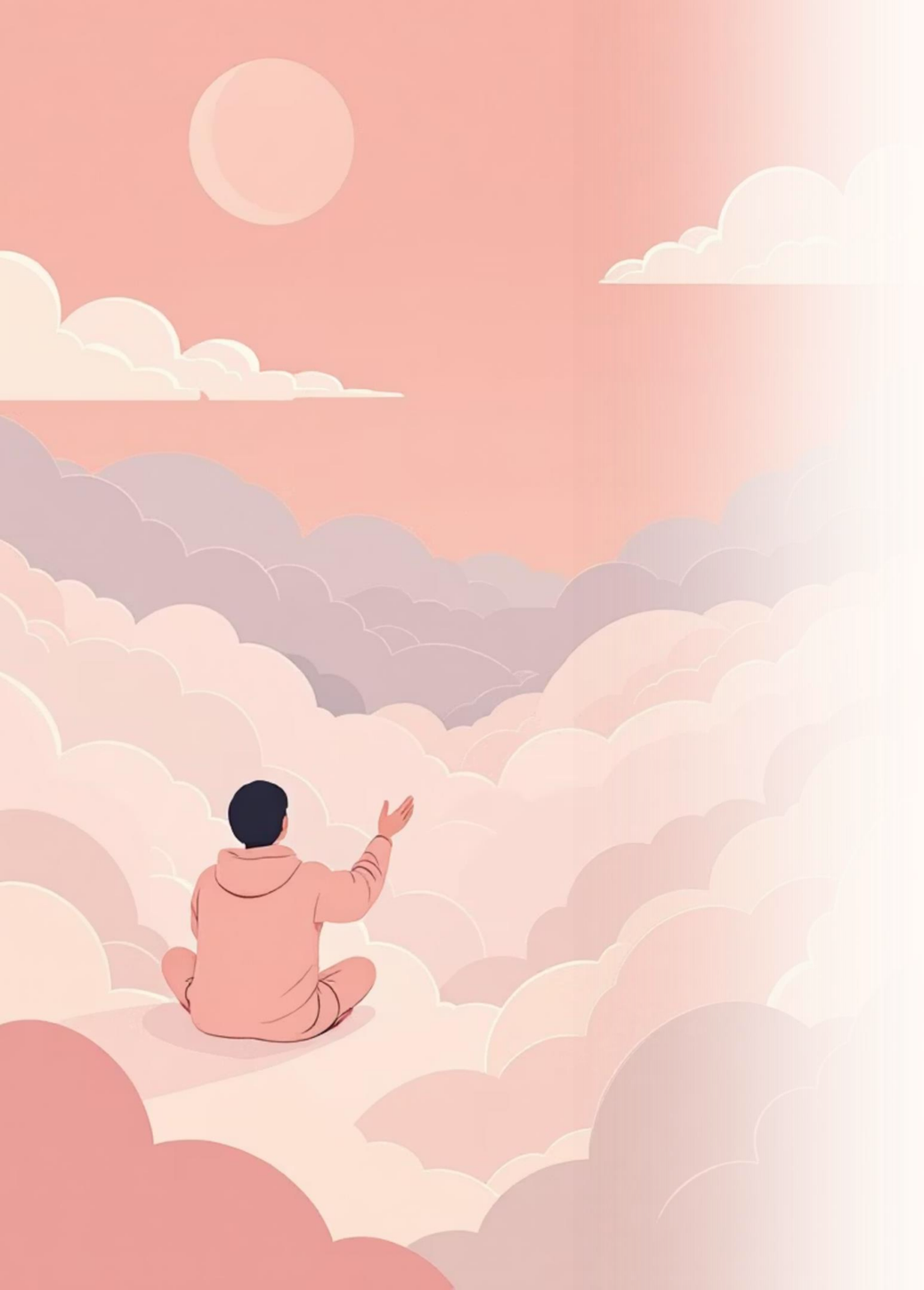
บทที่ 5

ความปลอดภัยเครือข่ายและ Wi-Fi สาธารณะ

Wi-Fi สาธารณะ: ความสะดวกที่แฝงภัยร้าย

Wi-Fi สาธารณะพบได้ทั่วไปในร้านกาแฟ สนามบิน ห้างสรรพสินค้า

แต่เครือข่ายเหล่านี้มักไม่มีการเข้ารหัสข้อมูล ทำให้ข้อมูลส่วนตัวเสี่ยงถูกดักจับ



กรณีศึกษา

ตัวอย่างภัยคุกคามจริง: Man-in-the-Middle (MitM)

