

จรรยาบรรณ สำหรับคนทำเว็บ

Ethical Web Development

Privacy • Accessibility • Security • Responsibility

▶ START



แอมป์ ศิริพัฒน์ กล่าวกลั่น

การศึกษา

- MSc. Management Information Systems
– University of Surrey, UK
- Graduate Diploma in Management
– University of Surrey, UK
- ปริญญาตรี รัฐกิจศึกษา – คอมพิวเตอร์
– RMUTT



การทำงาน

- ผู้อำนวยการศูนย์การเรียนรู้ตลอดชีวิต – มหาวิทยาลัยกรุงเทพ
- Nerve Digital Agency Co., Ltd. – CEO & Co-Founder
- Web2Print Solution Co., Ltd. – CEO & Co-Founder
- กรรมการสมาคมผู้ดูแลเว็บไซต์และสื่อออนไลน์ไทย
- กรรมการประเมินมาตรฐาน – สถาบันคุณวุฒิวิชาชีพ
- SAP Functional Consultant – PTT Digital Solutions
- ข้าราชการครู – สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน



“
สร้างคุณค่า
ผ่านความรู้
เทคโนโลยี
และการเรียนรู้
ตลอดชีวิต
”

Lifelong
Learner

Creator

Innovator

Helper

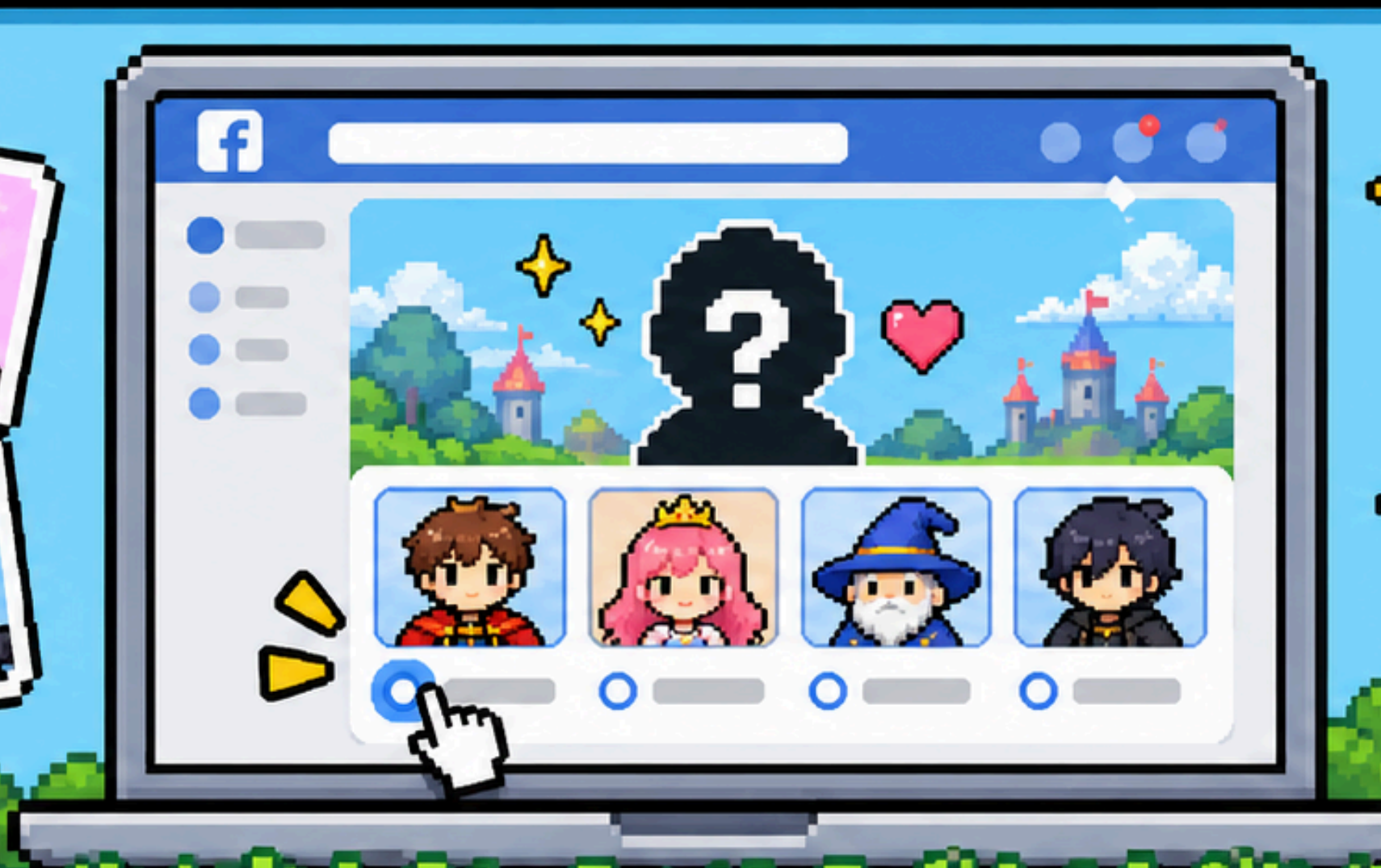


ใครเคยทำสิ่งนี้
ในโลกออนไลน์บ้าง?

