



มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย
Internet Foundation for the Development of Thailand

CYBER SECURITY

สำหรับเด็กและเยาวชน



มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย



น้อง ๆ เคยทำสิ่งเหล่านี้หรือไม่



- ใช้ Wi-Fi ฟรี
- กดลิงก์แปลก ๆ
- โหลดแอปใหม่
- ตั้งรหัสผ่านเหมือนกันทุกบัญชี



Cyber security คืออะไร

Cyber Security คือการปกป้องข้อมูล อุปกรณ์ และตัวเราเอง จากภัยบนโลกออนไลน์ ไม่ใช่แค่การป้องกันไวรัส

แต่รวมถึง

- ข้อมูลส่วนตัว
- บัญชีโซเชียล
- เงินในบัญชี
- ความปลอดภัยในชีวิตจริง





Wi-Fi สาธารณะ ใช้ฟรี ๆ ไม่ได้ได้ไง ???



Wi-Fi ฟรีตามร้านกาแฟ ห้างสรรพสินค้า
สนามบิน หรือสถานที่สาธารณะ
ช่วยให้ใช้อินเทอร์เน็ตได้สะดวก
แต่หากใช้งานโดยไม่ระมัดระวัง
อาจมีความเสี่ยงด้านความปลอดภัย
หลายรูปแบบ



อันตรายของ Wi-Fi สาธารณะ





คนร้ายอาจสร้างชื่อ Wi-Fi ปลอม คล้ายชื่อ Wi-Fi ฟรี แล้วดักรับข้อมูล

ถูกขโมยรหัสผ่าน
ขโมยข้อมูลบัญชีผู้ใช้
ขโมยเงินในบัญชี
ขโมยข้อมูลส่วนตัว



Layer 2: แผนภาพช่วยตัดสินใจ เชื่อมต่อ หรือ ตัดการเชื่อมต่อ?



มูลนิธิอินเทอร์เน็ตเพื่อร่วมพัฒนาไทย



มูลนิธิอินเทอร์เน็ตเพื่อร่วมพัฒนาไทย
Internet Foundation for the Development of Thailand



สิ่งที่ไม่ควรทำบน Wi-Fi ฟรี



- X ห้ามใช้คอมพิวเตอร์ที่ไม่ใช่
X ห้ามอยู่คนเดียว
มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย
- X ห้ามใช้คอมพิวเตอร์ที่ไม่ใช่
X ห้ามอยู่คนเดียว
มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย
- X ห้ามใช้คอมพิวเตอร์ที่ไม่ใช่
X ห้ามอยู่คนเดียว
มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย
- X ห้ามใช้คอมพิวเตอร์ที่ไม่ใช่
X ห้ามอยู่คนเดียว
มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย
- X ห้ามใช้คอมพิวเตอร์ที่ไม่ใช่
X ห้ามอยู่คนเดียว
มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย

ทำธุรกรรมธนาคาร
กรอกเลขบัตรเครดิต
กรอกรหัสผ่านสำคัญ
ดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
เปิดเผยข้อมูลส่วนตัว

มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย





วิธีใช้งาน Wi-Fi ฟรีให้ปลอดภัย



- ตรวจสอบชื่อ Wi-Fi ให้ดีก่อนเชื่อมต่อ
- ใช้เว็บไซต์ที่ขึ้นต้นด้วย HTTPS
- เปิดใช้รหัสผ่านหลายขั้นตอน MFA
- ปิดการแชร์ไฟล์
- ปิดการจดจำรหัสผ่านอัตโนมัติ
- อัปเดตระบบปฏิบัติการสม่ำเสมอ
- ใช้เครือข่ายมือถือ (4G/5G) เมื่อต้องทำธุรกรรมสำคัญ

