# Gu. Digital: รับมืออย่างไร เมื่อเจอภัยในโลกออนไลน์

นางสาวดวงสมร ชูดีจันทร์
ช่างภาพการแพทย์ชำนาญการ

ปัญหาด้านความปลอดภัยของการใช้งานโปรแกรมประเภท Social Network ก็คือ ความรู้เท่าไม่ถึงการณ์ของผู้ใช้ที่ไม่มีความรู้ความเข้าใจเรื่องความมั่นคงปลอดภัยสารสนเทศดีพอ เริ่มจากการใช้ Email address เป็นชื่อในการ Login และ ใช้รหัสผ่านของ Email ที่ใช้อยู่ เช่น Hotmail หรือ G-mail เป็นรหัสผ่านของโปรแกรมประเภท Social Network เช่น Facebook หรือ Twitter ซึ่งความจริงแล้วไม่จำเป็นต้องใช้รหัสผ่านเดียวกัน การที่ใช้รหัสผ่านเดียวกับ email จะทำให้ถูกเจาะระบบได้ง่ายเพราะโปรแกรม Social Network ส่วนใหญ่มัก Log on หรือ Sign on โดยใช้โปรโตคอล http ที่ไม่มีความปลอดภัยเท่ากับโปรโตคอล https หรือ "SSL" ที่ รู้จักกันดีในกลุ่มผู้ใช้งานอินเทอร์เน็ตแบงค์กิ้ง จึงสามารถถูกแฮกเกอร์ดักจับรหัสผ่านได้โดยง่าย จากนั้นแฮกเกอร์ก็สามารถเจาะเข้าถึง E-mail ของเหยื่อแล้วสวมรอยเป็นตัวเหยื่อได้อย่างง่ายดาย ดังนั้น จึงควรระมัดระวังเรื่องการใช้รหัสผ่านดังกล่าว

ปัญหาอีกปัญหาหนึ่งที่พบประจำ คือ ปัญหาข้อมูลส่วนตัวของรั่วไหลออกไปยังกลุ่มมิจฉาชีพโดยไม่ได้ตั้งใจ กล่าวคือ หากสมัคร Facebook จากโทรศัพท์มือถือทาง Facebook จะให้ Confirm ด้วยเบอร์โทรศัพท์มือถือของเท่ากับได้บอกเบอร์โทรศัพท์ให้กับ Facebook ไปโดยปริยาย ซึ่งการสมัคร Facebook จากเครื่อง Notebook หรือ เครื่อง Desktop จะไม่ต้องกรอกข้อมูลเบอร์โทรศัพท์ดังกล่าว นอกจากนั้นบางคนยังใส่เบอร์โทรศัพท์ รวมทั้ง วัน เดือน ปีเกิด เข้าไปในระบบของ Facebook โดย ไม่ระมัดระวัง เป็นเหตุให้มิจฉาชีพสามารถค้นหาเบอร์โทรศัพท์มือถือ และข้อมูลส่วนตัว เช่น วัน เดือน ปีเกิด ได้อย่างง่ายดาย จึงไม่ควรป้อนข้อมูลส่วนตัวดังกล่าวให้กับโปรแกรมประเภท Social Network โดยไม่จำเป็น ยิ่งใส่ข้อมูลส่วนตัวลงไปเท่าใดก็ยิ่งเปิดช่องให้แฮกเกอร์และเหล่ามิจฉาชีพสามารถเข้าถึงข้อมูลส่วนตัวของได้ง่ายมากขึ้นเท่านั้น