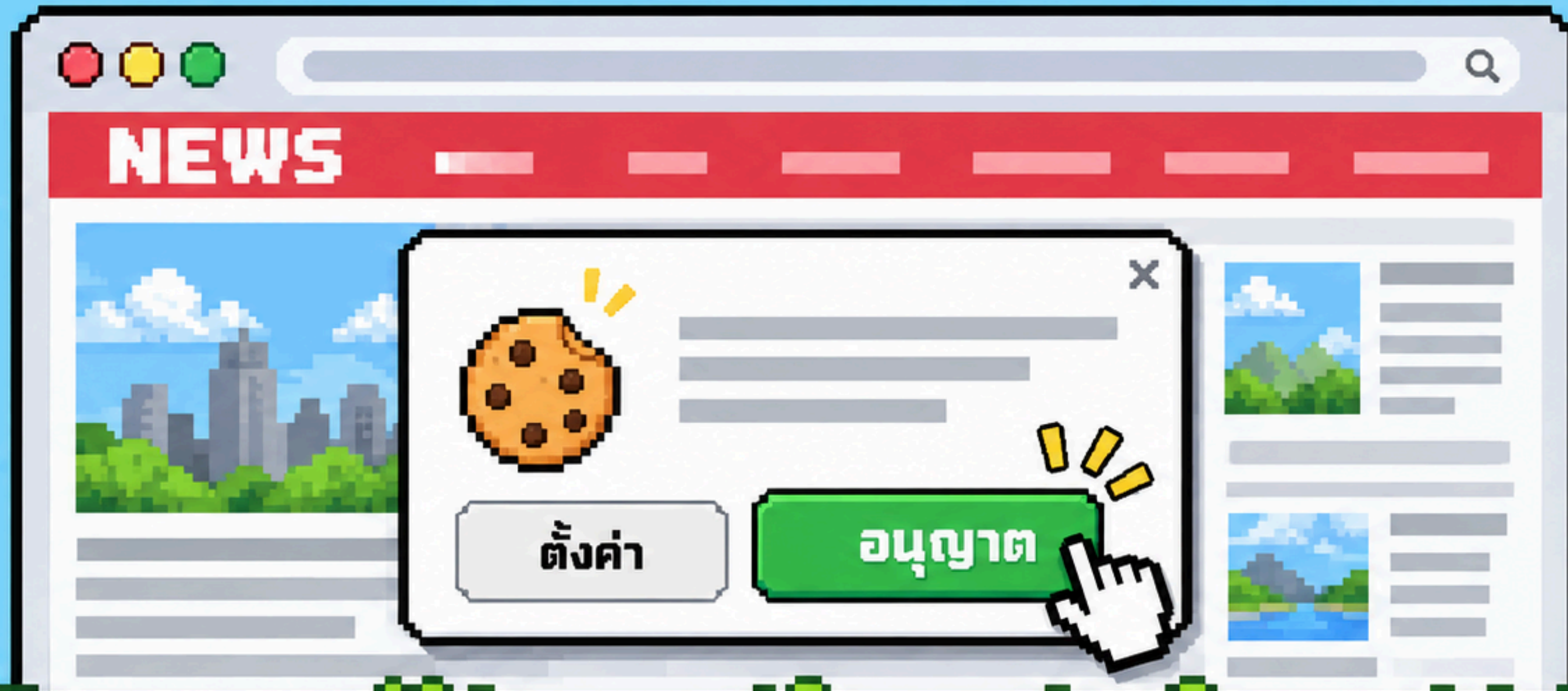


เล่นเกมบน Facebook Quiz

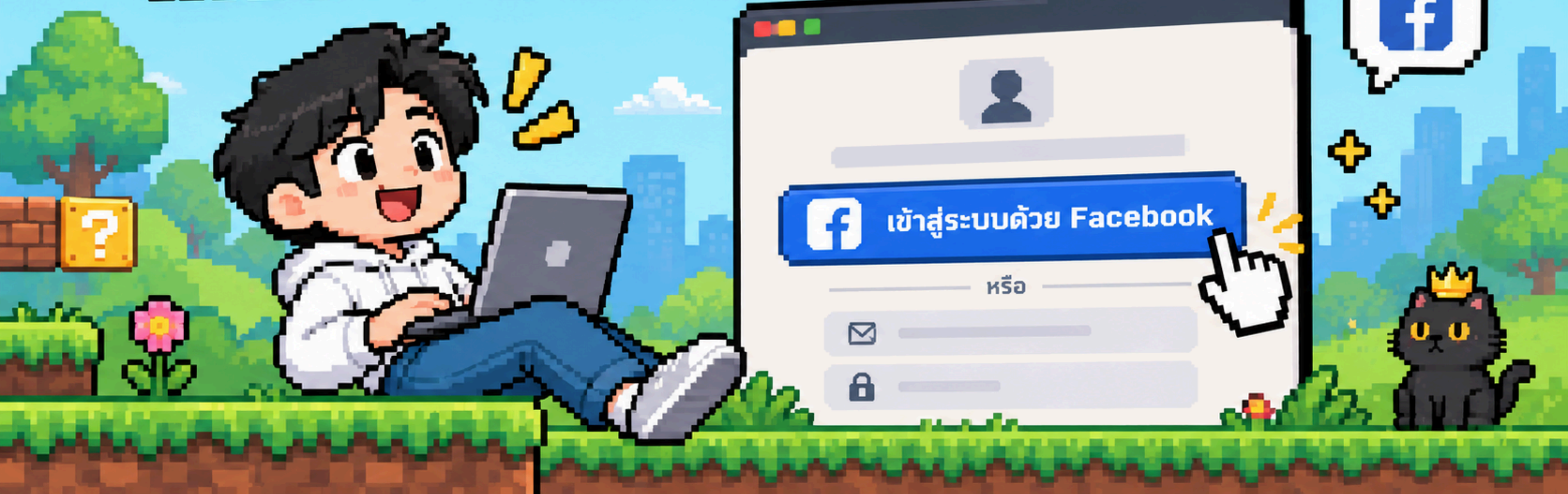
คุณเป็นตัวละครใดในซีรีส์นี้?



เข้าเว็บแล้วเจอ**ป๊อปอัพ**คุณก็
กดปุ่มอนุญาตผ่าน ๆ ไปก่อน จะได้อ่านข่าวต่อ



สมัครแอปด้วยปุ่ม “เข้าสู่ระบบด้วย Facebook” เพราะขี้เกียจตั้งรหัสใหม่



ปี 2014 มีนักวิจัยจากมหาวิทยาลัยเคมบริดจ์
ทำแอปชื่อ **thisisyourdigitallife**
ให้คนมาตอบคำถามเรื่องนิสัยตัวเอง



