# บทที่ 4 : ความปลอดภัยยุคดิจิทัล (DIGITAL SAFETY)

## รอยเท้าดิจิทัล — นิยาม/ความหมาย และเหตุผลที่ต้องตระหนัก **(หน้าที่ 324–326[5–7])**

• “รอยเท้าดิจิทัล” คือข้อมูลของผู้ใช้อินเทอร์เน็ต/โลกไซเบอร์ที่ถูกสร้างหรือทิ้งไว้ระหว่างใช้งานบริการต่างๆ (เช่น Facebook, IG, เว็บไซต์, อีเมล, แอปที่ยืนยันตัวตนและกรอกข้อมูลเพื่อเข้าสู่ระบบ) ทั้งจากการอัปโหลดข้อมูลส่วนตัว ไฟล์ รูปภาพ การใช้สมาร์ตโฟน/แท็บเล็ต/คอมพิวเตอร์ ระบบบนอินเทอร์เน็ตจะบันทึกข้อมูลผู้ใช้และส่วนบุคคล เช่น ที่อยู่ เบอร์โทร วันเดือนปีเกิด ตำแหน่งงาน ผลงาน การศึกษา ประวัติ ทำให้ผู้อื่นอนุมานสิ่งที่ชอบ สนใจ หรืออยากทำได้

• สถาบันสื่อเด็กและเยาวชน (2561) แนะให้ตระหนักเรื่องข้อมูลส่วนตัวเพื่อความปลอดภัย ด้วยเหตุผลสำคัญ ได้แก่ ปกป้องชื่อเสียง, สร้างขอบเขตการเข้าถึง, ป้องกันการสูญเสียทรัพย์สิน, และรักษาอิสรภาพ/ความเป็นส่วนตัว

## รอยเท้าดิจิทัล — ประเภท **(หน้าที่ 326–329[7–10])**

### 1. รอยเท้าที่เกิดโดยเจตนา (Active Digital Footprint)

• ตัวอย่าง: ใช้อีเมล, โพสต์/คอมเมนต์บนโซเชียล, พูดคุยบนเว็บบอร์ด

### 2. รอยเท้าที่ไม่ได้ตั้งใจฝากไว้ (Passive Digital Footprint)

• ตัวอย่าง: หมายเลข IP/ประวัติการค้นหา (จากเสิร์ชเอนจิน), ข้อมูลพิกัดภูมิศาสตร์ (Geolocation/GPS), สถิติการเข้าชมเว็บไซต์ (Hits)

## รอยเท้าดิจิทัล — ความสำคัญและการประยุกต์ใช้ **(หน้าที่ 329–330[10–11])**

• ภาคธุรกิจ: ใช้วิเคราะห์พฤติกรรม/ความสนใจเพื่อออกแบบบริการ/โฆษณา

• ภาคการศึกษา: ใช้ติดตามเส้นทางการเรียนรู้/หลักฐานกิจกรรมและผลงานผู้เรียน

## รอยเท้าดิจิทัล — แนวทางคุ้มครองความเป็นส่วนตัว **(หน้าที่ 330–334[11–15])**

• เตือนตนให้ปกป้องชื่อเสียง—ตระหนักว่าโพสต์/แชร์มีทั้งผลบวกและลบ

• กำหนดขอบเขตการเข้าถึง—จำกัดข้อมูลส่วนตัวที่จะเปิดเผย (เช่น สุขภาพ ที่อยู่อาศัย สถานที่ทำงาน) ลดความเสี่ยงบัญชีถูกสวมรอย

• ป้องกันการสูญเสียทรัพย์สิน—หลีกเลี่ยงโพสต์โชว์ของมีค่า (บ้าน รถ เงิน ทอง โฉนด) เพราะอาจนำไปสู่การหลอกลวง/อาชญากรรม

• รักษาอิสรภาพ/ความเป็นส่วนตัว—ไม่แชร์ตำแหน่งที่ตั้ง, ลดการถูกป้อนโฆษณาซ้ำจนเกิดพฤติกรรมซื้อเกินตัว

• ระวังไม่โพสต์ข้อมูลส่วนตัวโดยไม่จำเป็น, หลีกเลี่ยงเว็บไซต์ไม่น่าเชื่อถือ, ระวังลิงก์/ไฟล์ที่เป็นไวรัส, ระมัดระวังการให้ข้อมูลกับใครในโลกออนไลน์

