธุรกรรมต่างๆ หรือต้องมีการกรอกข้อมูลในการเข้าใช้งาน



Fake Maybank Website



The image compares two versions of the Maybank2u website. The left version is a 'Fake Website' with an 'Insecure Connection' (http://www.totalcoat.com/...). The right version is a 'Legitimate Website' with a 'Secured Site' (https://www.maybank2u.com.my/...). The legitimate site features a 'Security Tips' sidebar and a 'Maybank2u kini dalam Bahasa Malaysia' banner.

Fake Website
URL: <http://www.totalcoat.com/TONTONNDNDNDNDQ/m2uSession/Welcome.html>
Connection: Insecure Connection (http://)

Legitimate Website
URL: <https://www.maybank2u.com.my/m2u/common/M2ULogin.do?action=Login>
Connection: Secured Site (https://) Identified by The USERtrust...

Legitimate Website Content:
Welcome to Maybank2u
Please use your Online Banking username and password to log in.
Username: Next
Password: Next
Buttons: Self Reset Password, First time Login
Have you forgotten your password?
You can reset your password anytime by yourself by clicking the "Self Reset Password" button above.
Forgot Username/Password, Register Now
Have you forgotten your username or password?
Reset your login details by clicking "Forgot Username/Password"
English | Bahasa Malaysia
Maybank2u kini dalam Bahasa Malaysia
Login to Online Stocks, View & pay bills online
Should there be any irregularities or for other banking queries, please contact our Maybank Group Customer Care at 1300 88 6688 or 603-7844 3696 (overseas) immediately.