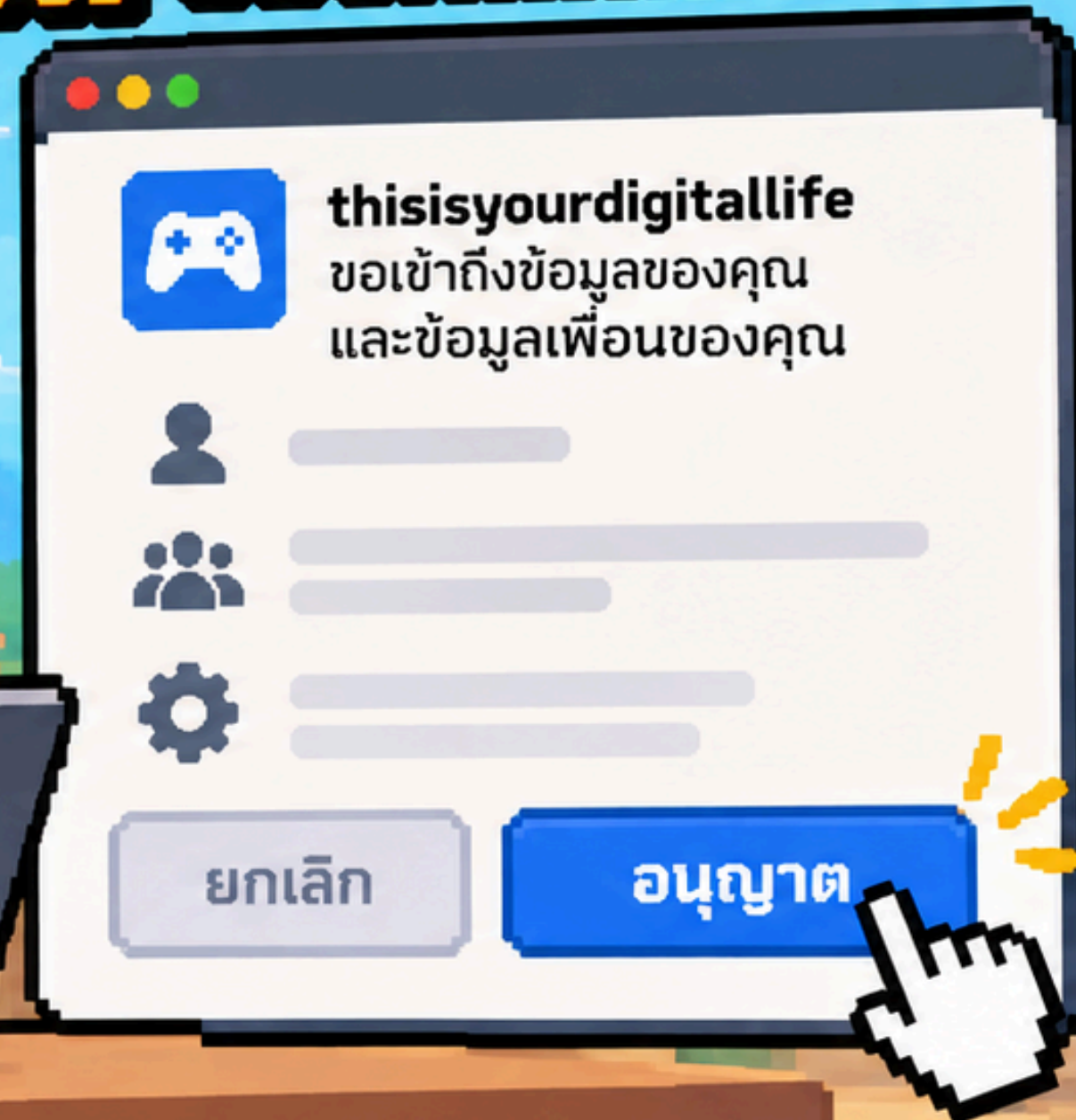
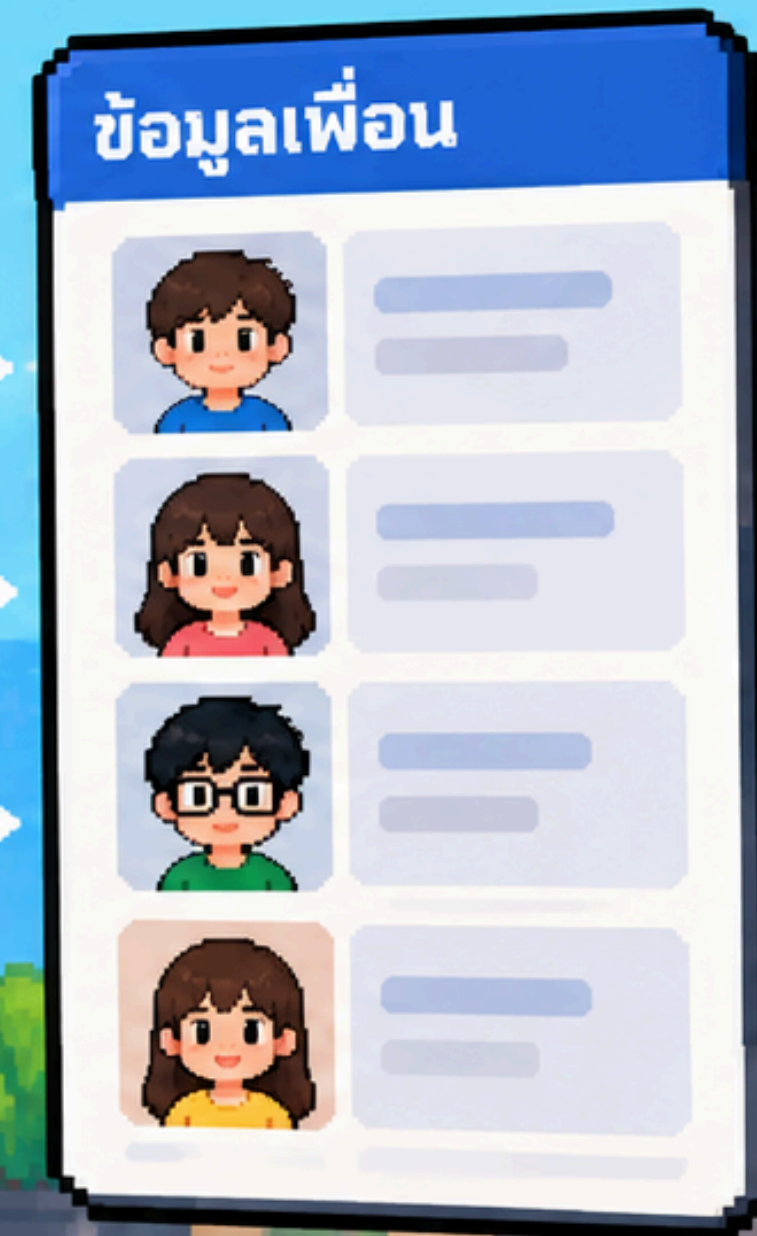
thisisyourdigitallife



