แนวทางการป้องกันภัยคุกคาม Smart phone ในยุคปัจจุบัน

ดลยา สุขปิติ*

ในช่วง 1-2 ปีที่ผ่านมา ได้มีภัยคุกคามทางอินเตอร์เน็ตในหลายทิศทางและมีหลากหลายรูปแบบ ทั้งๆที่มีการป้องกันแล้ว แต่ยังมีช่องโหว่ที่ทำให้เกิดปัญหาได้อีก เข้าสู่ปี 2013 ในปีนี้ ภัยคุกคามทางอินเตอร์เน็ตก็ยังคงมีมากขึ้นในการทำงานหรือในชีวิตประจำวัน เครื่องมือสื่อสารกลายเป็นส่วนที่สำคัญ การทำงานในกรมวิทยาศาสตร์บริการเกือบทุกหน่วยงานต้องใช้อุปกรณ์เหล่านี้ เพื่อติดต่อสื่อสาร ทำการประชาสัมพันธ์ เผยแพร่ข้อมูลความรู้ เป็นต้น ซึ่งปีที่ผ่านมาเทคนิคที่แฮคเกอร์ผู้ไม่หวังดีนิยมใช้เป็นช่องทางในการโจรกรรมข้อมูล ได้แก่ เทคนิค Pixsteal ที่ใช้เทคนิคการอัพโหลดรูป ที่แฝงมัลแวร์ (ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย) เอาไว้เข้าไปไว้บนเซิฟเวอร์ผ่านช่องทาง FTP, Passteal การสืบรหัสพาสเวิร์ดผ่าน Forget Password ตัวช่วยเหลือเวลาเราลืมพาสเวิร์ดต่างๆ และวิธีการสุดท้ายที่นิยมกันคือช่องโหว่ อย่าง Blackhole Explolit kit เครื่องมือที่จะทำการโจรกรรมข้อมูลโดยที่ผู้ใช้ไม่ทันได้รู้ตัว เพราะจะไม่มีการหลอกล่อหรือหลอกให้เรากดคลิกปุ่มใดๆ แต่จะแอบขโมยข้อมูลของเราไปโดยที่เราไม่รู้ตัว

สำหรับในปี 2013 ได้มีการคาดการณ์ว่า วิธีที่แฮคเกอร์ใช้ในปีที่ผ่านมา จะยังคงได้รับความนิยมในปีนี้ และขยายวงกว้างไปยังอุปกรณ์ต่างๆ มากกว่าเดิม ไม่ได้จำกัดวงอยู่แค่ในคอมพิวเตอร์เป็นหลัก แต่สมาร์ทโฟนและแท็บเล็ต จะเป็นเป้าหมายใหม่ที่สำคัญ เพื่อที่จะรักษาและถนอมเครื่องมือสื่อสารต่างๆไว้ จึงควรมีหลักการและแนวทางในการป้องกัน และ รับมือกับภัยคุกคามเหล่านี้

หลักในการป้องกันตัวเองเบื้องต้น

1. ติดตามข่าวสารความเคลื่อนไหวของไวรัสอย่างสม่ำเสมอ

2. ระมัดระวังตัวในการดาวน์โหลดไฟล์จากเว็บไซต์ต่างๆ ที่ไม่คุ้นเคย และสแกนไวรัสไฟล์ที่ดาวน์โหลดมาก่อนทำการเปิดทุกครั้งให้เป็นประจำเสมอ

3. ตรวจสอบลิงค์ต่างๆ ก่อนที่จะคลิกทุกครั้ง โดยเฉพาะพวกลิงค์ที่มีคำว่า คลิกแล้วได้เงิน เพราะอะไรที่ได้มาโดยไม่มีค่าใช้จ่าย เป็นไปได้ยาก ไม่ควรเชื่อถือ

4. ศึกษาเรื่อง How Social Engineering works เทคนิคการล้วงข้อมูลโดยที่เราไม่รู้ตัว เอาไว้เบื้องต้น

ปี 2012 เป็นปีทองของมัลแวร์ที่มากับแอพพลิเคชั่นในสมาร์ทโฟน และปีนี้ก็ยังจะเป็นปีทองต่อไป วิธีการที่แฮกเกอร์ใช้มีตั้งแต่แอพพลิเคชั่นปลอมที่ทำเลียนแบบแอพพลิเคชั่นจริง แอพพลิเคชั่นที่ทำมาแล้วขอสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้ ซึ่งหากผู้ใช้ไม่อ่านข้อตกลงการใช้แอพพลิเคชั่นให้ดีก่อน ก็มีสิทธิ์ถูกล้วงข้อมูลได้ง่ายๆ