เว็บไซต์หลอกลวงที่ดูน่าเชื่อถือ

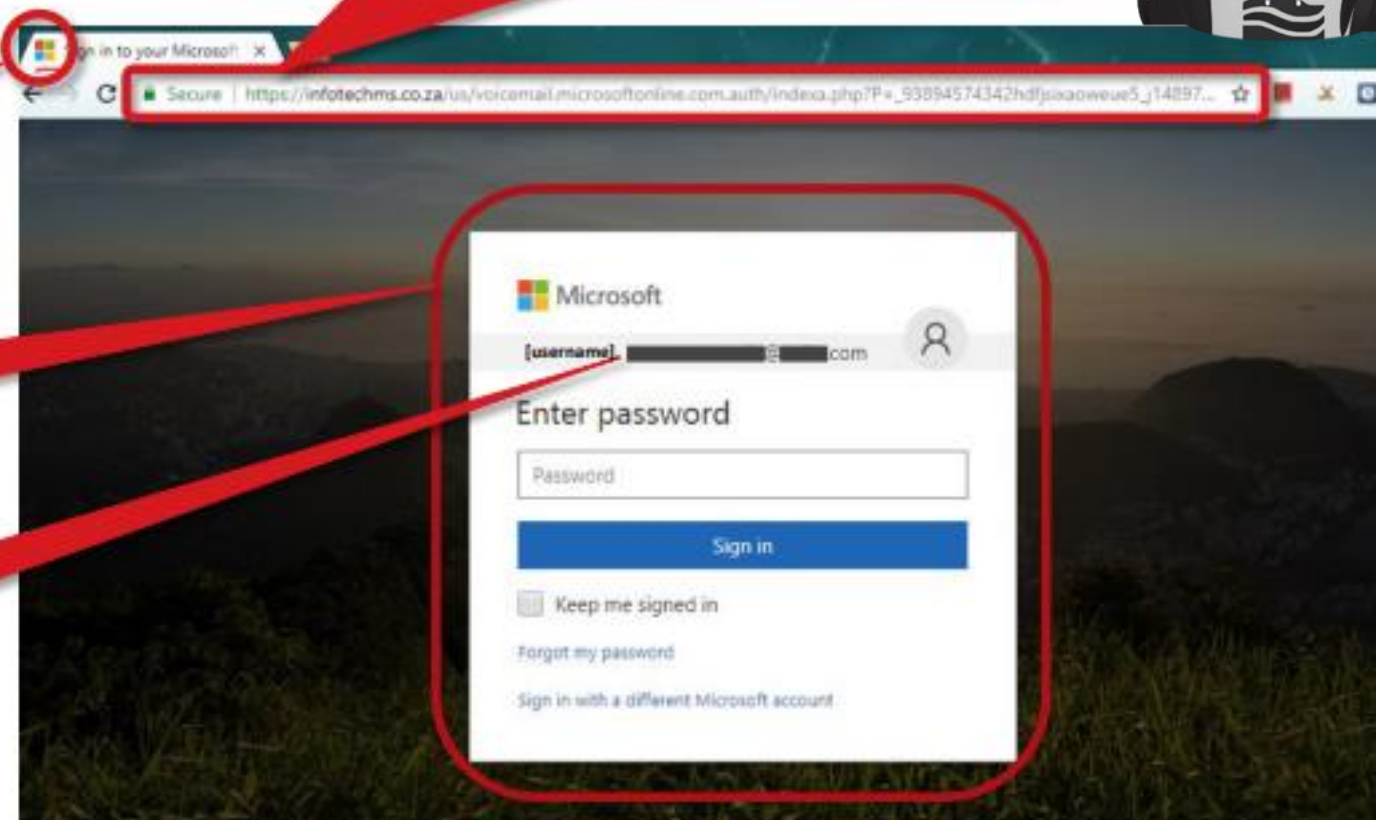


เป็น URL ปลอม แต่บางครั้งมีเครื่องหมาย