6 กุมภาพันธ์ 2023

เขียนโดยคุณนาราซากิ ฝ่ายปฏิบัติการ

# การรับมือปัญหาของความมั่นคงปลอดภัยของข้อมูลสารสนเทศจากสมาร์ทโฟน

สวัสดีครับ ผม นาราซากิจากฝ่ายปฏิบัติการครับ

（提供：総務省）

วันนี้ผมอยากจะเขียนถึงเรื่องความปลอดภัยของข้อมูลสารสนเทศจากโทรศัพท์สมาร์ทโฟนที่ทุกท่านใช้กันอยู่ในปัจจุบันครับ ในปัจจุบันมีบริการต่างๆที่สามารถใช้บริการผ่านสมาร์ทโฟนได้นะครับ อย่างเช่น รูปทางขวาที่ผมยกมาให้ดู จะเห็นว่าสมาร์ทโฟนหนึ่งเครื่องนั้นเก็บข้อมูลของผู้ใช้ไว้มากมายเลยนะครับ ข้อมูลเหล่านี้จะถูกส่งต่อให้บริษัทที่ทำการตลาดหรือโฆษณา ไม่ว่าจะเป็นข้อมูลความสนใจหรืองานอดิเรกของผู้ใช้ หากข้อมูลส่วนตัวเหล่านี้ถูกนำไปใช้ในทางที่ผิดก็จะเกิดผลเสียตามมามากมาย จึงจำเป็นอย่างยิ่งที่จะต้องระมัดระวังให้มากครับ

รายการด้านล่างที่ผมยกมา คือเหตุการณ์ 10 อันดับของภัยจากการโจรกรรมข้อมูลสารสนเทศปี 2022 อันดับเหล่านี้ตัดสินจากความร้ายแรงของผลกระทบจากเหตุการณ์การโจรกรรมข้อมูลสารสนเทศที่เกิดในปี 2021 ซึ่งพิจารณาคัดเลือกโดยนักวิจัยด้านความปลอดภัยของข้อมูลสารสนเทศและผู้ปฏิบัติงานในบริษัทกว่า 150 คน ความเสียหายนั้นเกิดจากทั้งส่วนบุคคลและองค์กร แต่ในครั้งนี้จะขอยกมาเล่าสู่กันฟังเฉพาะหัวข้อส่วนบุคคล (แน่นอนว่าความเสียหายจากส่วนบุคคลก็กระทบถึงองค์กรด้วยเช่นกันนะครับ)

（ที่มา：IPA 10 อันดับภัยจากการโจรกรรมข้อมูลสารสนเทศปี 2022）

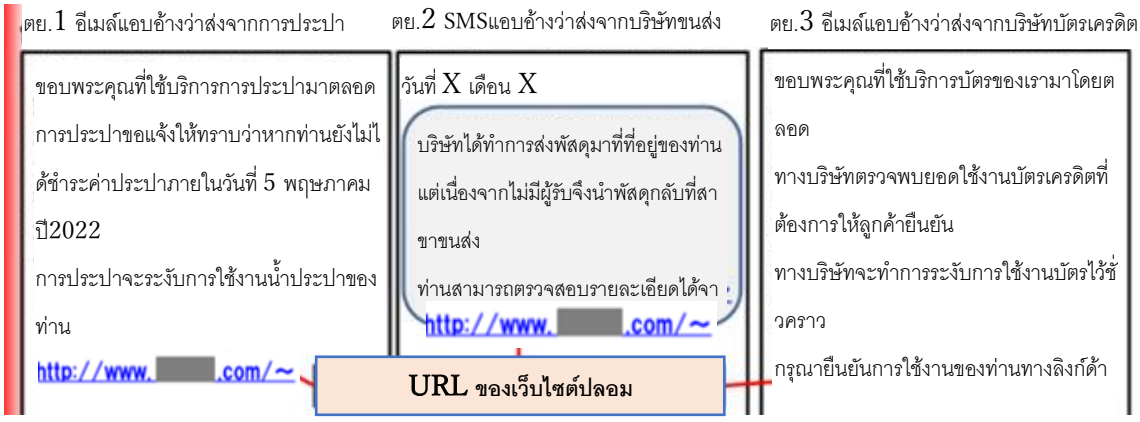
1. การโดนฟิชชิ่งหรือการถูกหลอกเอาข้อมูลส่วนตัวที่สำคัญไป
2. การว่าร้าย กล่าวคำหมิ่นประมาท นินทาใส่ร้าย ทางอินเตอร์เน็ต
3. การหลอกลวง ฉ้อโกงผ่านทางอีเมล์หรือ SMS
4. การฉ้อโกงโดยใช้ข้อมูลบัตรเดรดิต
5. การฉ้อโกงโดยใช้ข้อมูลการชำระเงินด้วยสมาร์ทโฟน
6. การฉ้อโกงโดยแจ้งเรื่องหรือแจ้งเตือนในเรื่องที่ไม่เป็นความจริง
7. ภัยจากการใช้แอปที่ไม่ปลอดภัย
8. การขโมยข้อมูลส่วนบุคคลผ่านทางบริการอินเตอร์เน็ต
9. การฉ้อโกงผ่านอินเตอร์เน็ตแบงค์กิ้ง
10. การถูกสวมรอยเข้าระบบผ่านบริการอินเตอร์เน็ต