UNIVERSITY OF
CAMBRIDGE



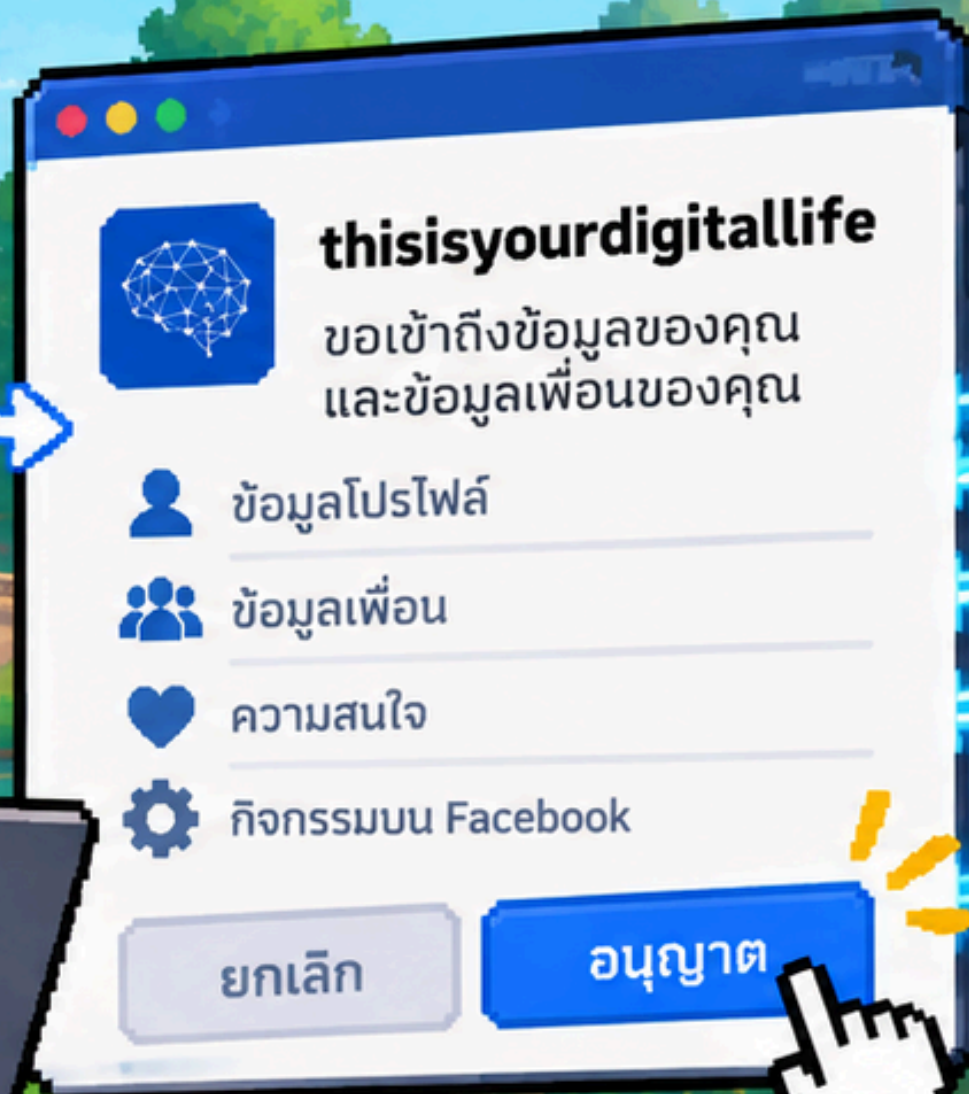
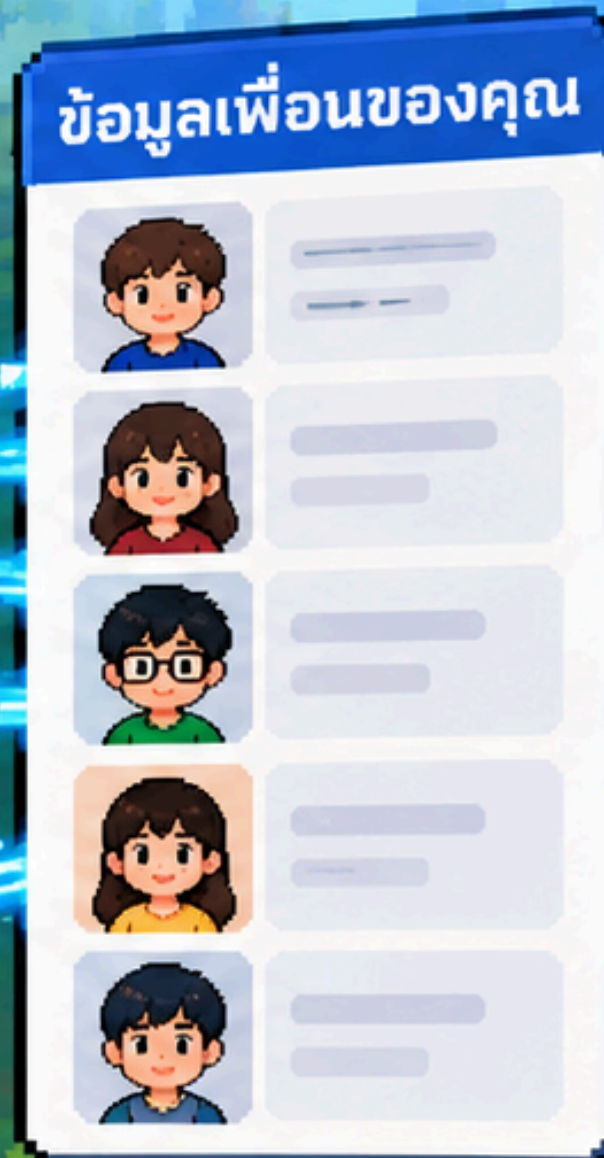
ก่อนเล่น แอปขอดูโปรไฟล์
คนก็กด **อนุญาต** เหมือนที่เรากดทุกวัน
แต่ Facebook สมัยนั้นยอมให้แอปเห็น
ข้อมูลเพื่อน ของคนที่กดด้วย



เพื่อนพวกนั้น **ไม่ได้เล่น** ไม่ได้กดอะไร
และไม่มีใครถามเขาสักคำ
ข้อมูลทั้งก้อนถูกส่งต่อให้ **Cambridge Analytica**
บริษัทที่รับทำแคมเปญหาเสียงเลือกตั้ง