SSL และจดทะเบียนด้วยโดเมนที่ถูกต้อง

Favicon มีความเหมือนหรือคล้ายกับเว็บไซต์นั้นจริง ๆ

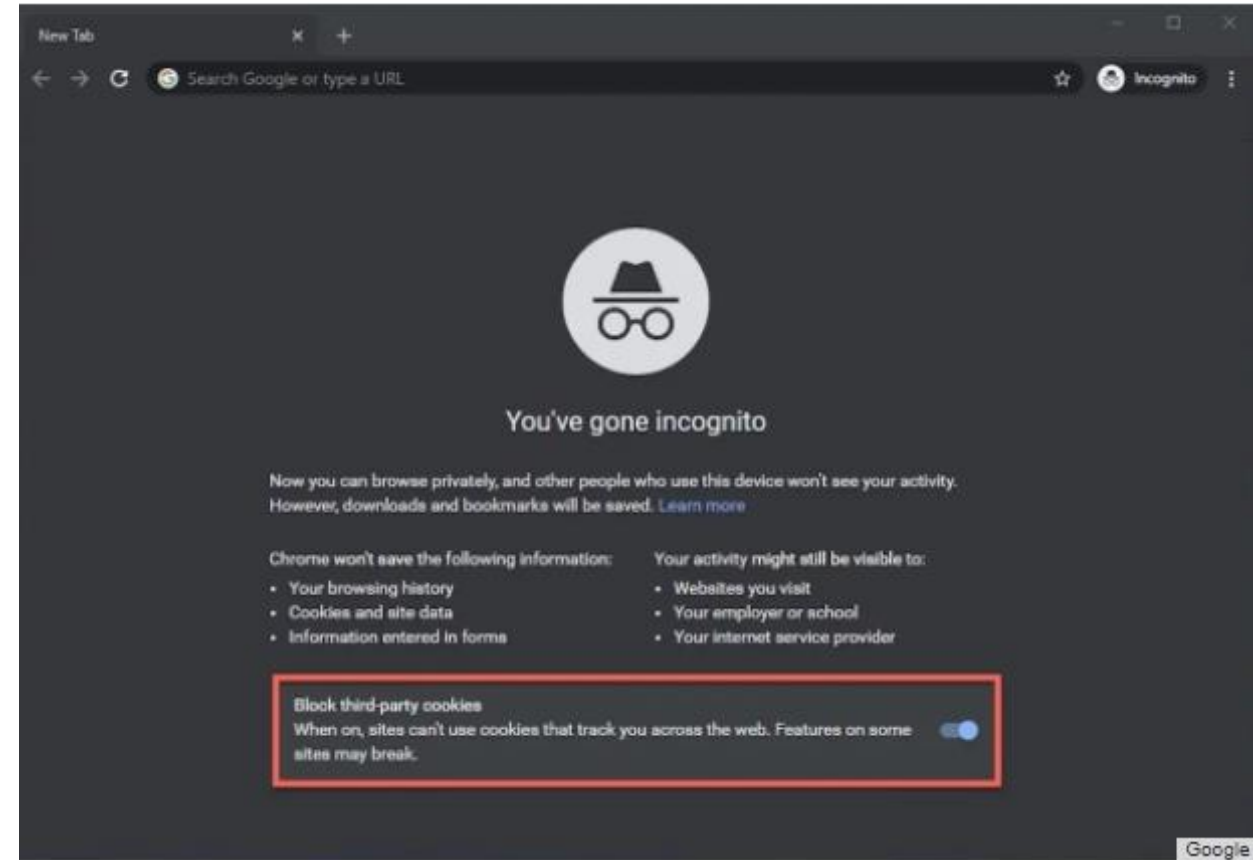
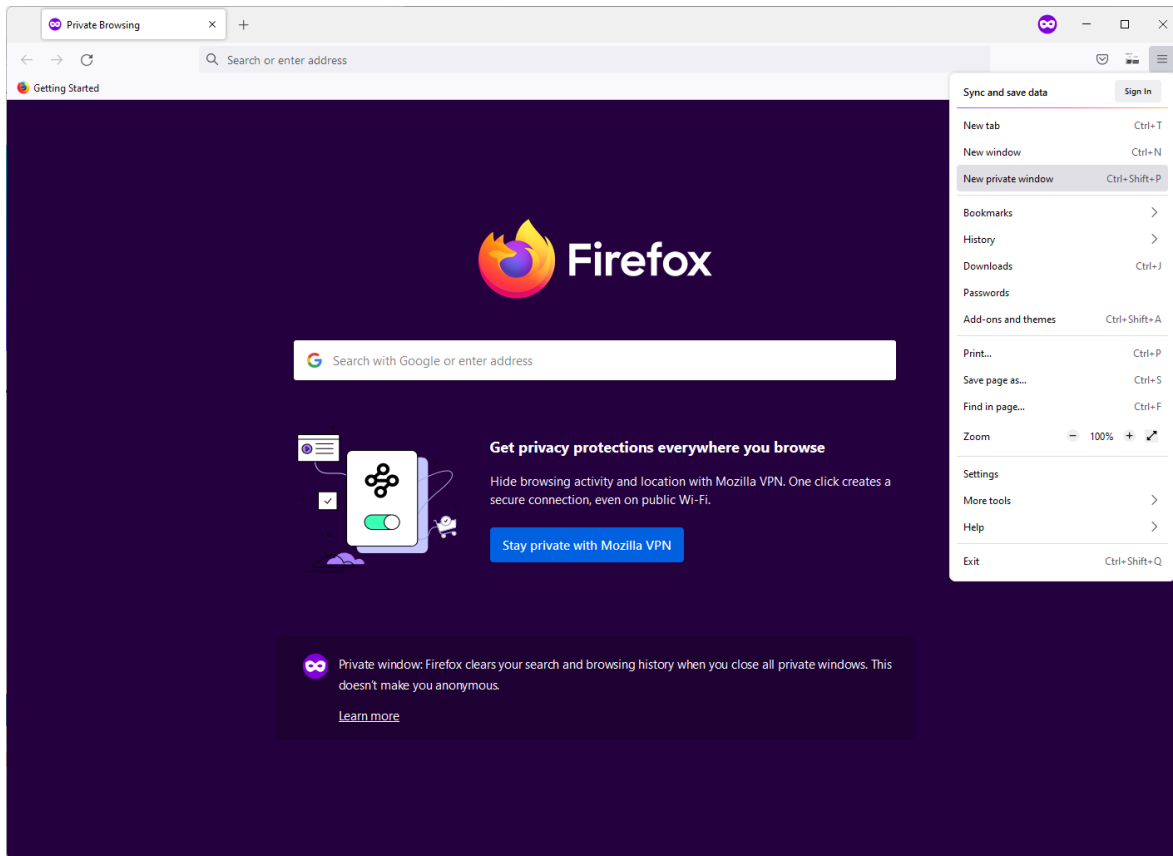
แบบฟอร์มเข้าสู่ระบบคล้ายกับเว็บไซต์จริง

