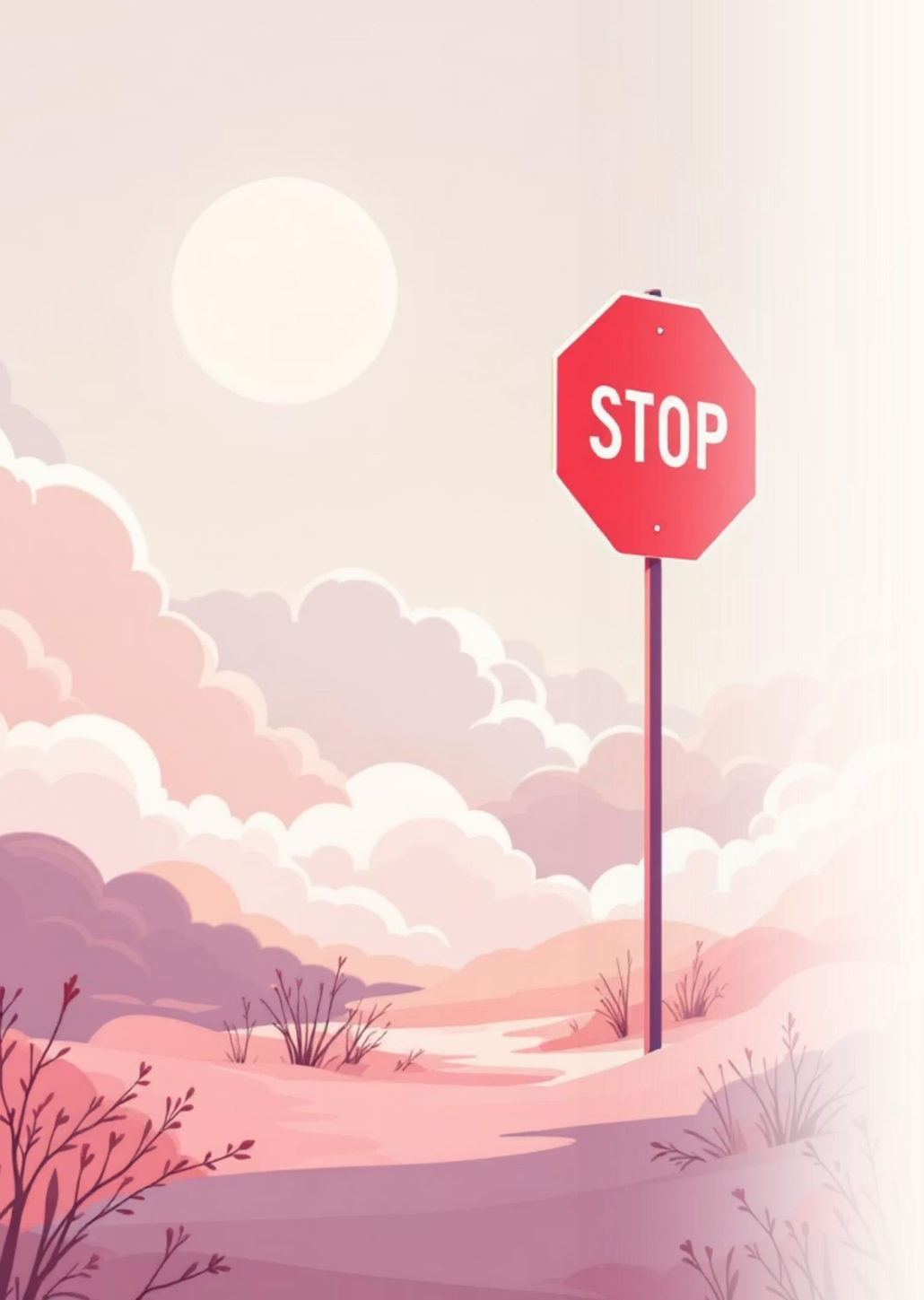
บทที่ 2: รหัสผ่านและการยืนยันตัวตน (Authentication & Password Security)

ทำไมรหัสผ่านถึงสำคัญ?