• วิธีเบื้องต้นให้รอยเท้าปลอดภัยขึ้น: คิดก่อนโพสต์/แชร์, ตั้งค่าความเป็นส่วนตัว (Private), ค้นหาชื่อตนเองใน Google เพื่อตรวจร่องรอย

• วิธีลดการทิ้งข้อมูลสำคัญ: ยกเลิก/ปิดบัญชีที่ไม่ใช้, ลบข้อมูลในเว็บที่รวบรวมข้อมูล, ใช้ Stealth/Incognito/Tor, ปิดบัญชีอีเมลเก่า, ตรวจค่าความเป็นส่วนตัวของแอ็กเคานต์, ใช้ส่วนเสริม/ปลั๊กอินเพื่อความเป็นส่วนตัว, ใช้สิทธิ “ขอลบจากผลค้นหา”, ใช้ข้อมูลสมมติในแบบฟอร์ม, หลีกเลี่ยงแบบสอบถามไม่น่าเชื่อถือ

## การเก็บข้อมูลส่วนตัวโดยผู้ให้บริการ (Data Controller) **(หน้าที่ 334–336[15–17])**

• หน้าที่ของผู้ควบคุมข้อมูล: แจ้งวัตถุประสงค์การเก็บ (ชัดเจนก่อนเก็บ), ให้เจ้าของข้อมูลมีอิสระในการยินยอม, เก็บเท่าที่จำเป็นและลบทันตามกำหนด, แจ้งช่องทางติดต่อผู้ดูแล, โดยหลักควรเก็บจากเจ้าของข้อมูลโดยตรง—หากต้องใช้จากแหล่งอื่น ต้องรีบขอยินยอม (ภายใน 30 วัน)

• แนวปฏิบัติระดับองค์กร (ผสค.ข้อมูลส่วนบุคคลร่วมทุกฝ่าย: IT, PR, Marketing, Customer Service, Compliance, Sales, กฎหมาย, บัญชี) 6 ขั้นตอน: 1) จัดทำนโยบาย/มาตรฐานความปลอดภัยข้อมูลร่วมกัน, 2) ให้แต่ละฝ่ายระบุชนิดข้อมูล/ระยะเวลาจำเป็น/แนวทางลบทิ้ง, 3) จัดเก็บตามกำหนดและเป็นระเบียบให้ตรวจสอบย้อนกลับได้, 4) ปฏิบัติตามนโยบาย (อาจรวมกับ Privacy Policy) และแจ้ง/ขอยินยอมอย่างชัดเจน, 5) จ้าง DPO ที่เชี่ยวชาญ PDPA/GDPR เป็นที่ปรึกษา/ประสานงานเหตุละเมิด, 6) สร้างความรู้ความเข้าใจให้บุคลากร ลดความเสี่ยงการละเมิด

## การแบ่งปันเนื้อหาในโลกออนไลน์: ควร/ไม่ควร และการตั้งค่าความเป็นส่วนตัว **(หน้าที่ 337–342[18–23])**

• ประเภทสื่อสังคมหลัก: Weblogs, Social Networking, Micro Blogging/Sharing, Online Video, Photo Sharing, Wikis, Virtual Worlds, Crowd Sourcing, Podcast, Discuss/Review/Opinion

• ตัวอย่าง “ไม่ควรแชร์”: ข้อมูลส่วนตัว, ภาพบ้าน/ส่วนหนึ่งของบ้าน, ตั๋วเครื่องบิน, หนังสือเดินทาง, เช็กอินสถานที่, วิจารณ์ที่ทำงาน, ทัศนคติลบ (การเมือง/ศาสนา), ข่าวปลอม

• ภาพรวมการตั้งค่าความเป็นส่วนตัวบนสังคมออนไลน์: Facebook, Twitter, Instagram (ดูรายละเอียดหัวข้อถัดไป)

## การตั้งค่าความเป็นส่วนตัว — Facebook **(หน้าที่ 341–363[22–44])**

### 1. ตั้งค่าความเป็นส่วนตัวของโพสต์ (Posts)

• เลือกกลุ่มผู้เห็น: สาธารณะ/เพื่อน/ยกเว้นบางคน/เฉพาะบางคน/เฉพาะฉัน (ตั้งค่าผ่านตัวเลือกความเป็นส่วนตัวก่อนโพสต์)