แสดงที่อยู่อีเมลของผู้ใช้ในรูปแบบที่ถูกต้อง



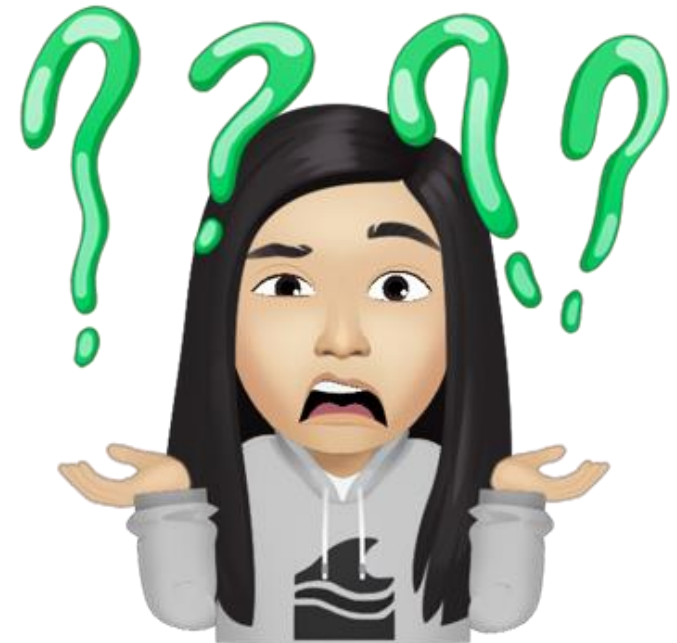
เข้าใช้งานผ่าน Private / Incognito Mode

เมื่อไม่ได้ใช้งานจากเครื่องส่วนตัว



Security Checklist สำหรับข่าวปลอม (Fake News)

1. มีการพาดหัวข่าว หรือข้อความที่กล่าวอ้างเกินจริงเพื่อสร้างความน่าสนใจ
2. ส่วนใหญ่จะถูกเผยแพร่ผ่านทางโซเชียลมีเดีย เช่น LINE, Facebook เป็นต้น
3. ระบุที่มาของข่าวไม่ได้
4. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
5. จำนวนการเขียนออกแนวการโฆษณา
6. เป็นข่าวแนวการสร้างกระแสหรือแนวทางปฏิบัติที่ผิด
7. ไฟล์แนบต่างๆ มักจะเป็นไฟล์ไม่ดี ห้ามดาวน์โหลดเด็ดขาด



ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

<https://www.antifakenewscenter.com/>



ข่าวปลอม อย่าแชร์! กรุงเทพฯ ออมสินปล่อยสินเชื่อเงินกู้เพิ่มทุน 5,000 - 500,000 บาท ผ่อน 24 เดือน ผ่านทาง...

! ข่าวปลอม การเงิน-หุ้น

17 มกราคม 2565 | 16:00 น.



ข่าวปลอม อย่าแชร์! สูตรเครื่องดื่มรักษาโรคน้ำอ้วกรซีสามารถรักษาโรคมะเร็งได้

! ข่าวปลอม ผลกระทบสุขภาพ

17 มกราคม 2565 | 14:30 น.



บขส. มอบส่วนลดค่าเครื่องดื่ม ภายในสถานีขนส่งหมอชิต2 ถึง 31 ธ.ค. 65 จริงหรือ?

✓ ข่าวจริง นโยบายรัฐบาล-ข่าวสาร

17 มกราคม 2565 | 13:00 น.