มูลนิธิอินเทอร์เน็ตเพื่อการพัฒนาไทย



การกดลิงก์ และโหลดแอปฯ จากแหล่งที่ไม่รู้จัก เป็นอันตรายคล้ายการใช้ Wi-Fi ฟรี



อาจถูกดักจับข้อมูล

หรืออาจถูกลงโปรแกรมมิจาชีพที่แฝงมัลแวร์

โดยหลอกให้ผู้ใช้ติดตั้งผ่านลิงก์ SMS หรือ LINE ปลอม
เมื่อติดตั้งสำเร็จ มิจาชีพจะควบคุมหน้าจอมือถือระยะไกล

และทำทุกอย่างได้เหมือนโทรศัพท์เราอยู่ในมือ

ซึ่งรวมถึงการโอนเงินทั้งหมดออกจากบัญชี



ก่อนกดลิงก์ ให้ใช้หลัก “หยุด-คิด-ตรวจสอบ”




หยุด อย่ารีบกดทันที
คิด ใครส่งมา? ทำไมถึงส่งมา?
ตรวจสอบ ดู URL ให้ดีก่อน
หรือเข้าเว็บไซต์ทางการ
โหลดแอปฯ จากแหล่งที่น่าเชื่อถือเท่านั้น





ไวรัส วายร้าย








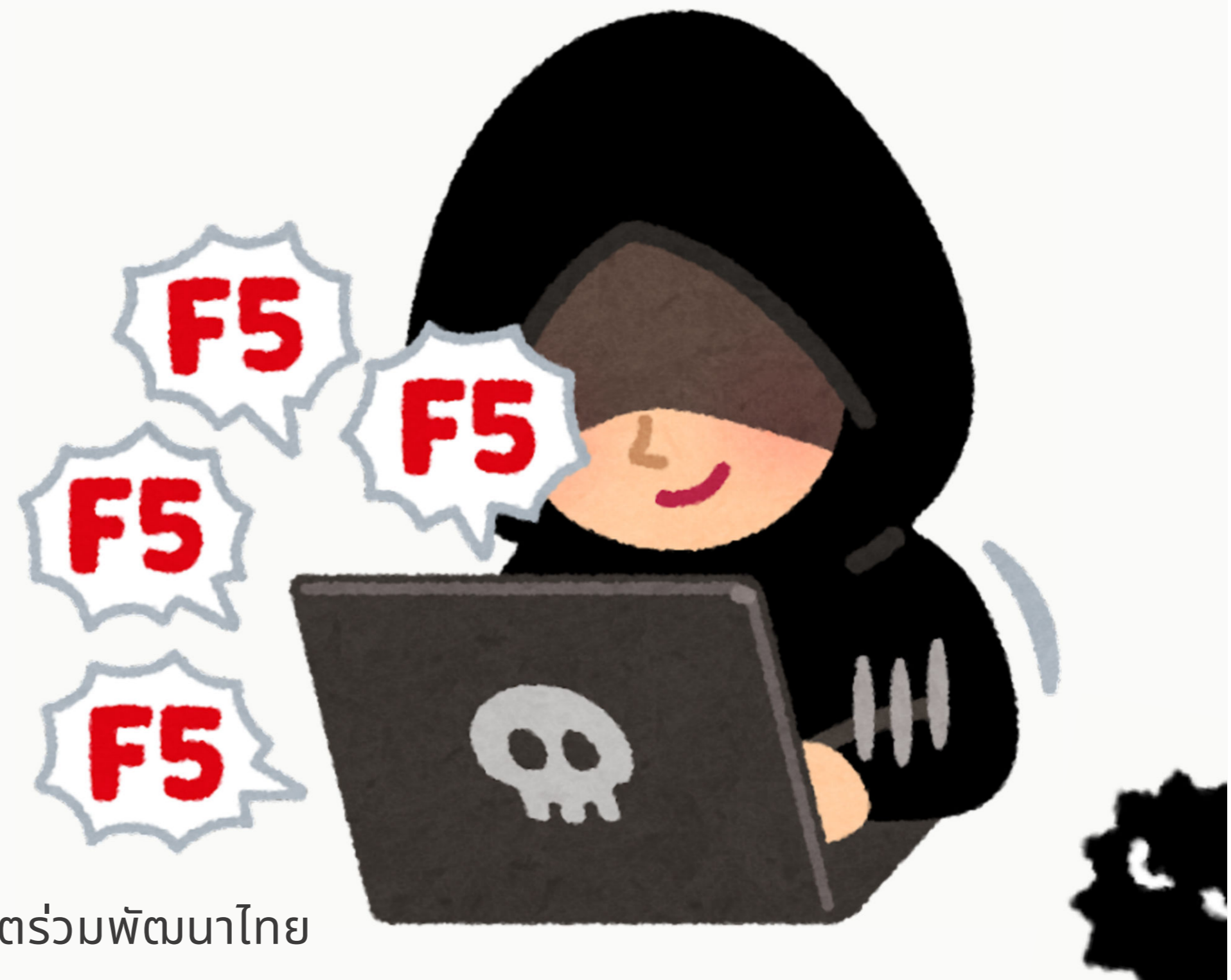
 **ไวรัสคอมพิวเตอร์**
ไม่ได้ทำให้คนป่วย
แต่ทำให้อุปกรณ์มีปัญหา
แพร่กระจายได้ทั่ว
ทั้งในคอมพิวเตอร์ แท็บเล็ต
และโทรศัพท์มือถือ