ในปัจจุบันแฮกเกอร์สมัยใหม่ได้ใช้เทคนิคใหม่ๆ ในการหาข้อมูลของเป้าหมายที่เรียกว่า"Target Profiling" หรือ "Targeted Attack" โดยใช้เทคนิค"Intelligence Information Gathering" ซึ่งมีความล้าหน้ากว่าการหาข้อมูลจากการ Search จาก Google โดยการใช้ Software ที่ถูกออกแบบมาเจาะหลังบ้านของ Facebook และ Twitter โดยตรง ซึ่งปกติแล้วจาก Twitter และ Facebook จะเปิดช่องหรือเปิด API ให้โปรแกรมเมอร์เข้ามาใช้ดึงข้อมูลของผู้ใช้ Facebook และ Twitter เพื่อใช้ในการเขียนโปรแกรม Game ต่าง ๆ ที่ท างานอยู่ใน Social Network โดยปกติแล้วเฉพาะโปรแกรมเมอร์ที่มี API เท่านั้นจึงสามารถเข้าถึงข้อมูลหลังบ้านจาก Server ที่เรียกว่า "TAS" หรือ "Transformation Server" แต่โปรแกรมที่แฮกเกอร์ใช้ในการเจาะระบบ Social Network หรือ โปรแกรมที่หน่วยข่าวกรอง เช่น CIA หรือ FBI ใช้มีความสามารถเข้าไป "Search" ข้อมูลเชิงลึกจาก Server หลังบ้านในระบบผู้ให้บริการ Social Network ดังกล่าวได้จึงต้องระวังให้มากเวลาที่จะป้อนข้อมูลส่วนตัวของลงในโปรแกรมประเภท Social Network ดังกล่าว

# Gu. Digital: รับมืออย่างไร เมื่อเจอภัยในโลกออนไลน์

นอกจากนี้ ผู้ใช้หลายท่านยังไม่ทราบว่า ข้อมูลที่อยู่ในระบบ Social Network สามารถค้นหาได้โดยง่ายจากการใช้ Google โดยบางคนนำข้อมูลที่ควรเป็นความลับขององค์กร เช่น Network Diagram หรือ Minute Of Meeting ทำการ upload เข้าสู่โปรแกรม Social Network โดยไม่ระมัดระวัง ทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ควรจะเป็นข้อมูลลับขององค์กรหรือข้อมูลส่วนตัวของโดยที่ไม่รู้ตัวเลยว่าข้อมูลของได้หลุดไปเรียบร้อยแล้ว

การป้องกันภัยจากความไม่รู้ดังกล่าวนั้นสามารถทำได้ไม่ยาก คือ ต้องมี "สติ" "รู้ตัว" ในการใช้งานโปรแกรม "Social Network" อยู่ตลอดเวลา โดยการระมัดระวังไม่ป้อนข้อมูลที่ "Sensitive" หรือ ข้อมูลส่วนตัวเข้าสู่โปรแกรมดังกล่าว ก็สามารถใช้งาน Facebook หรือ Twitter ได้อย่างปลอดภัยและได้ประโยชน์จากการใช้โปรแกรม Social Network โดยไม่ต้องกังวลเรื่องความมั่นคงปลอดภัยโดยในปัจจุบันมีหลายมหาวิทยาลัยที่จัดให้มีการสอนวิชา "Social Network Marketing" โดยเรียนวิธีการท าการตลาดโดยผ่านทาง Social Network ซึ่งใช้ได้ผลมาแล้วในหลายองค์กร ดังนั้นสามารถใช้งานโปรแกรมประเภท Social Network ให้มีประโยชน์แก่องค์กรได้เช่นกัน

ไม่ว่าจะเป็น การคุกคามของแฮกเกอร์ผ่านทางใดก็แล้วแต่ ควรที่จะศึกษาเพื่อหาวิธีป้องกันอาชญากรรมที่อาจจะเกิดขึ้นกับตนเอง ดังนี้

**ปัจจัยที่ก่อให้เกิดภัยคุกคาม มาจากองค์ประกอบสำคัญในการกระทำความผิด Security in Social Networking**

- แรงจูงใจ
- ช่องโอกาส
- ทักษะ

**วิธีการเก็บรวบรวมพยานหลักฐาน**

| List | Method | Process | Note |
|---|---|---|---|
| 1 | Manual | Capture/Take Photo | Free |
| 2 | App Backup | Chat Backup/File Backup | Free |
| 3 | Logical Backup | Manufactory Backup | Free |
| 4 | Logical Extraction | Forensic Extraction | Commercial Tool/ Command Line |
| 5 | Physical Extraction | Forensic Extraction | Commercial Tool/ Command Line |

**ข้อควรระวังในการใช้โซเชียลมีเดีย**

- ระวังโปรไฟล์ปลอม
- การแบ่งปันและชื่อเสียงทางออนไลน์ของคุณ
- ใช้รหัสผ่านที่คาดเดายากที่แตกต่างกันสำหรับบัญชีโซเชียลแต่ละบัญชี (และการรับรองความถูกต้องแบบหลายปัจจัย หรือ Multi factor authentication)
- จัดการโปรไฟล์ของคุณและอัปเดตเป็นประจำ ทราบการตั้งค่าความปลอดภัยและความเป็นส่วนตัวของแต่ละแพลตฟอร์ม