ข่าวบิดเบือน เชื้อโควิด-19 สายพันธุ์โอมิครอนไม่โจมตีปอด ทำให้อาการเจ็บป่วยไม่รุนแรง

? ข่าวบิดเบือน ผลกระทบสุขภาพ



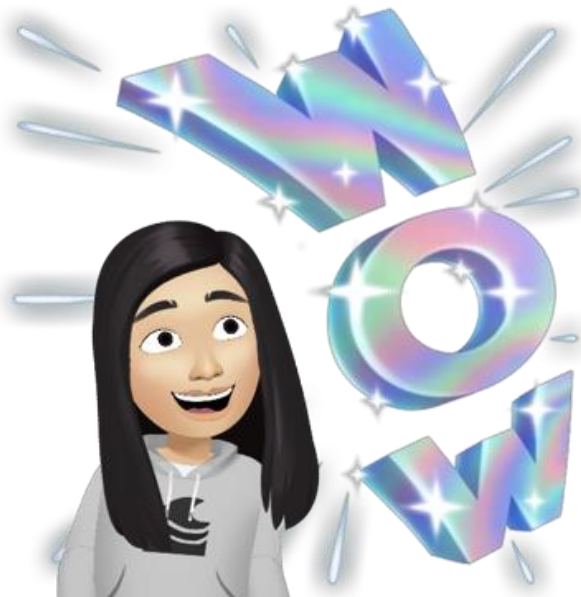
ศูนย์ฉีดวัคซีนกลางบางซื่อ เปิดรับวัคซีนฉีดวัคซีนเข็ม 1 และ 2 เท่านั้น จริงหรือ?

✓ ข่าวจริง นโยบายรัฐบาล-ข่าวสาร



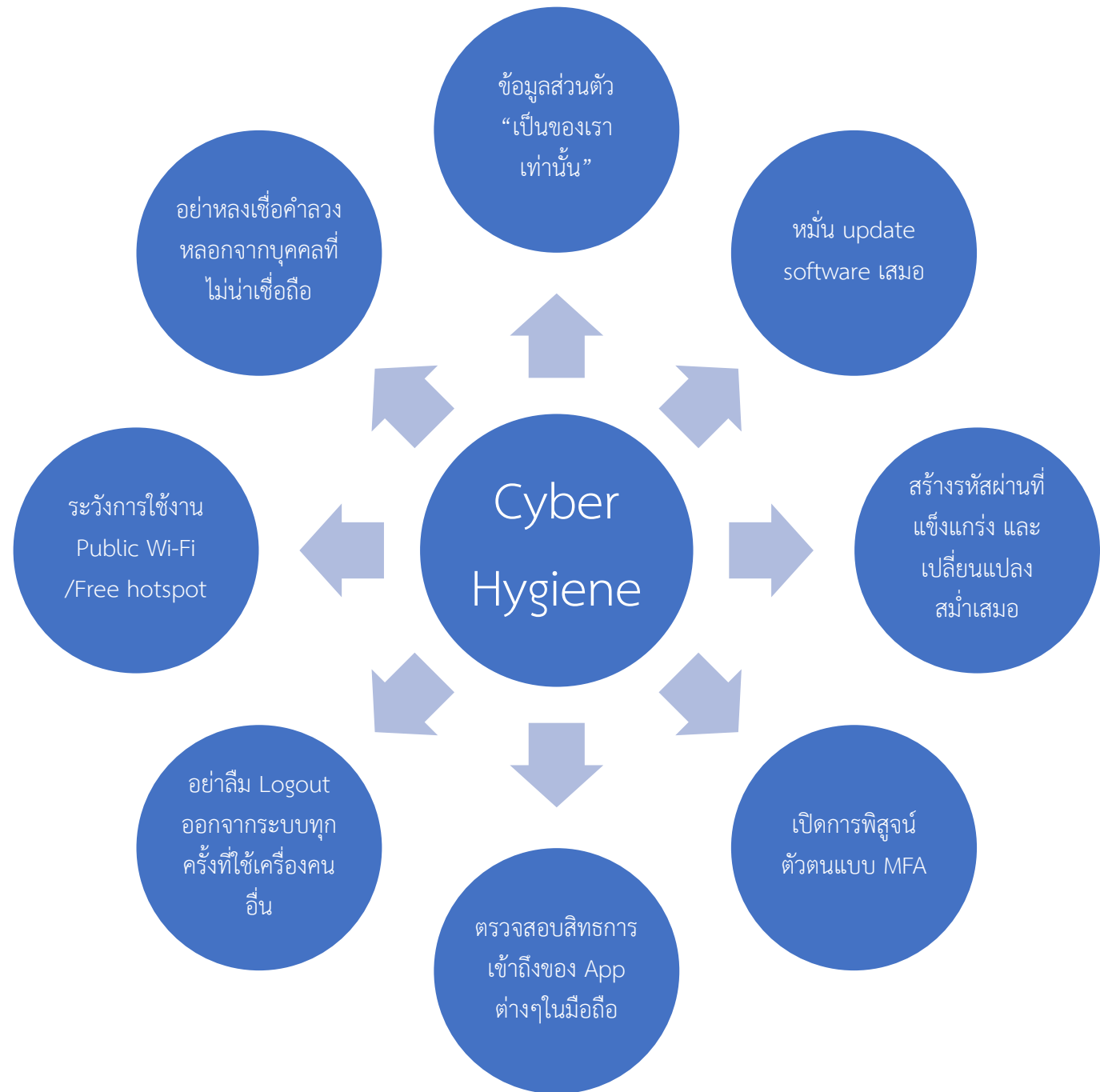
ข่าวบิดเบือน รัฐบาลเตรียมเก็บค่าใช้น้ำทำนา ไร่ละ 25 บาทต่อปี