รหัสผ่านเปรียบเสมือนกุญแจดิจิทัลที่ช่วยปกป้องข้อมูลส่วนตัวและบัญชีออนไลน์ของคุณจากผู้ไม่หวังดี การมีรหัสผ่านที่อ่อนแอจึงเป็นเหมือนการเปิดประตูให้แฮกเกอร์เข้าถึงข้อมูลสำคัญได้โดยง่าย

- รหัสผ่านคือกุญแจดิจิทัลที่ปกป้องข้อมูลส่วนตัวและบัญชีออนไลน์ของคุณ
- รหัสผ่านที่อ่อนแอ = ช่องโหว่ให้แฮกเกอร์เข้าถึงข้อมูลสำคัญได้ง่าย
- กรณีตัวอย่าง: รหัสผ่านง่ายๆ เช่น "123456" ถูกใช้โดยผู้ใช้จำนวนมากและถูกแฮกบ่อยครั้ง



รหัสผ่านที่ควรหลีกเลี่ยง

สั้นเกินไป

เช่น น้อยกว่า 8 ตัวอักษร

ง่ายต่อการคาดเดา

ใช้คำง่ายๆ หรือข้อมูลส่วนตัว เช่น ชื่อ วันเกิด เบอร์โทรศัพท์

ใช้ซ้ำ

ใช้รหัสผ่านซ้ำในหลายบัญชี

ตัวอย่าง

"password", "qwerty", "abc123" เป็นรหัสผ่านยอดนิยมที่แฮกเกอร์โจมตีง่าย

วิธีตั้งรหัสผ่านที่ปลอดภัย

ความยาว

อย่างน้อย 12-16 ตัวอักษร

ผสมผสาน

ตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์พิเศษ เช่น !@#$%^&*

วลี

ใช้วลีหรือข้อความที่ไม่มีความหมายตรง เช่น “I_have2Dogs&3Cats!”

เครื่องมือช่วย

ใช้เครื่องมือจัดการรหัสผ่าน (Password Manager) เช่น LastPass, 1Password

การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication, 2FA)

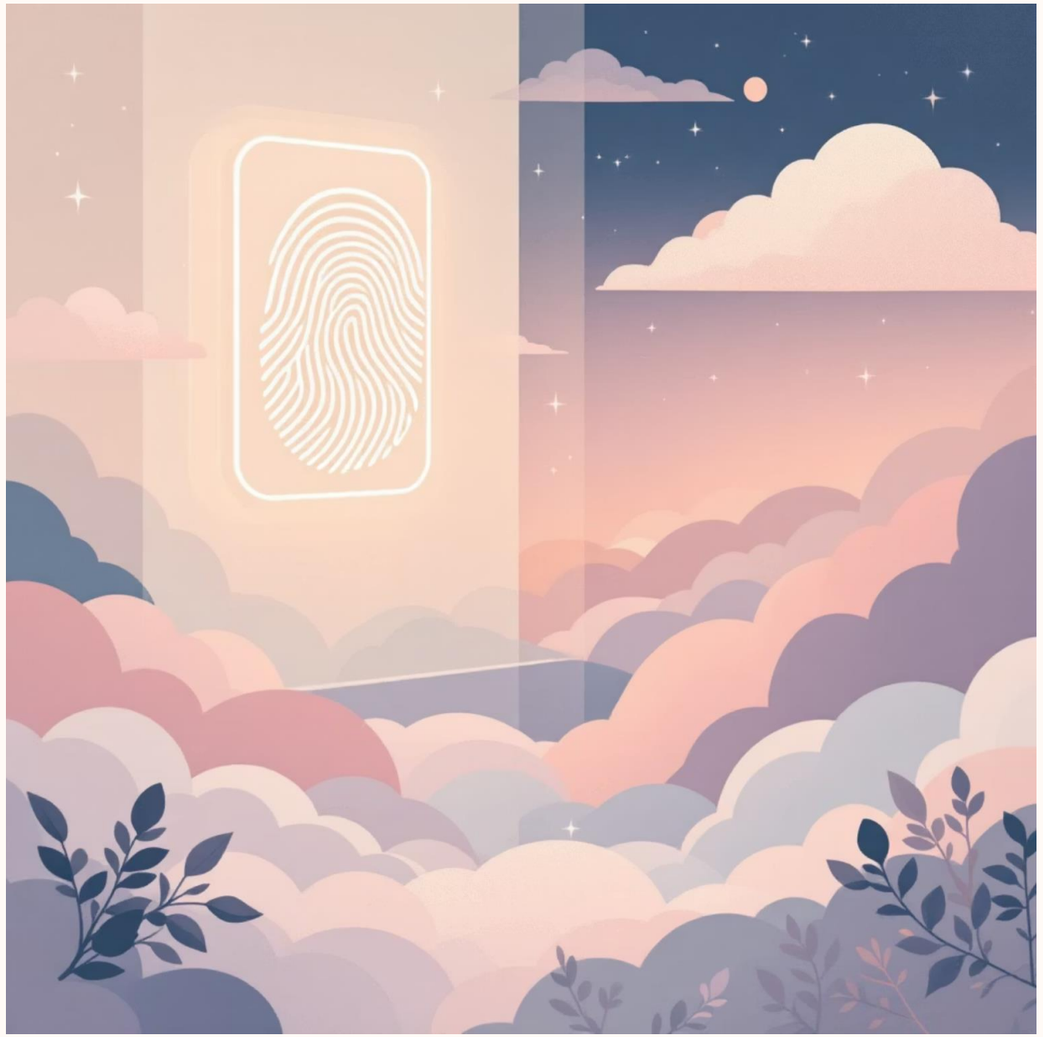
2FA คือการเพิ่มชั้นความปลอดภัยอีกหนึ่งชั้นนอกเหนือจากรหัสผ่าน โดยผู้ใช้จะต้องกรอกรหัส OTP (One-Time Password) ที่ส่งไปยังมือถือหรือแอปพลิเคชันยืนยันตัวตน เช่น Google Authenticator