# Gu. Digital: รับมืออย่างไร เมื่อเจอภัยในโลกออนไลน์

- ตระหนักถึงการหลอกลวง: การหลอกลวงบนโซเชียลมีเดียมี 5 ประเภทหลักๆ ได้แก่ การหลอกลวงเรื่องรักๆ ใคร่ๆ การหลอกลวงลอตเตอรี การหลอกลวงเงินกู้ การขโมยโทเค็นการเข้าถึง และ การหลอกลวงงาน
- สร้างโปรไฟล์ส่วนตัวหรือใช้นามแฝง
- ปิดการตั้งค่าตำแหน่งและ / หรือข้อมูลพื้นหลัง
- อย่าเปิดเผยข้อมูลการเข้าสู่ระบบของคุณ
- ตรวจสอบลิงค์ก่อนคลิก อ่านก่อนอนุญาตให้แอปเข้าถึงข้อมูลของคุณหรืออนุญาตเมื่อคุณใช้แอปเท่านั้น

**การใช้มือถือเพื่อความปลอดภัย**

- หลีกเลี่ยงการเข้าร่วมเครือข่าย Wi-Fi ที่ไม่รู้จัก
- ใช้ Multi-Factor Authentication (MFA)
- สำรองข้อมูลของคุณ
- หลีกเลี่ยงการเปิดไฟล์คลิกลิงก์หรือโทรเข้าหมายเลขจากข้อความที่ไม่ได้ร้องขอ
- เปลี่ยนชื่อผู้ใช้และรหัสผ่านเริ่มต้นที่ตั้งไว้จากโรงงาน
- ลบข้อมูลทั้งหมดที่จัดเก็บไว้ในอุปกรณ์ก่อนที่จะทิ้ง
- ปิดใช้งานคุณสมบัติที่ไม่ได้ใช้งานเช่น Bluetooth หรือ Wi-Fi
- เข้ารหัสข้อมูลที่ละเอียดอ่อนและเส้นทางการสื่อสารทั้งหมด
- เปิดใช้งานการล็อกหน้าจอโดยใช้รหัสผ่านที่คาดเดายากหรือหมายเลขประจำตัวส่วนบุคคล (PIN)
- ปฏิบัติตามนโยบาย บริษัท และแนวทางการจัดการข้อมูลของคุณ
- บำรุงรักษาซอฟต์แวร์และระบบปฏิบัติการที่ทันสมัย
- อย่าเปิดอุปกรณ์ของคุณทิ้งไว้โดยไม่มีใครดูแล
- ปิดอุปกรณ์ของคุณหรือวางไว้ในโหมดเครื่องบินก่อนจัดเก็บ
- ตั้งค่าอุปกรณ์ที่ใช้ Bluetooth เป็นไม่สามารถค้นพบได้
- ปิดการเชื่อมต่ออัตโนมัติเมื่อไม่ใช้งาน

**เว็บไซต์ที่เป็นประโยชน์**

- เว็บไซต์สำหรับตรวจสอบไวรัส ทั้งจากไฟล์ และจาก URL คือ “www.virustotal.com”
- เว็บไซต์สำหรับตรวจสอบที่อยู่จริงของ URL แบบย่อ คือ “https://longurl.info/?lang=en”
- เว็บไซต์สำหรับการตั้งค่า Multi factor authentication คือ “https://www.theverge.com/22215571/factor-authentication-2fa-apple-microsoft-google-how-to”

# Gu. Digital: รับมืออย่างไร เมื่อเจอภัยในโลกออนไลน์

- เว็บไซต์สำหรับมาตรฐานความปลอดภัย (NIST)
- เว็บไซต์สำหรับหน่วยงานที่รับผิดชอบเกี่ยวกับคดีทางเทคโนโลยี (ปอท.)
- เว็บไซต์ที่เกี่ยวข้องส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

**เอกสารอ้างอิง:**


- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.(2558).“เล่น Social Network ให้ปลอดภัย “รู้” ไว้เลี่ยงอันตราย”. [ออนไลน์]: https://www.etda.or.th/content/social-network-security.html
- ความปลอดภัยทางไซเบอร์ Cyber Security Fortinet NSE Training Institute “https://training.fortinet.com/”