### 2. การเชื่อมต่อกับแอป (Apps)

• ตรวจรายชื่อแอป/เว็บไซต์ที่เชื่อมต่อและ “ลบออก” ได้ หากไม่ใช้งานแล้ว

### 3. การแสดงผลโปรไฟล์ (Profile)

• กำหนดว่าจะแสดงข้อมูล “เกี่ยวกับ” (อีเมล วันเกิด บ้านเกิด สถานะความสัมพันธ์ ฯลฯ) หรือไม่

### 4. ความเป็นส่วนตัวของบัญชี (ค้นหา/การมองเห็น)

• จำกัดการค้นหาบัญชีโดยบุคคลทั่วไป/เสิร์ชเอนจิน

### 5. การอนุญาตโพสต์บน Timeline และ Tagging

• ควบคุมว่าใครโพสต์ได้ ใครเห็นสิ่งที่คนอื่นโพสต์ และตรวจสอบการแท็กก่อนขึ้น Timeline

### 6. การบล็อก (Blocking)

• รายชื่อจำกัด (Restricted), บล็อกผู้ใช้/ข้อความ/คำเชิญแอป/คำเชิญกิจกรรม/แอป/เพจ ได้ละเอียด

### 7. การเชื่อมต่อ Apps (ซ้ำในส่วน “แอปและเว็บไซต์”)

• เปิด/ปิดการเชื่อมต่อ “Log in with Facebook” ได้จากการตั้งค่า > แอปและเว็บไซต์

### 8. ผู้ติดตาม (Followers)

• ตั้งค่า “โพสต์สาธารณะ” กำหนดใครติดตาม/แสดงความเห็นบนโพสต์สาธารณะได้

### 9. การตั้งค่าโฆษณา (Ads)

• จัดการการรับโฆษณาตามความสนใจ/ข้อมูลส่วนตัวในระบบโฆษณา Facebook

## การตั้งค่าความเป็นส่วนตัว — Twitter **(หน้าที่ 364–367[45–48])**

• เส้นทาง: การตั้งค่าและความเป็นส่วนตัว > ความเป็นส่วนตัวและความปลอดภัย

• “ป้องกันทวีตของคุณ” เพื่อให้เห็นเฉพาะผู้ติดตามที่อนุญาต และสามารถสลับกลับ “สาธารณะ” ได้

## การตั้งค่าความเป็นส่วนตัว — Instagram **(หน้าที่ 368–369[49–50])**

• ยกเลิกการเข้าถึง (Revoke access) แอปที่เชื่อมต่อจากหน้าเว็บ “Authorized Applications” เพื่อรีเซ็ตการเชื่อมต่อที่ไม่ต้องการ

## การตั้งค่าความเป็นส่วนตัว — บริการเว็บไซต์/เบราว์เซอร์ **(หน้าที่ 370–374[51–55])**

• Chrome: ใช้ส่วนขยายเน้นความเป็นส่วนตัว (เช่น Cookie AutoDelete, uBlock Origin, Privacy Badger, HTTPS Everywhere) เพื่อสกัดกั้นตัวติดตาม (Tracker)

• Android: Chrome ไม่รองรับส่วนเสริม—พิจารณาใช้แอปที่เน้นความเป็นส่วนตัว (เช่น DuckDuckGo)

• ตั้งค่าบล็อกคุกกี้บุคคลที่สาม: การตั้งค่า > ข้อมูลส่วนบุคคลและความปลอดภัย > คุกกี้และข้อมูลอื่นของไซต์ > บล็อกคุกกี้บุคคลที่สาม (ลดการติดตามข้ามเว็บไซต์/โฆษณาตามสนใจ)

## การกลั่นแกล้งบนโลกออนไลน์ (Cyberbullying) — นิยาม/ตัวอย่าง/ผลกระทบ/การรับมือ **(หน้าที่ 375–388[56–69])**

### 1. ความหมาย

• การกระทำที่ตั้งใจทำให้ผู้อื่นทุกข์ เจ็บปวด เพื่ออำนาจเหนือ เกิดต่อเนื่องยาวนาน (ทั้งออนไลน์และออฟไลน์)

### 2. ตัวอย่างรูปแบบในโลกออนไลน์

• โจมตี/ขู่ทำร้าย/ใช้ถ้อยคำหยาบคาย, คุกคามทางเพศ, แอบอ้างตัวตน, แบล็กเมล์, หลอกลวง, ตั้งกลุ่มเพื่อรุมโจมตี

### 3. ผลกระทบ

• เดือดเนื้อร้อนใจ เบื่อชีวิต ไม่อยากไปโรงเรียน/พบใคร เครียดหนัก กินไม่ได้ นอนไม่หลับ จนถึงคิดทำร้ายตนเอง; ฝ่ายที่รังแกอาจรู้สึกผิดภายหลัง