ผู้ใช้สมาร์ทโฟนหลายท่าน เมื่อมีสิ่งอำนวยความสะดวกที่ทำให้สามารถใช้งานได้ง่าย ก็เป็นธรรมดาที่ความระมัดระวังจะต่ำลง เราจึงไม่ควรหละหลวม และระมัดระวังในการใช้งานอย่างปลอดภัย ไม่ให้เกิดความเสียหายเหมือนเช่นตัวอย่างสิบอันดับที่ยกมาให้ดูกันนะครับ

จากอันดับที่ยกมาข้างต้น ผมจะขอลงรายละเอียดอันดับที่ 「 1. การโดนฟิชชิ่ง, อันดับที่ 「5.การฉ้อโกงโดยใช้ข้อมูลการชำระเงินด้วยสมาร์ทโฟน และ อันดับที่ 「6.การฉ้อโกงโดยการแจ้งเรื่องเท็จ แจ้งเตือนเท็จ

1. การโดนฟิชชิ่งหรือการถูกหลอกเอาข้อมูลส่วนตัวที่สำคัญไป

การฟิชชิ่งในปัจจุบันนั้นมาในรูปแบบของหน่วยงานราชการ หรือหน่วยงานสาธารณะต่างๆ มาลองดูตัวอย่าง SMS หรืออีเมล์ด้านล่างกันนะครับ




⇒ก่อนอื่นสิ่งสำคัญคือให้สงสัยไว้ก่อนเลยว่าอีเมล์หรือ SMS ที่ได้รับนั้นเป็นของปลอมนะครับ

เมื่อได้รับอีเมล์หรือSMSเช่นนี้ ส่วนใหญ่เราจะรู้สึกตกใจ แม้ว่าข้อมูลที่แจ้งมาจะน่าเป็นห่วง แต่ก่อนอื่นขอให้ใจเย็นๆ สูดหายใจเข้าลึกๆให้มีสติก่อนนะครับ

5. การฉ้อโกงโดยใช้ข้อมูลการชำระเงินด้วยสมาร์ทโฟน

หากโดนยึดบัญชีที่ลงทะเบียนการชำระเงินผ่านระบบออนไลน์ต่าง ๆ (เช่น PayPay เป็นต้น) ผลที่จะเกิดตามมาคือมิจฉาชีพจะใช้เงินคงเหลือในบัญชีในการชำระค่าใช้จ่าย หรือมีการเก็บเงินไปที่บัญชีที่ลงทะเบียนไว้

▪ หากถูกนำ ID และรหัสผ่านไปใช้เพื่อเข้าระบบโดยพลการ

⇒ ป้องกันด้วยวิธีเดียวกับการฟิชชิ่ง

▪ ผู้ที่ ”ใช้รหัสผ่านซ้ำ ๆ กัน” เป็นเป้าหมายในการโจรกรรมข้อมูล

⇒ ▪ ไม่ใช้รหัสผ่านเดียวกันกับทุกบัญชีที่ใช้งาน

▪ ตั้งรหัสผ่านที่ยาวและมีความซับซ้อน

6. การฉ้อโกงโดยแจ้งเรื่องหรือแจ้งเตือนในเรื่องที่ไม่เป็นความจริง

ในระหว่างใช้งานอินเตอร์เน็ตจะมีข้อความหลอกลวงแจ้งเตือนเช่น「ตรวจพบไวรัสในคอมพิวเตอร์ของคุณ」เป็นต้น เพื่อให้ผู้ใช้ติดต่อหน่วยงานบริการลูกค้าที่เป็นหน่วยงานหลอกลวง มิจฉาชีพจะทำทีเป็นช่วยเหลือและแนะนำ จากนั้นก็ชักชวนให้ทำสัญญาการให้บริการที่ไม่จำเป็น หรือแนะนำซอฟแวร์ที่ไปก่อให้เกิดความเสียหายต่อทรัพย์สินของผู้ใช้