Cambridge
Analytica

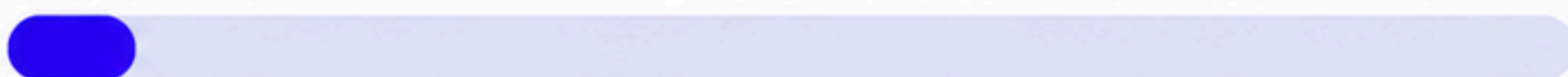


ความเสียหายจาก Cambridge Analytica

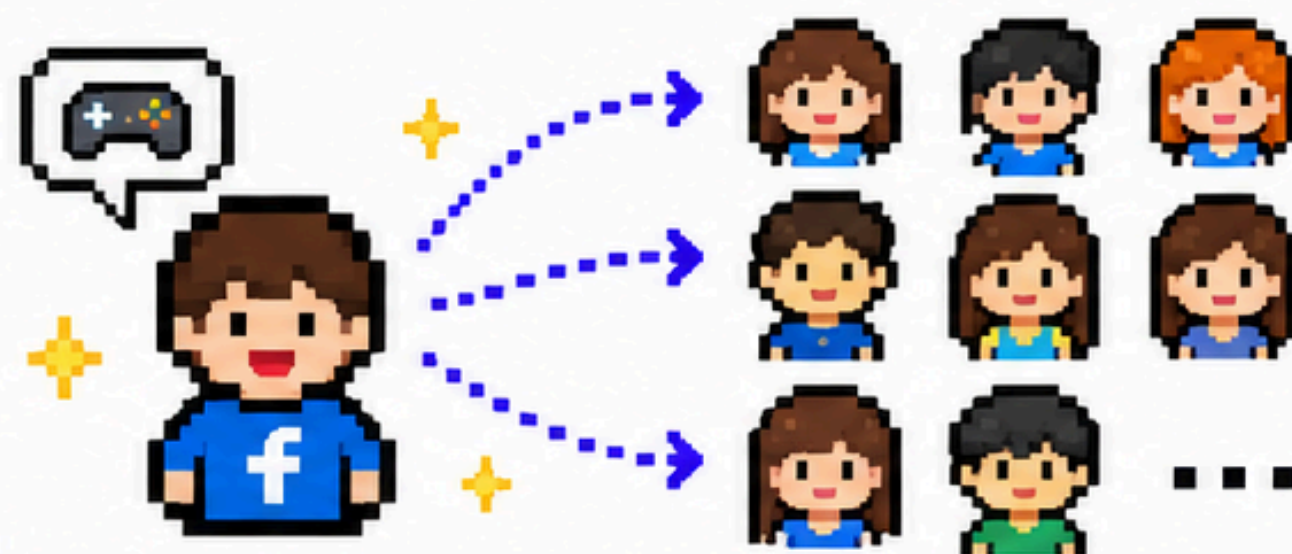


คนที่เล่น

≈ 270,000



คนเล่นหนึ่งคน พาเพื่อนติดไปด้วย เฉลี่ยราว 320 คน

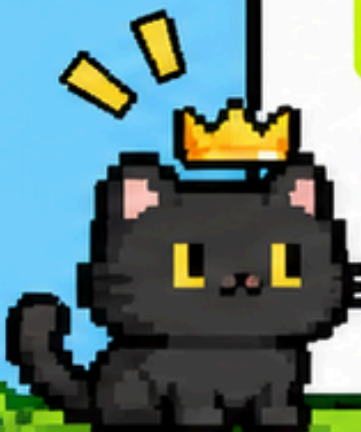


คนที่ข้อมูลหลุด

≈ 87,000,000



มากกว่าคนไทยทั้งประเทศ ที่มีราว 66 ล้านคน



ไทม์ไลน์ Cambridge Analytica

★ เกิดอะไรขึ้น • ใครได้รับผลกระทบ ★

ปี	เกิดอะไรขึ้น	ใครเจ็บ
 2014	แบบทดสอบดูดข้อมูลคนเล่นกับเพื่อนของคนเล่นออกไป	 คนใช้ Facebook ที่ไม่รู้ตัว
 2016	ข้อมูลถูกใช้แบ่งกลุ่มคนตามนิสัย แล้วยิงโฆษณาหาเสียงให้ตรงใจแต่ละกลุ่ม	 คนที่ไปเลือกตั้ง
 มี.ค. 2018	อดีตพนักงานของ Cambridge Analytica เล่าทุกอย่างให้หนังสือพิมพ์ฟัง ข่าวย่ออกทั่วโลก	 ความเชื่อใจที่คนมีต่อ Facebook
 เม.ย. 2018	ผู้ก่อตั้ง Facebook ต้องไปนั่งตอบคำถามต่อสภาองเกรสสหรัฐฯ	 Facebook
 พ.ค. 2018	Cambridge Analytica ปิดบริษัท	 พนักงานทั้งบริษัท
 ก.ค. 2019	FTC ปรับ Facebook 5,000 ล้านดอลลาร์	 Facebook



★ ถ้าเป็นเรา เขียนแอปเสร็จแล้วเพิ่งรู้ว่าดึงข้อมูล
เพื่อนของคนเล่นได้ทั้งหมด จะดึงไหม