ไวรัส (Computer Virus) คือ โปรแกรมอันตราย ที่แอบเข้ามาในอุปกรณ์ เพื่อ...

-  ขโมยข้อมูล
-  ทำให้อุปกรณ์ทำงานช้า
-  แสดงโฆษณาที่กวนใจ
-  ยึดบัญชีโซเชียลมีเดีย
-  เรียกค่าไถ่ข้อมูล



ไวรัสเข้ามาได้อย่างไร?



ดาวน์โหลดไฟล์แปลก ๆ
กดลิงก์ที่ไม่น่าเชื่อถือ
โหลดเกมหรือโปรแกรมเถื่อน
เปิดไฟล์แนบจากคนแปลกหน้า





มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

5 วิธีป้องกันไวรัส



มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

ดาวน์โหลดแอปจาก App Store หรือ Google Play เท่านั้น

มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

ไม่กดลิงก์แปลก ๆ

มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

อัปเดตโทรศัพท์และแอปฯ สม่ำเสมอ

มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

ใช้โปรแกรมป้องกันไวรัส (ถ้ามี)

มีโปรแกรมป้องกันไวรัส (ถ้ามี)
สำรองข้อมูลสำคัญเป็นประจำ
มูลนิธิเพื่อพัฒนาไทย

สำรองข้อมูลสำคัญเป็นประจำ





สัญญาณว่าอุปกรณ์เราอาจติดไวรัส



มีแอปฯ ชักช้าลง
คอมพิวเตอร์หรือสมาร์ทโฟน
ทำงานผิดปกติ

เครื่องช้าผิดปกติ

มีแอปฯ ชักช้าลง
คอมพิวเตอร์หรือสมาร์ทโฟน
ทำงานผิดปกติ

มีโฆษณาเต็มตลอดเวลา

มีแอปฯ ชักช้าลง
คอมพิวเตอร์หรือสมาร์ทโฟน
ทำงานผิดปกติ

แบตเตอรี่หมดเร็วมาก

มีแอปฯ ชักช้าลง
คอมพิวเตอร์หรือสมาร์ทโฟน
ทำงานผิดปกติ

มีแอปฯ แปลก ๆ ติดตั้งเอง

มีแอปฯ ชักช้าลง
คอมพิวเตอร์หรือสมาร์ทโฟน
ทำงานผิดปกติ

เพื่อนบอกว่าได้รับข้อความแปลก ๆ จากบัญชีเรา





ตั้งรหัสผ่านเหมือนกันทุกบัญชี อันตรายอย่างไร ?