- เพิ่มชั้นความปลอดภัยนอกเหนือจากรหัสผ่าน
- ต้องกรอกรหัส OTP ที่ส่งไปยังมือถือหรือแอปยืนยันตัวตน
- ป้องกันการเข้าถึงบัญชีแม้รหัสผ่านถูกขโมย
- ตัวอย่าง: Google, Facebook, ธนาคารหลายแห่งเปิดใช้ 2FA เป็นมาตรฐาน

พาสคีย์ (Passkeys): เทคโนโลยีใหม่แทนรหัสผ่าน

พาสคีย์เป็นการใช้งานการล็อกหน้าจอของอุปกรณ์ เช่น การสแกนลายนิ้วมือ หรือการสแกนใบหน้า แทนการพิมพ์รหัสผ่าน ทำให้เกิดความปลอดภัยที่สูงขึ้นและใช้งานง่าย

- ใช้การล็อกหน้าจอของอุปกรณ์ เช่น สแกนลายนิ้วมือ หรือสแกนใบหน้าแทนการพิมพ์รหัสผ่าน
- ปลอดภัยสูง ป้องกันฟิชชิงและการโจมตีระยะไกล
- ใช้งานง่าย ไม่ต้องจำรหัสผ่าน
- รองรับทุกแพลตฟอร์มและอุปกรณ์ที่ซิงค์บัญชี Google



แนวทางปฏิบัติที่ดีในการจัดการรหัสผ่าน

01

เปลี่ยนรหัสผ่าน

ทุก 3-6 เดือน โดยเฉพาะบัญชีสำคัญ

02

ไม่จดบันทึก

ไม่จดรหัสผ่านไว้ในที่สาธารณะหรือแชร์กับผู้อื่น

03

ใช้รหัสผ่านแตกต่างกัน

ในแต่ละบัญชี

04

ตั้งค่าล็อกบัญชี

เมื่อมีการล็อกอินผิดพลาดหลายครั้ง

ตัวอย่างเหตุการณ์และผลกระทบจากรหัสผ่านอ่อนแอ

หลายครั้งที่ข้อมูลรั่วไหลจากบริษัทขนาดใหญ่เป็นผลมาจากรหัสผ่านที่อ่อนแอหรือการใช้รหัสผ่านซ้ำซ้อน ทำให้ผู้ใช้งานหลายล้านคนต้องเผชิญกับการถูกแฮกข้อมูลส่วนตัว

- กรณีข้อมูลรั่วไหลจากบริษัทใหญ่หลายแห่งเพราะรหัสผ่านง่ายหรือซ้ำซ้อน
- ผู้ใช้หลายล้านคนถูกแฮกบัญชีและข้อมูลส่วนตัวถูกขโมย
- การเปิดใช้ 2FA ช่วยลดความเสี่ยงได้มากกว่า 99%

การยืนยันตัวตนระดับสูง (Identity Assurance Level: IAL)

มาตรฐานสูง

การพิสูจน์และยืนยันตัวตนตามมาตรฐาน เช่น การใช้บัตรประชาชนแบบชิป NFC

ข้อมูลชีวมิติ

ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติ (Biometric) เช่น Face Verification

ความน่าเชื่อถือ

เหมาะกับบริการที่ต้องการความน่าเชื่อถือสูง เช่น ธนาคาร รัฐบาล

สรุปและคำแนะนำ

- รหัสผ่านที่ปลอดภัยและการยืนยันตัวตนหลายชั้นคือเกราะป้องกันสำคัญ
- ใช้รหัสผ่านยาว ซับซ้อน และไม่ซ้ำกันในแต่ละบัญชี
- เปิดใช้ 2FA หรือพาสคีย์เพื่อเพิ่มความปลอดภัย
- จัดการรหัสผ่านอย่างมีวินัย เปลี่ยนรหัสผ่านเป็นประจำ และใช้เครื่องมือช่วยจัดการ

> “ความปลอดภัยของคุณเริ่มต้นที่รหัสผ่านที่แข็งแกร่งและการยืนยันตัวตนที่มั่นคง”