A

ดึงสิ ระบบให้ป่ะ

B

ไม่เอาดีกว่า

สิ่งที่ผิดกฎหมาย

เขียนโค้ดเป็น แสกเว็บเป็น ทำได้หมด

สิ่งที่กฎหมายไม่ห้าม

ไม่มีใครมาจับ แต่อาจมีคนเจ็บ

สิ่งที่ควรทำ

ทำแล้วคนปลายทาง
ไม่เดือดร้อน



ยกตัวอย่างใกล้ชิด
เพื่อน ลืมล็อคมือถือ
วางไว้บนโต๊ะแล้วไปเข้าห้องน้ำ





ความเป็นส่วนตัว

★ Privacy ★



เคสจริง: ข้อมูลผู้ป่วยรั่ว 3 ล้านราย

★ Advocate Aurora Health • Meta Pixel Tracker ★



สรุปเคส



เครือข่ายโรงพยาบาล Advocate Aurora Health
มีข้อมูลผู้ป่วยรั่วประมาณ 3 ล้านราย



สาเหตุสำคัญมาจากการติดตั้ง Meta Pixel tracker
แบบไม่เหมาะสม



ข้อมูลการใช้งานบนเว็บด้านสุขภาพอาจถูกส่งต่อออกไป
โดยผู้ไม่รู้ตัว



เหตุการณ์นี้ทำให้เกิดการสอบสวน และกลายเป็น
บทเรียนเรื่อง Privacy by Design

KEYWORD

Tracking

Meta Pixel

Health Data

Privacy

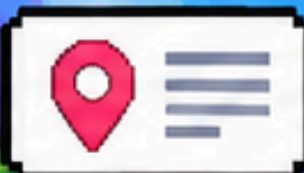
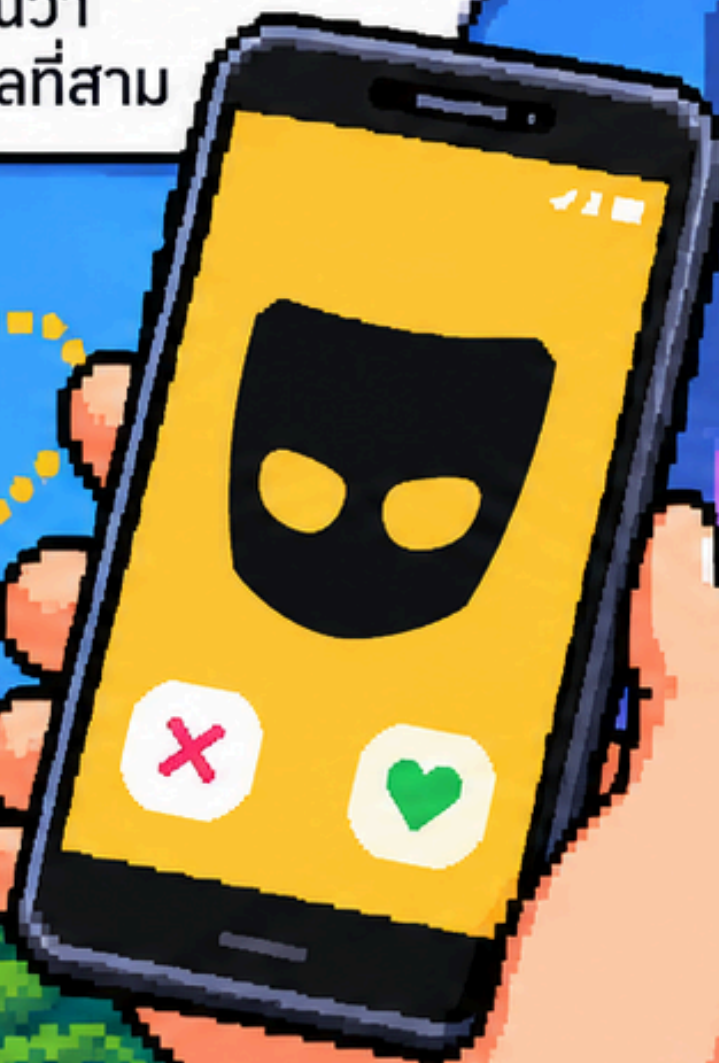
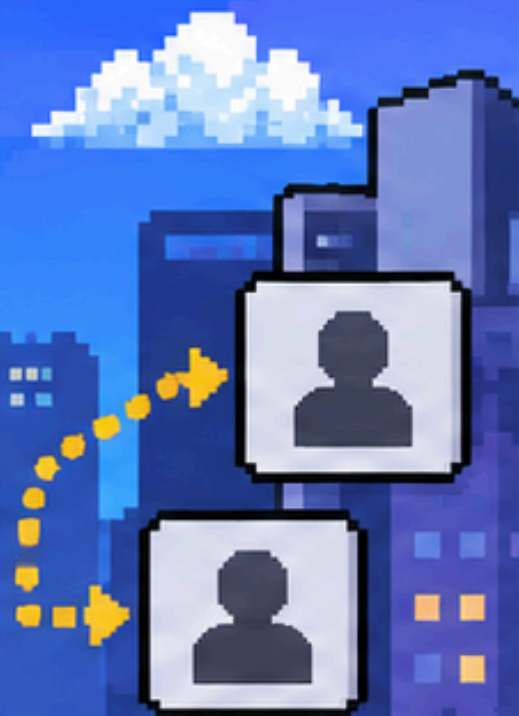


เคสจริง: Grindr แชร์ข้อมูล HIV

★ Sensitive Data • Privacy • PDPA ★

Grindr's HIV data-sharing

แอปหาคู่เกย์ถูกวิจารณ์ว่า
แชร์ข้อมูล HIV ให้บุคคลที่สาม



สรุปเคส



แอป Grindr เคยมีประเด็นแชร์ข้อมูล HIV
และข้อมูลส่วนตัวใกล้ชิดให้กับบุคคลที่สาม



ข้อมูลลักษณะนี้เกี่ยวข้องกับสุขภาพและรสนิยมทางเพศ
ซึ่งเป็นข้อมูลอ่อนไหว



ตามแนวคิด PDPA การเก็บ ใช้ หรือเปิดเผยข้อมูลแบบนี้
ต้องขอความยินยอมอย่างชัดเจน



บทเรียนสำคัญคือ ต้องปกป้อง Sensitive Data
ให้เข้มกว่าข้อมูลทั่วไป



ข้อมูลอ่อนไหวตาม PDPA



สุขภาพ / ความพิการ / พันธุกรรม



ลายนิ้วมือ / ใบหน้า / ชีวภาพอื่น



ศาสนา / ความเชื่อ / ความคิดเห็นทางการเมือง



เชื้อชาติ / พฤติกรรมทางเพศ / ประวัติอาชญากรรม



Sensitive Data ต้องขอความยินยอมแบบชัดเจน



ปุ่มยอมรับอยู่ตรงหน้า ปุ่มปฏิเสธซ่อนอยู่หลายชั้น



มกราคม 2022 หน่วยงานคุ้มครองข้อมูลของฝรั่งเศส (CNIL) ปรับ Google 150 ล้านยูโร
และ Facebook 60 ล้านยูโร เพราะกดปฏิเสธคุณที่ยากกว่ากดยอมรับ