รหัสผ่าน = กุญแจ
ถ้าเรามีรถหลายคัน



เราจะใช้กุญแจเดียวกันไหม ?





รหัสผ่านที่แย่ที่สุดก็คือ...



123456

password

วันเดือนปีเกิด

ชื่อแฟน

เบอร์โทรศัพท์





การตั้งรหัสผ่าน และการเก็บรักษารหัสผ่าน



ยาวอย่างน้อย 8 ตัว



ผสมตัวอักษร ตัวเลข สัญลักษณ์



ไม่ซ้ำกันทุกบัญชี หมั่นเปลี่ยนอยู่เสมอ



ไม่จดไว้ในที่ ๆ เห็นได้ง่าย



ไม่บอกคนอื่น



รหัสผ่านต้องคาดเดายาก แต่เราต้องจำได้





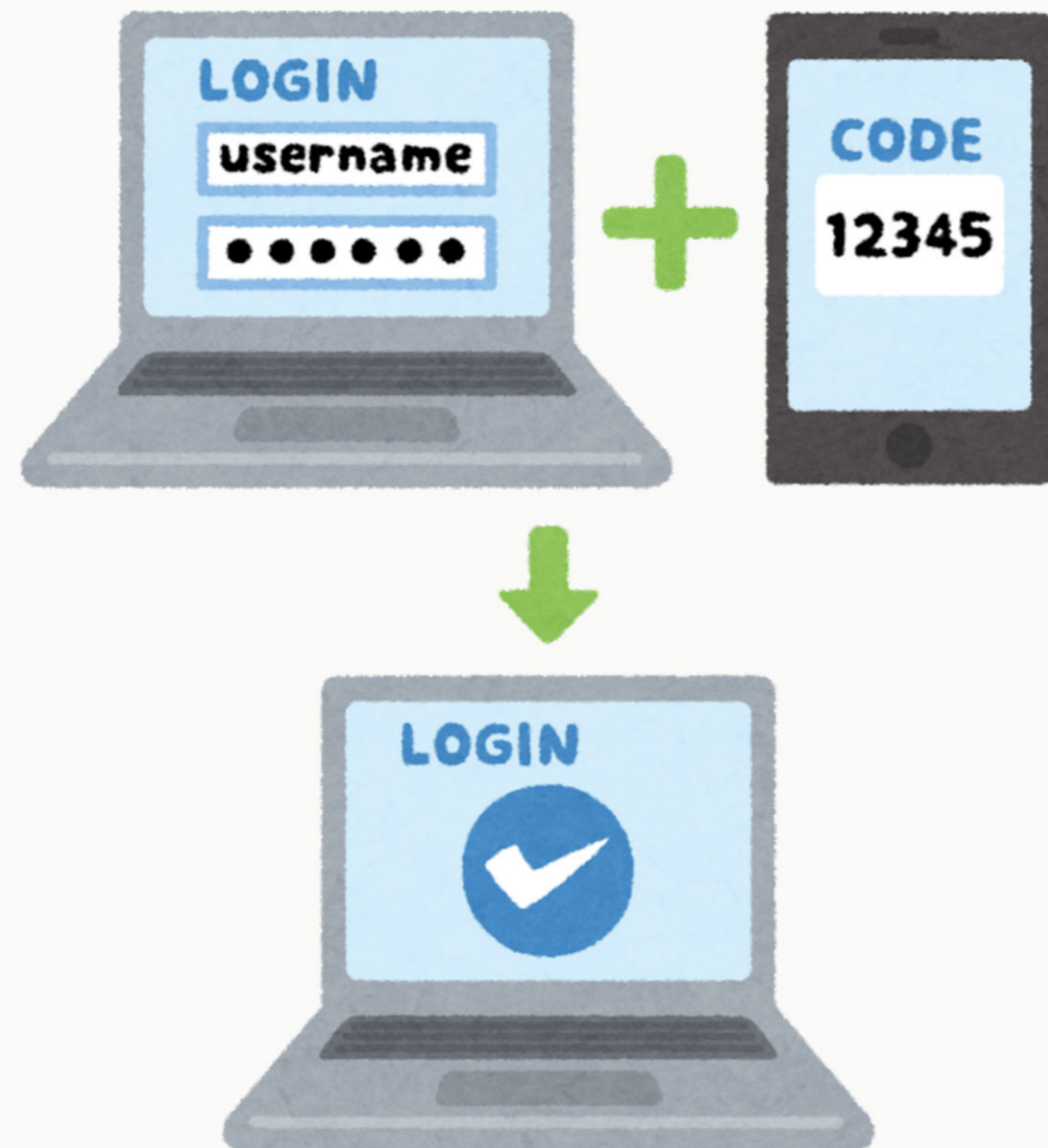
MFA ภัยหลากหลายชั้น ป้องกันแน่นหนา

MFA (การยืนยันตัวตนแบบหลายขั้นตอน)
คือ ระบบการยืนยันตัวตนที่มีขั้นตอนหลายขั้นตอน