### 4. แนวทางรับมือ (ผู้ถูกกระทำ)

• อย่าตอบสนอง/อย่าตอบโต้ (ไม่ปะทุความขัดแย้ง)

• เก็บหลักฐานให้มากที่สุด (ใช้กฎหมายคุ้มครองสิทธิ/ร้องเรียนได้)

• บล็อกผู้กระทำ (ตัดช่องทางรบกวน)

• ขอความช่วยเหลือ: บอกผู้ปกครอง/ครู/ผู้มีอำนาจ; ผู้ใหญ่สามารถลงบันทึกประจำวันกับตำรวจเพื่อให้ผู้กระทำเกรงกฎหมาย

• ใช้เครื่องมือรายงานของแพลตฟอร์มเพื่อระงับ/ถอดโพสต์ที่ไม่เหมาะสม

• ไม่ทำร้าย/กลั่นแกล้งใครกลับ (ไม่เป็นชนวนให้วงจรยืดเยื้อ)

### 4.1 แนวทางป้องกันในเด็ก

• ไม่ไว้ใจคนแปลกหน้าในออนไลน์

• ผู้ปกครองสอดส่องว่าเด็กคุยอะไร ที่ไหน กับใคร

• สอนเก็บข้อมูลส่วนตัว ไม่นัดเจอเพื่อนออนไลน์ส่วนตัว, แนะนำการตั้งค่าความปลอดภัยในโซเชียล

• ตกลงกติกาก่อนให้ใช้อุปกรณ์/โซเชียล เพื่อให้ตรวจสอบการใช้งานได้

• สร้างความสัมพันธ์ที่ไว้วางใจ ให้ลูกกล้าบอกทุกเรื่อง

### 4.2 แนวทางป้องกันในคนทั่วไป

• ไม่สื่อสารเนื้อหาสร้างความเกลียดชัง

• ไม่เปิดเผยข้อมูลส่วนตัวโดยไม่จำเป็น

• ตักเตือนอย่างสุภาพเมื่อเห็นการกลั่นแกล้ง และอย่าร่วมขยายวง (ไม่ดู/ไม่แชร์/ไม่คอมเมนต์)

### 5. การช่วยเหลือผู้ถูกกลั่นแกล้ง

• ความต่างระหว่าง “ผู้ยืนดูเฉยๆ (Passive Bystander)” กับ “ผู้ลุกขึ้นช่วย (Upstander)”

• วิธีช่วยเหลือที่เหมาะสม — บทบาทของ: พ่อแม่ (รับฟังด้วยเหตุผล, ช่วยบล็อก/ลบภาพไม่เหมาะสม, ประสานครู/เจ้าหน้าที่, สอนภัยไซเบอร์และการตั้งค่าความปลอดภัย), ครู (ไม่เพิกเฉย, เปิดพื้นที่คุยร่วม, สอนทักษะรู้เท่าทันสื่อ, ชวนฉุกคิดเรื่องข่าวลวง/การส่งต่อ), ผู้ให้บริการ (ประกาศชัดเจน/มีมาตรการ, ช่องทางลบเนื้อหาเร่งด่วน, จัดเจ้าหน้าที่ให้คำปรึกษาและดำเนินการกับผู้กระทำ)

## การตั้งค่าการเข้าถึงบนบัญชีออนไลน์และอุปกรณ์ดิจิทัล **(หน้าที่ 392–401[73–82])**

### 1. การตั้งรหัสผ่านที่ปลอดภัย

• ความยาวอย่างน้อย 12–14 ตัวอักษร; หลีกเลี่ยงคำพจนานุกรม/รูปแบบยอดนิยม; อย่าแปลงตัวอักษรเป็นตัวเลขที่เดาง่าย

• วิธีตั้งรหัสผ่านที่ยากแต่จำได้: ใช้ตัวอักษรแรกของประโยค/วลีที่จำได้, ผสมคำสั้น 2–3 คำแล้วกดตำแหน่งบนคีย์บอร์ดแบบมีรูปแบบ, ค่อยๆ เพิ่มความซับซ้อน

• ตัวอย่างการออกแบบ: นำเนื้อเพลง/วลีที่ชอบมาแปลง/สลับภาษาคีย์บอร์ด/สลับพิมพ์เล็กใหญ่ เพื่อสร้างรหัสที่ซับซ้อน