❌ แบบที่โดนปรับ



เราใช้คุกกี้เพื่อมอบประสบการณ์ที่ดีที่สุดให้คุณ



ยอมรับทั้งหมด

[ตั้งค่าเพิ่มเติม](#)



จะปฏิเสธต้องกดลิงก์ตัวเล็ก ไล่ปิดทีละหมวด แล้วกดยืนยันอีกที
ทำไปครึ่งทางคนก็ถอดใจ กลับมากดปุ่มใหญ่



✅ แบบที่ถูก



เว็บนี้ใช้คุกกี้วัดสถิติและทำโฆษณา จะให้เก็บไหม



ยอมรับ

ปฏิเสธ

เลือกเอง



ยอมรับกับปฏิเสธ ขนาดเท่ากัน สีเดียวกัน อยู่ข้างกัน
กดครั้งเดียวจบเหมือนกัน



ก่อนทำฟอร์มสักอัน ตามตัวเองห้าข้อ

1  **ช่องนี้เอาไปใช้ทำอะไร** ถ้าตอบไม่ได้ ลบช่องนั้นทิ้ง



2  **บอกคนกรอกหรือยัง** ว่าเก็บอะไร เอาไปทำอะไร เก็บไว้นานแค่ไหน
เขียนให้คนทั่วไปอ่านรู้เรื่อง



3  **ถ้าเขาไม่อยากให้** ปฏิเสธได้ง่ายเท่ากับตอบตกลงไหม



4  **โค้ดคนอื่นที่แปะไว้ในหน้านี้** ส่งอะไรออกไปบ้าง



5  **งานจบแล้ว ลบข้อมูลหรือยัง** ข้อมูลเก่าที่ไม่มีใครใช้ ก็ยังรู้ได้



การเข้าถึง

Accessibility



Domino's · ผู้ชายคนหนึ่ง แค่อยากสั่งพิซซ่า

เรื่องราวของ Guillermo Robles ผู้ชายตาบอดในแคลิฟอร์เนีย ที่พยายามสั่งพิซซ่าผ่านเว็บไซต์และแอปของ Domino's ได้ยากลำบาก จนกลายเป็นคดีสำคัญที่สะท้อนว่า “การเข้าถึง” คือสิทธิของทุกคน

1

ปี 2016

Guillermo Robles ชายตาบอดในแคลิฟอร์เนีย พยายามสั่งพิซซ่าผ่านเว็บไซต์และแอปของ Domino's ด้วยโปรแกรมอ่านหน้าจอ แต่สั่งไม่ได้ เขาเลยฟ้อง

2

ปี 2019

Domino's เลือกสู้ในศาล บอกว่ากฎหมายคนพิการ ไม่ได้ครอบคลุมเว็บ แต่สุดท้ายศาลอุทธรณ์ตัดสินว่า **เว็บไซต์และแอปก็ต้องให้คนพิการใช้ได้**

3

ตุลาคม 2019

Domino's ยื่นต่อถึงศาลฎีกาสหรัฐฯ แต่ ศาลฎีกา **ไม่รับพิจารณา** คำตัดสินเดิมจึงใช้ต่อ



“การเข้าถึงไม่ใช่เรื่องของความสะดวก แต่เป็นสิทธิพื้นฐานของทุกคน”



≈ 1.3 พันล้าน

คนทั่วโลกมีความพิการระดับใดระดับหนึ่ง
ราว 1 ใน 6 ของคนทั้งโลก
(องค์การอนามัยโลก)



≈ 1 ใน 5

ของคนไทยอายุ 60 ปีขึ้นไปแล้ว
หลายคนอาจเข้าถึงเทคโนโลยีไม่ได้
อย่างเต็มที่



ความปลอดภัย



Security



Equifax - ตัวแก้มีแล้ว แต่ไม่มีใครกดติดตั้ง

Equifax เก็บประวัติการเงินของคนอเมริกันแทบทั้งประเทศ ปี 2017 ระบบถูกเจาะผ่านช่องโหว่ใน Apache Struts ที่มีตัวแก้ออกมา ตั้งแต่สองเดือนก่อน



147 ล้านคน

มากกว่าคนไทยสองเท่า ที่หลุดไปมีเลขประกันสังคมวันเกิด และที่อยู่



ราว 2 เดือน

ที่ตัวแก้รออยู่เฉย ๆ ต่อมาบริษัทยอมความเป็นเงินสูงสุดราว 700 ล้านดอลลาร์ (2019)

เคสจริง: British Airways ข้อมูลรั่ว

Magecart • Card Skimming • GDPR



เกิดอะไรขึ้น?

แฮกเกอร์ฝังโค้ดอันตรายในเว็บไซต์และแอปของ British Airways เพื่อดักข้อมูลการชำระเงินแบบเรียลไทม์ ขณะลูกค้าจองตั๋ว



เกิดเมื่อไร?

การโจมตีเกิดขึ้นช่วง 21 ส.ค. 2018 – 5 ก.ย. 2018 และบริษัทเปิดเผยเหตุการณ์ในวันที่ 6 ก.ย. 2018



ใครอยู่เบื้องหลัง?

เหตุการณ์นี้ถูกโยงกับกลุ่ม Magecart ที่เชี่ยวชาญการโจมตีแบบดักข้อมูลบัตรเครดิตบนเว็บอีคอมเมิร์ซ



ผลกระทบ

ข้อมูลส่วนบุคคลและข้อมูลการเงินของลูกค้าหลายแสนรายถูกเปิดเผย และคดีนี้นำไปสู่ค่าปรับ GDPR ก้อนใหญ่



15 วัน

ช่วงเวลาที่โค้ดอันตรายทำงานในระบบ



บทเรียนสำคัญ

เว็บที่รับชำระเงินต้องเฝ้าระวัง JavaScript ภายนอกและความเสี่ยงของ supply-chain attack

หกนิสัยที่กันเรื่องเมื่อก็ได้ทั้งหมด



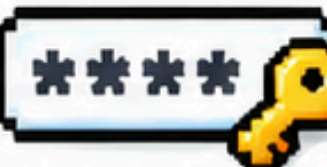
1 มีตัวแก้ความปลอดภัยออกมา อัปเดตให้เร็ว