1

การโจมตี MitM

แฮกเกอร์แทรกกลางระหว่างผู้ใช้กับเว็บไซต์เพื่อดักจับข้อมูล

2

ข้อมูลที่ถูกดักจับ

สามารถดักจับข้อมูลสำคัญ เช่น รหัสผ่าน หรือแม้แต่รายละเอียดธุรกรรมการเงิน

3

ความเปราะบาง

HideMyAss ทดสอบพบว่าเด็ก 7 ขวบก็สามารถแฮ็ก Wi-Fi สาธารณะสำเร็จได้ภายใน 11 นาที

เทคนิคแฮ็ก Wi-Fi สาธารณะที่ต้องระวัง

Fake Hotspot

การปลอมชื่อเครือข่าย (SSID) เพื่อหลอกให้ผู้ใช้เชื่อมต่อ

DNS Spoofing

เปลี่ยนเส้นทางเว็บไซต์ไปยังเว็บปลอมที่แฮกเกอร์สร้างขึ้น

Session Hijacking

ขโมยข้อมูลเซสชันเพื่อเข้าถึงบัญชีผู้ใช้โดยไม่ต้องรู้รหัสผ่าน

ผลกระทบจากการใช้ Wi-Fi สาธารณะไม่ปลอดภัย

ข้อมูลส่วนตัวรั่วไหล

เช่น ชื่อ-นามสกุล, เลขบัตรประชาชน, ที่อยู่

โดนขโมยรหัสผ่าน

รวมถึงข้อมูลทางการเงินจากแอปพลิเคชันหรือเว็บไซต์

ติดมัลแวร์และไวรัส

จากเครือข่ายที่ไม่มีมาตรการป้องกันที่เพียงพอ

วิธีป้องกันขั้นพื้นฐานเมื่อใช้ Wi-Fi สาธารณะ

ตรวจสอบเครือข่าย

ให้แน่ใจว่าเป็นชื่อเครือข่ายที่ถูกต้องและเป็นทางการ

ปิด Wi-Fi อัตโนมัติ

เพื่อป้องกันการเชื่อมต่อกับเครือข่ายที่ไม่ปลอดภัยโดยไม่ตั้งใจ

หลีกเลี่ยงธุรกรรมสำคัญ

ไม่ควรทำธุรกรรมทางการเงินหรือกรอกข้อมูลส่วนตัวที่สำคัญ

เครื่องมือช่วยเพิ่มความปลอดภัย

ใช้ VPN

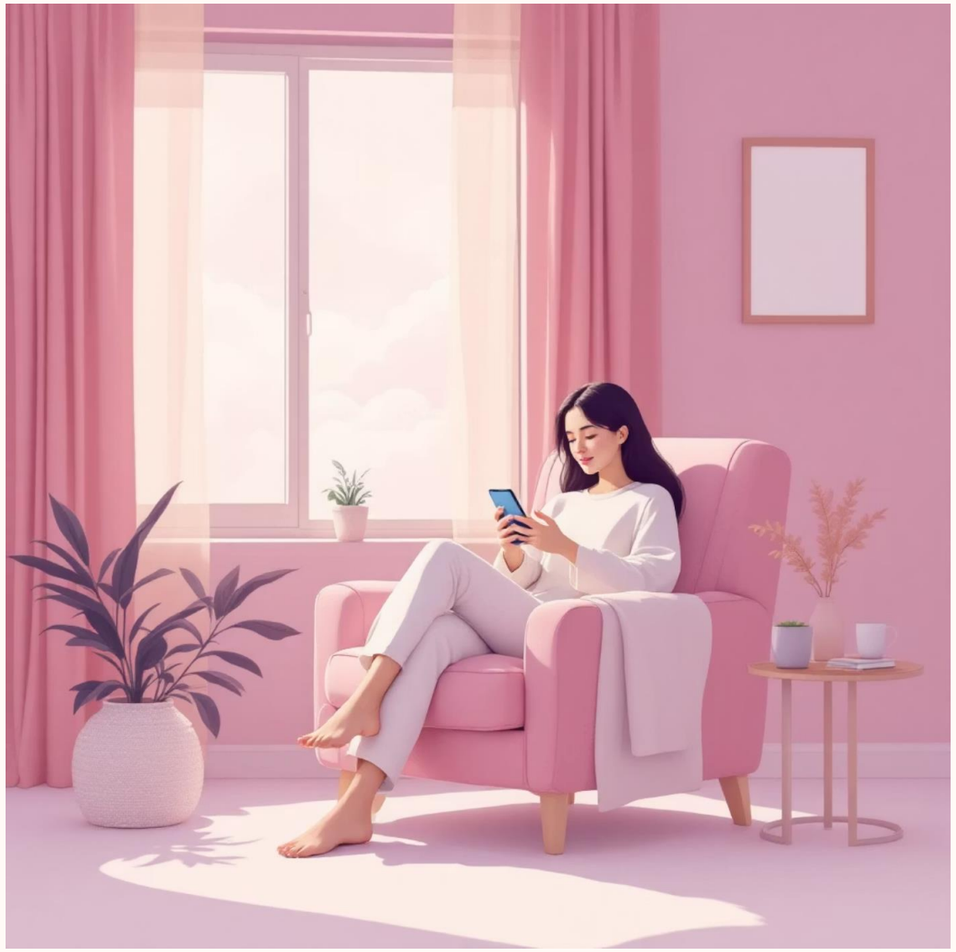
เพื่อเข้ารหัสข้อมูลทั้งหมด ช่วยปกป้องความเป็นส่วนตัวของคุณ