• เมื่อรหัสแข็งแรงแล้ว: เปิดใช้ 2FA เมื่อทำได้, หลีกเลี่ยงใช้รหัสเดียวกันข้ามเว็บไซต์ (ป้องกัน “Credential Reuse”), ใช้ Password Manager ที่น่าเชื่อถือ

### 2. เทคโนโลยีการพิสูจน์ตัวบุคคล (Authentication)

• MFA: ใช้มากกว่า 1 ปัจจัย — ความรู้ (สิ่งที่รู้: รหัสผ่าน/พิน), การครอบครอง (สิ่งที่มี: SMS/แอป/โทเคน/USB key), และความเป็นตัวตน (สิ่งที่เป็น: ลายนิ้วมือ/เรตินา/ใบหน้า/เสียง)

• 2FA: รูปแบบย่อยของ MFA ที่นิยม (เช่น รหัสผ่าน + ยืนยันทางมือถือ) ควรใช้กับแอปการเงิน, โซเชียล, อีเมล

• Biometric Authentication: โหมดยืนยัน (1–1) และระบุตัว (1–n); ประเภทชีววิทยา (ลายนิ้วมือ/เรขาคณิตมือ/ใบหน้า/ไอริส/เรตินา) และพฤติกรรม (เสียง/จังหวะการกดแป้น/ลายเซ็น) — แต่ละแบบมีข้อดี/ข้อจำกัด (เช่น ใบหน้าต้องมี Liveness Detection ในสภาพไม่มาตรฐาน)

## ภัยคุกคามในระบบสารสนเทศและแนวทางป้องกัน **(หน้าที่ 410–421[91–102])**

### 1. ประเภทการโจมตีโดยทั่วไป

• มัลแวร์ (Malware): ไวรัส, เวิร์ม, โทรจัน, แบ็กดอร์, สปายแวร์, คีย์ล็อกเกอร์, บอตเน็ต, รูทคิต — อาจทำลายข้อมูล/ยึดอุปกรณ์ (เช่น WannaCry)

• ฟิชชิง (Phishing): หลอกให้เปิดไฟล์/ลิงก์อันตราย (ปลอมเป็นผู้บริหาร/หน่วยงานน่าเชื่อถือ)

• SQL Injection: เจาะฐานข้อมูลบนเซิร์ฟเวอร์ เข้าถึงข้อมูลสำคัญ (ลูกค้า/ส่วนบุคคล/บัตรเครดิต/การเงิน)

• Cross‑Site Scripting (XSS): ฉีดสคริปต์โจมตีผู้ใช้เว็บ ไม่ทำลายตัวเว็บ แต่ขโมยข้อมูลฝั่งผู้ใช้

• DoS/DDoS: ถล่มทราฟฟิกจนระบบให้บริการไม่ได้

• Session Hijacking / Man‑in‑the‑Middle: ดักเซสชัน/สวมกลางทาง

• การใช้ข้อมูลยืนยันซ้ำ (Credential Reuse): ใช้รหัสซ้ำข้ามระบบเพิ่มความเสี่ยงรั่วไหลเป็นลูกโซ่

### 2. แนวทางป้องกันด้านความปลอดภัย (ระดับผู้ใช้)

• เปลี่ยนรหัสทันทีเมื่อเกิดเหตุเกี่ยวกับความปลอดภัยกับบริการที่ใช้อยู่, ใช้ 2FA/MFA, อัปเดตแพตช์/แอนติไวรัส, สำรองข้อมูล, ระวังลิงก์/ไฟล์แนบ, ตรวจสิทธิ์แอป, แยกบัญชีงาน/ส่วนตัว

## สรุปและกรณีศึกษา — ความเป็นส่วนตัวยุคดิจิทัล/รอยเท้าดิจิทัล **(หน้าที่ 422–424[103–105])**

• กรณี Facebook และ Cambridge Analytica: นักพัฒนาภายนอกเข้าถึงข้อมูลส่วนตัวผู้ใช้ผ่านการเชื่อมต่อแอป/แบบสอบถามบุคลิกภาพ แล้วนำไปวิเคราะห์วางแนวทางหาเสียงทางการเมือง (กรณี Donald Trump) — ทำให้สังคมตั้งคำถามเรื่องการคุ้มครองข้อมูลจนเกิดกระแส #DeleteFacebook สะท้อนการตระหนัก “รอยเท้าดิจิทัล/ความเป็นส่วนตัว” ของประชาชนมากขึ้น