โดยผู้ใช้งานต้องกรอกข้อมูลอย่างน้อย 2 รูปแบบที่แตกต่างกัน
ก่อนที่จะเข้าสู่ระบบ
ช่วยป้องกันการถูกขโมยบัญชีได้
แม้ว่าแฮกเกอร์จะทราบรหัสผ่านของเราก็ตาม





ตัวอย่างการยืนยันหลายชั้น



แม้ว่าจะกรอกรหัสผ่านแล้ว
แต่ยังคงต้องป้อนรหัสผ่านแบบใช้ครั้งเดียว
(OTP)

ที่จะส่งไปยังโทรศัพท์มือถือของเรา
เพื่อให้สามารถเข้าสู่ระบบได้





ตัวอย่างการยืนยันหลายชั้น



แม้ว่าจะกรอกรหัสผ่านแล้ว
แต่ยังคงต้องสแกนลายนิ้วมือ
เพื่อให้สามารถเข้าสู่ระบบได้





ถ้าโดนแฮกเกอร์โจมตี ต้องทำอะไร?



- ✓ เปลี่ยนรหัสผ่านทันที
- ✓ ออกจากระบบทุกอุปกรณ์
- ✓ เปิด MFA
- ✓ แจ้งผู้ปกครอง/ครู
- ✓ แจ้งแพลตฟอร์ม