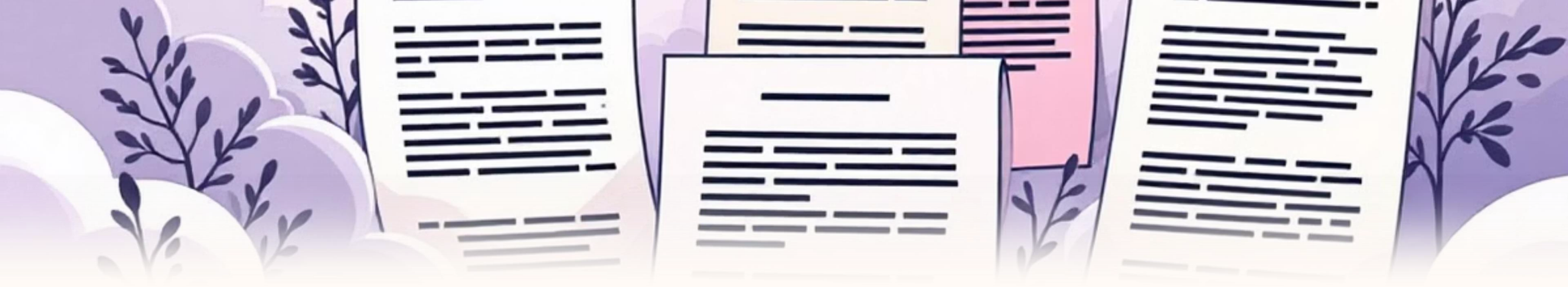
HTTPS และสัญลักษณ์กุญแจ

เชื่อมต่อเฉพาะเว็บไซต์ที่ขึ้นต้นด้วย HTTPS และมีสัญลักษณ์กุญแจล็อก

เปิด 2FA

เปิดใช้งานระบบยืนยันตัวตนสองชั้น (2FA) ในทุกบัญชีออนไลน์





นโยบายและมาตรฐานความปลอดภัยที่ควรรู้

มาตรฐาน ETDA & OWASP

ศึกษามาตรฐานความปลอดภัยเว็บไซต์จาก ETDA และ OWASP

อัปเดตซอฟต์แวร์

อัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ

รหัสผ่านที่แข็งแรง

ตั้งรหัสผ่านที่แข็งแรง ไม่ซ้ำกัน และเปลี่ยนเป็นประจำ

กรณีศึกษา: การโจมตี Wi-Fi สาธารณะที่เกิดขึ้นจริง

การโจมตีในร้านกาแฟ