? ข่าวบิดเบือน นโยบายรัฐบาล-ข่าวสาร

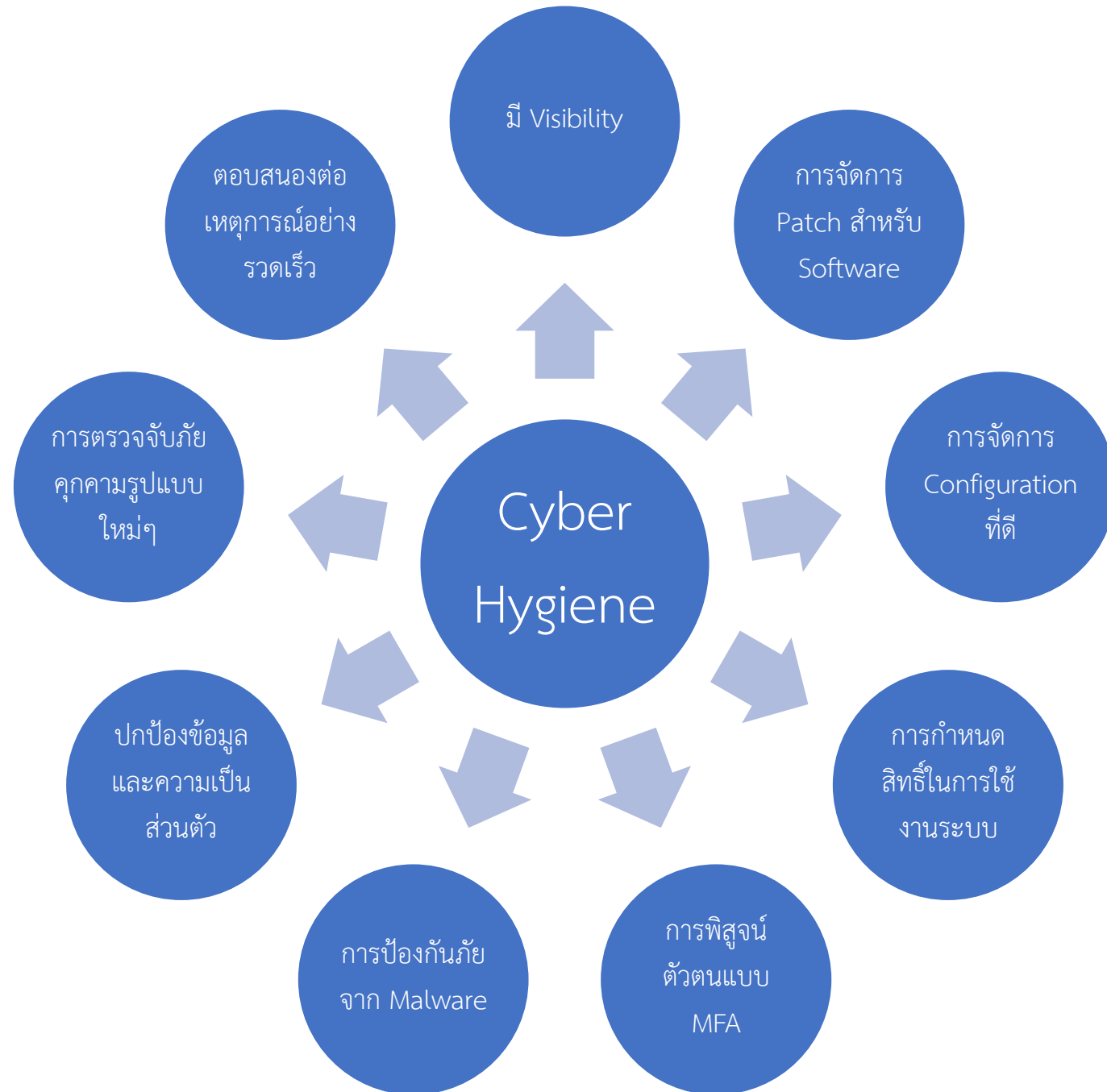


Cyber Hygiene

สำหรับผู้ใช้งานทั่วไป



Cyber Hygiene สำหรับองค์กร



เทคโนโลยีหรือผลิตภัณฑ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

Firewall



Cloud Security



Web Application Firewall



Sandboxing



Endpoint / Server Security



Data Loss Prevention



Intrusion Prevention



Mobile Security



Web Proxy



Extended Detection & Response (XDR)



Security Checklist สำหรับการ WFH

1. มีโปรแกรมป้องกันไวรัส ป้องกันการเจาะช่องโหว่ของระบบและป้องกันการรั่วไหลของข้อมูล / การเชื่อมต่อจากอุปกรณ์ไม่พึงประสงค์ติดตั้งบนเครื่องของพนักงาน
2. บริหารจัดการเรื่อง VPN License และ Bandwidth ให้เพียงพอ
3. จำกัดสิทธิในการเข้าถึงระบบงานภายในจากการเชื่อมต่อ VPN
4. อนุญาตให้เข้าใช้ VPN ได้ 12 ชั่วโมงต่อวัน / 1 พนักงาน และตัดการเชื่อมต่ออัตโนมัติ
5. ตรวจสอบการเข้าสู่ระบบของผู้ใช้อย่างต่อเนื่อง
6. แนะนำให้แยกเครื่องส่วนตัวกับบริษัทออกจากกัน
7. ให้พนักงานทำการสำรองข้อมูลตามกฎ 3-2-1
8. ให้พนักงานสร้างพื้นฐานความปลอดภัยกับคอมพิวเตอร์เครื่องอื่นๆ ในบ้าน เช่น เครื่องที่ถูกใช้เรียนออนไลน์



กฎพื้นฐาน 3 ข้อ เพื่อความปลอดภัยบนโลกออนไลน์

1. ถ้าสิ่งนั้นไม่ใช่สิ่งที่เรากำลังมองหาอยู่ **อย่าติดตั้ง**
2. ถ้าเราติดตั้งโปรแกรมไหนก็ตามบนเครื่องแล้ว **ต้องอัปเดตเสมอ**
3. ถ้าหากเมื่อไรก็ตาม ไม่ต้องการโปรแกรมนั้นแล้ว ให้ **ลบทิ้งซะ**



เอกสารอ้างอิง

- หลักสูตรเสริมสร้างการรับรู้ที่แข็งแกร่งด้านความมั่นคงปลอดภัยทางไซเบอร์

Build a Strong Security Awareness Program

โดยคุณสุทธินันท์ แทนนินิล

ที่ปรึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์, เทรนดีไมโคร (ประเทศไทย)