ข้อมูลส่วนตัวที่ไม่ควรโพสต์

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

เลขบัตรประชาชน

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

ตารางเรียน

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

ที่อยู่

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

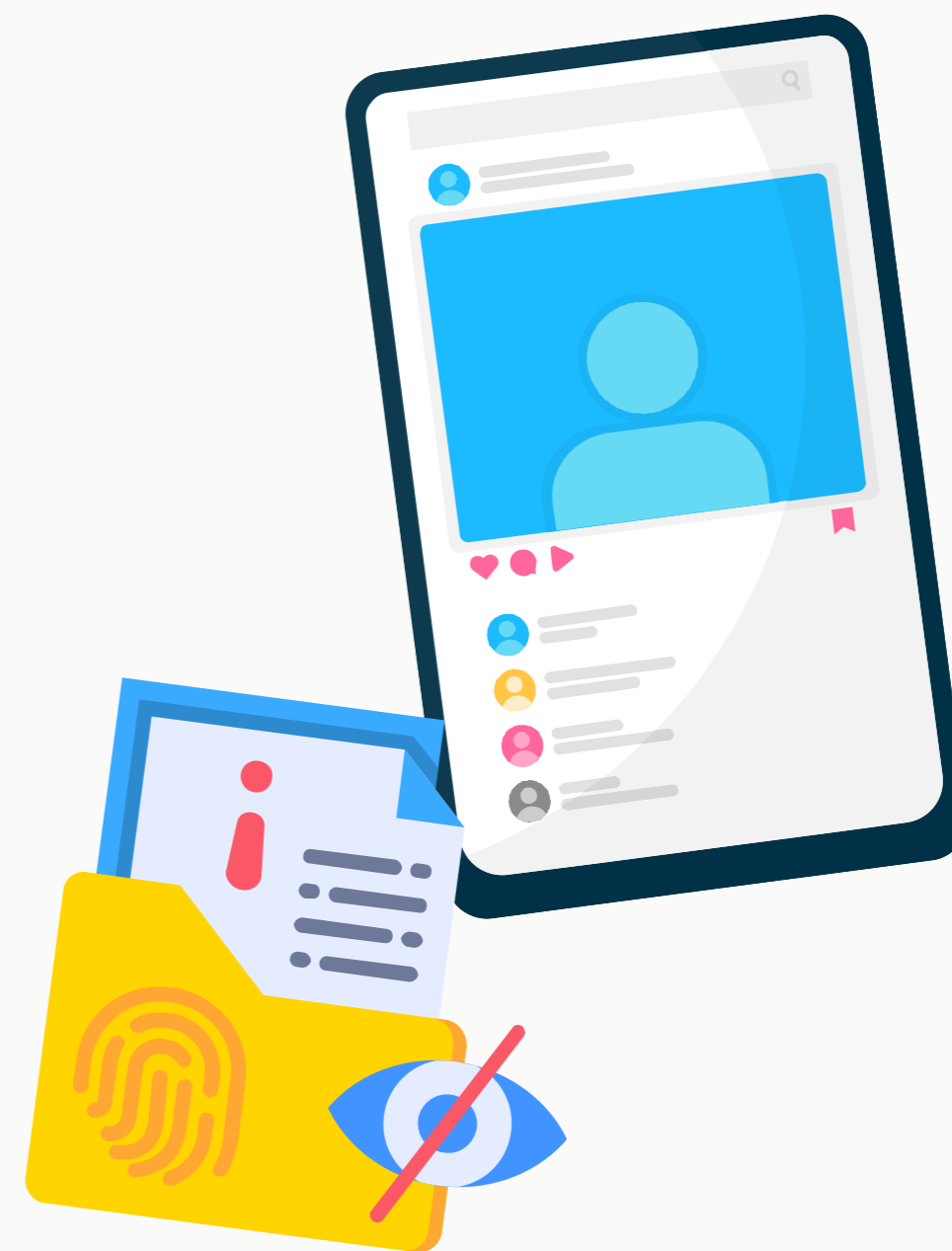
รูปบัตรนักเรียน

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

รูปตัวเครื่องบิน

✗ ส่งต่อเรื่องลับ
✗ รั่วไหลที่สำคัญ

รหัส QR ที่สำคัญ



ขั้นตอนปฏิบัติ:เมื่อข้อมูลส่วนบุคคลรั่วไหล





ความปลอดภัยในโซเชียลมีเดีย
ก่อนที่น้อง ๆ จะโพสต์ ควรพิจารณาสามข้อดังนี้:



1. ใครจะมีโอกาสเห็นโพสต์นี้
2. มันจะอยู่บนอินเทอร์เน็ตนานแค่ไหน?
3. หากครูหรือพ่อแม่เห็น จะเป็นเรื่องที่เหมาะสมไหม?





5 เช็ค เพื่อความปลอดภัยไซเบอร์



01  เช็ครหัสผ่าน - ยากพอหรือยัง?

02  เช็คการยืนยันตัวตน - เปิด MFA แล้วหรือยัง?

03  เช็คลิงก์ - แปกไหม? น่าเชื่อถือหรือไม่?

04  เช็คคนส่ง - ตัวจริงหรือบัญชีปลอม?

05  เช็คก่อนแชร์ - จริงหรือมั่ว?





ถามมา - ตอบไป



มูลนิธิอินเทอร์เน็ตเพื่อพัฒนาไทย