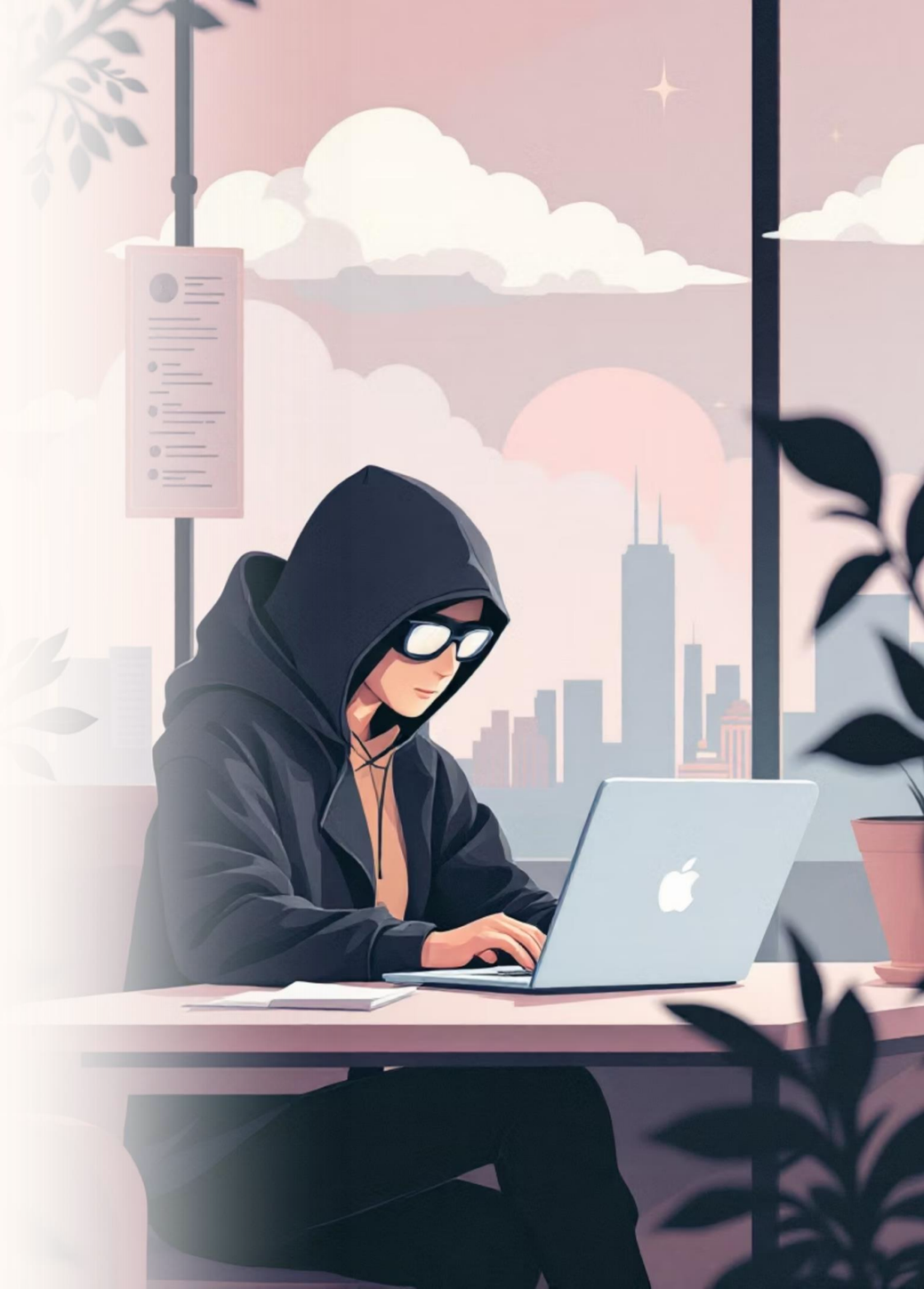
แฮกเกอร์วางอุปกรณ์ดักจับข้อมูลในร้านกาแฟชื่อดังหลายแห่ง

ผลกระทบต่อผู้ใช้

ผู้ใช้หลายรายถูกขโมยข้อมูลเข้าสู่ระบบธนาคารออนไลน์และบัญชีโซเชียลมีเดีย

บทเรียนสำคัญ

ความระมัดระวังและการใช้เครื่องมือป้องกันเป็นสิ่งจำเป็นอย่างยิ่ง



สรุปและคำแนะนำสุดท้าย

ใช้ด้วยความระมัดระวัง

Wi-Fi สาธารณะสะดวกแต่มีความเสี่ยงสูง

ใช้ VPN เสมอ

และตรวจสอบความปลอดภัยของเว็บไซต์ (HTTPS)

หลีกเลี่ยงการเปิดเผยข้อมูล

บนเครือข่ายสาธารณะที่ไม่น่าเชื่อถือ

ปกป้องตัวเอง

การรักษาความปลอดภัยออนไลน์ คือการปกป้องตัวเองในยุคดิจิทัล