(ที่มา : IPA 10 อันดับภัยจากการโจรกรรมข้อมูลสารสนเทศปี 2022)


⇒ แม้จะได้รับการแจ้งเตือนที่ทำให้ท่านไม่สบายใจ แต่ก็อย่าเชื่อและปฏิบัติตามคำแนะนำในทันที การหลอกลวงนั้นมาในหลากหลายรูปแบบ ในกรณีที่ยังตัดสินไม่ได้ว่าเป็นเรื่องหริงหรือหลอกลวง อย่าทำตามที่ถูกแนะนำง่ายๆ ให้ปรึกษาคนที่ท่านไว้ใจก่อน

อย่างที่เกริ่นไปในตอนเริ่มบทความว่าการใช้งานสมาร์ทโฟนนั้นทำให้เข้าถึงการบริการออนไลน์ต่าง ๆ ได้
ในส่วนของทางบริษัทเราเองมีระบบควบคุมการเข้างาน（VGคลาวด์）、และมีการเริ่มให้สลิปเงินเดือนแบบดิจิตอลแล้ว
นอกจากนี้ทางเราเองก็มีแผนจะแนะนำระบบแชทที่ชื่อว่า elgana ด้วยครับ
（ ※ elgana เป็นระบบแชทของบริษัทในเครือของ NTT ซึ่งจะแตกต่างจาก LINE ตรงที่เป็นระบบแชทเพื่อการใช้งานในธุรกิจ รายละเอียดการใช้งานนั้นผมขออธิบายในโอกาสถัดไปนะครับ）

เราลองมาดูตารางด้านล่างที่ระบุวิธีพื้นฐานที่จะช่วยให้ใช้งานสมาร์ทโฟนได้อย่างปลอดภัยกันนะครับ
ทุกท่านสามารถนำไปประยุกต์ใช้ได้เลยครับ

| ปัจจัยที่ทำให้ถูกโจรกรรม | วิธีรับมือเบื้องต้น | วัตถุประสงค์ |
|---|---|---|
| ช่องโหว่ของซอฟแวร์ | เปลี่ยนซอฟแวร์ที่ใช้งาน | เพื่อลดความเสี่ยงที่จะถูกโจรกรรม |
| ช่องโหว่ของซอฟแวร์ | ติดตั้งโปรแกรมป้องกันไวรัส | บล็อคการโจรกรรมได้ |
| โดนขโมยรหัสผ่าน | ควบคุมรหัสและทำให้รหัสผ่านซับซ้อน | ลดความเสี่ยงการโจรกรรมรหัสผ่าน |
| การติดตั้งไม่ดี | ตรวจสอบการตั้งค่า | ป้องกันการติดตั้งผิดพลาด |
| ถูกชักจูงแบบต่าง ๆ | ติดตามข้อมูลการโจรกรรมรูปแบบต่าง ๆ | ทำให้รู้เท่าทันกลอุบายต่าง ๆ |

（ที่มา：IPA 10 อันดับภัยจากการโจรกรรมข้อมูลสารสนเทศปี 2022）

สุดท้ายนี้มาลองตอบคำถามกันนะครับ
ลองดูกันว่ารหัสผ่านด้านล่างข้อ１～４ รหัสผ่านในข้อใดเป็นรหัสผ่านที่ดีที่สุดนะครับ

1. 92674538
2. nR9Wj8vZ
3. m9Wu1f
4. w5ux8psf

⇒เฉลย 2
เนื่องจากมีการใช้ตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่ มีความยาวของรหัสผ่านมากกว่า 3 ตัวอักษร ในบรรดาตัวเลือกทั้งหมด นี่จึงเป็นตัวเลือกที่ดีที่สุดครับ (รหัสยิ่งยาวยิ่งดีนั่นเองครับ)
เราไม่ควรตั้งรหัสผ่านที่เดาได้ง่ายเกินไป เช่น 12345678 หรือ abcdefgh เพราะจะทำให้มิจฉาชีพเดารหัสได้ง่ายนะครับ