2 ที่เก็บไฟล์บนคลาวด์ ตั้งเป็นส่วนตัวไว้ก่อนเสมอ



3 รหัสผ่าน เก็บแบบ hash เช่น bcrypt ห้ามเก็บตัวหนังสือตรง ๆ



4 API key กับรหัสผ่าน อย่าเผลออัปขึ้น GitHub



5 สคริปต์จากข้างนอก ที่อยู่หน้าสำคัญ ต้องรู้ว่ามาจากไหน



6 บอกลูกค้ายาลบแล้ว ต้องลบจริง รวมไฟล์สำรองด้วย





ความรับผิดชอบ

★ Responsibility ★

npm install หนึ่งครั้ง เราใส่ใจคนแปลกหน้าที่คน

แพ็กเกจเล็ก ๆ ที่เราติดตั้ง อาจถูกพัฒนาและดูแลโดยคนที่เราไม่รู้จัก
แต่กลับมีสิทธิ์เข้าถึงโค้ดและข้อมูลของเราได้มหาศาล



left-pad · มีนาคม 2016

11 บรรทัด ที่ทำให้งานของคนทั้งโลกพัง

นักพัฒนาคนหนึ่งเข้าใจเรื่องชื่อแพ็กเกจ เลยลบแพ็กเกจทั้งหมด
ของตัวเองออกจาก npm หนึ่งในนั้นคือ left-pad ยาวราว 11 บรรทัด
แต่โปรเจกต์ใหญ่ทั่วโลกพึ่งมันอยู่ทางอ้อม วันนั้น build พังกันทั่วโลก



event-stream · พฤศจิกายน 2018

ยกไลบรารีให้คนที่อาสาช่วย

คนดูแลไลบรารีที่มีคนโหลดหลายล้านครั้งต่อสัปดาห์ เหนื่อยแล้ว
เลยยกให้คนที่อาสาช่วย คนนั้นแอบใส่โค้ดที่เล็งขโมยบิตคอยน์
จากแอปกระเป๋าเงินแอปหนึ่ง



AI คัดใบสมัครงาน ที่เรียนอคติมาจากอดีต

- 1 Amazon ทำ AI ช่วยคัดใบสมัคร โดยให้เรียนจากใบสมัครที่บริษัทได้รับตลอด **10 ปี** ซึ่งส่วนใหญ่มาจากผู้ชาย
- 2 AI สรุปเองว่าคนที่ดีคือคนที่หน้าตาใบสมัครเหมือนผู้ชาย ใบไหนมีคำว่า **"women's"** เช่น หัวหน้าชมรมหมากรุกหญิง ก็โดนหักคะแนน
- 3 ทีมพยายามแก้ แต่ไม่มั่นใจว่าจะไม่มีอคติแบบอื่น ซ่อนอยู่อีก สุดท้าย **เลิกใช้** (Reuters รายงาน ปี 2018)



ก่อนเอาโค้ดที่ AI เขียนไปใช้

อย่าเพิ่งไว้วางใจ! ตรวจสอบให้ดี เพื่อความปลอดภัยของงานและข้อมูล

-  **อ่านทุกบรรทัด**
บรรทัดไหนอธิบายไม่ได้ว่าทำอะไร อย่าเพิ่งใช้
-  **פקגעที่ AI แนะนำ มีอยู่จริงไหม**
AI เคยแต่งชื่อแพ็กเกจขึ้นมาเอง แล้วมีคนร้ายไปจดชื่อนั้นร่อไว้
-  **ข้อมูลส่วนตัวของคนใช้กับ API key**
อย่าแปะลงแชต AI
-  **ถ้าระบบตัดสินใจเรื่องคน**
ลองกับคนหลายแบบ ดูว่ามันเอียงไปทางไหน
-  **ถามเรื่องความปลอดภัยตรง ๆ**
เช่น “โค้ดนี้โดน SQL Injection ได้ไหม”





PDPA ฉบับคนทำเว็บ



พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้เต็มรูปแบบ
ตั้งแต่ 1 มิถุนายน 2565 คนดูแลคือสำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล (สคส.)



บอกก่อนเก็บ ว่าจะเอาไปทำอะไร



เจ้าของข้อมูลขอได้ ขอดู ขอแก้ ขอลบ หรือเปลี่ยนใจ
ไม่ยินยอมแล้วก็ได้



ข้อมูลรั่ว ต้องแจ้ง สคส. ภายใน 72 ชั่วโมงหลังรู้ตัว



ต้องมีวิธีกันข้อมูลรั่ว ให้เหมาะกับข้อมูลที่เก็บ



ถ้าพลาด โดนได้สามทาง



ทางแพ่ง

จ่ายค่าเสียหายจริง แล้วศาลสั่งเพิ่ม
ได้อีกไม่เกิน 2 เท่า



ทางอาญา

กรณีร้ายแรง เช่น เอาข้อมูลอ่อนไหว
ไปใช้ในทางที่ผิด จำคุกไม่เกิน 1 ปี
หรือปรับไม่เกิน 1 ล้านบาท



ทางปกครอง

ปรับได้สูงสุด 5 ล้านบาทต่อกรณี



สิงหาคม 2567 • คำปรับ PDPA ครั้งแรกของไทย

สคส. ปรับบริษัทขายสินค้าไอทีรายใหญ่รวม 7 ล้านบาท หลังข้อมูลลูกค้าหลุด แล้วไปอยู่ในมือแก๊งคอลเซ็นเตอร์

ขั้นที่ 1



ลูกค้าสั่งของออนไลน์
กรอกชื่อ เบอร์ ที่อยู่
ตามปกติ

ขั้นที่ 2



ข้อมูลลูกค้ารั่วออก
จากระบบของร้าน

ขั้นที่ 3



แก๊งคอลเซ็นเตอร์โทรหา
อ้างรายละเอียดออเดอร์จริง
จนลูกค้าเชื่อ

ขั้นที่ 4



สคส. ตรวจสอบ
แล้วปรับ 7 ล้านบาท



ไม่มี DPO

ไม่ได้ตั้งคนดูแลข้อมูล
ส่วนบุคคล ทั้งที่กฎหมาย
บังคับ



กันไม่ดีพอ

วิธีป้องกันข้อมูลไม่สมกับ
ข้อมูลลูกค้าจำนวนมาก
ที่เก็บไว้



รั่วแล้วไม่แจ้ง

ไม่แจ้งเหตุข้อมูลรั่วต่อ สคส.
ตามที่กฎหมายกำหนด





ขอบคุณครับ

★ Thank You ★