สมาร์ทโฟนจะมีทั้งเบอร์โทรศัพท์และรูปถ่าย บางคนมีการจดบันทึกและพาสเวิร์ดที่สำคัญเอาไว้มากมาย และแอพพลิเคชั่นบนสมาร์ทโฟนสามารถเข้าถึงข้อมูลเหล่านั้นได้อย่างง่ายดาย ดังนั้นก่อนจะติดตั้งแอพพลิเคชั่นใดๆ ก็ตาม เราควรตรวจสอบให้รอบคอบ

*นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักพัฒนาศักยภาพนักวิทยาศาสตร์ห้องปฏิบัติการ

แนวทางในการดาวน์โหลดแอพพลิเคชั่นบนสมาร์ทโฟน

1. ควรดาวน์โหลดแอพพลิเคชั่นจากผู้พัฒนาโดยตรง ไม่ควรดาวน์โหลดผ่านลิงค์ที่ได้จากการใช้ search engine (โปรแกรมค้นหา และคือ โปรแกรมที่ช่วยในการสืบค้นหาข้อมูล โดยเฉพาะข้อมูลบนอินเทอร์เน็ต โดยครอบคลุมทั้งข้อความ รูปภาพ ภาพเคลื่อนไหว)

2. หลีกเลี่ยงแอพพลิเคชั่นที่มีการขออนุญาต Permissions มากเกินความจำเป็น

3. ถ้าเป็นไปได้อย่าใช้แอพพลิเคชั่นที่มีโฆษณาให้เรากดเปิดบราวเซอร์ โดยมากมักจะมาพร้อมกับแอพพลิเคชั่นฯ ฟรี ซึ่งอาจจะแสดงลิงค์พาเราไปยัง website อันตรายได้

4. ศึกษาข้อมูลของแอพพลิเคชั่นบน Android

4.1 การตั้ง Password ให้เครื่อง มีประโยชน์อย่างมาก ในกรณีที่หากเราเผลอวางโทรศัพท์ทิ้งไว้ และมีผู้ไม่ประสงค์ดีแอบหยิบไปกดดูข้อมูลสำคัญ/ส่วนตัวของเราได้

4.2 หลีกเลี่ยงการติดตั้ง แอพพลิเคชั่นที่มาจาก Unknown Sources โดยไม่จำเป็น และก่อนจะติดตั้งแอพพลิเคชั่นทุกครั้ง ควรตรวจสอบและอ่านความเห็นของแอพพลิเคชั่นจากผู้ใช้ก่อน อาจจะมีคำเตือนที่มีประโยชน์อยู่ในนั้น

4.3 หลีกเลี่ยงการใช้ Wi-Fi สาธารณะโดยไม่จำเป็น เพราะมันไม่มีระบบรักษาความปลอดภัยแม้แต่น้อย Hacker สามารถเข้าถึงผู้ใช้งานในกลุ่ม Wi-Fi เดียวกันเพื่อเข้ามาขโมยข้อมูลได้อย่างง่ายดาย

4.4 อ่านคำขออนุญาตของแอพพลิเคชั่นให้ดีว่าต้องการเข้าถึงข้อมูลของเราในส่วนไหนบ้าง ถ้าพบอะไรน่าสงสัยไม่น่าจะเกี่ยวกับการทำงาน ก็อย่าติดตั้งลงไป

4.5 ตอนนี้มีโปรแกรมแอนตี้ไวรัส สำหรับ Android แล้ว เช่น Trend Micro (บริษัทผลิต software) Mobile Security for Android ที่สามารถสแกนแอพพลิเคชั่นในเครื่องได้ว่ามีตัวไหนที่มีแอบแฝงการทำงานที่ไม่ปลอดภัย รวมถึงการป้องกันขณะเล่นเว็บผ่านมือถืออีกด้วย

จากการสำรวจข้อมูลพบว่า โดยเฉลี่ยผู้ใช้อินเตอร์เน็ตหนึ่งรายจะมีบัญชีอินเตอร์เน็ตตามเว็บไซต์ต่างๆ เฉลี่ยประมาณ 10 บัญชีต่อผู้ใช้หนึ่งราย ซึ่งบัญชีเหล่านี้จะมีข้อมูลส่วนตัวอยู่มากมาย ถูกบันทึกไว้บนเซิฟเวอร์ และหากมีการใช้งานผ่านสมาร์ทโฟน มันก็เหมือนมีการใช้งานบัญชีมากขึ้นเป็นสองเท่า ปัญหาก็คือเมื่อเวลาผ่านไปมักจะมีบัญชีหลายบัญชีที่อาจจะไม่ได้เข้าไปใช้งานอีกแล้วจนลืมมันไป แต่ว่าข้อมูลของเราจะยังอยู่ตลอดไปบนเซิฟเวอร์ ซึ่งแน่นอนว่าไม่ใช่เรื่องดีแน่ๆ ที่ข้อมูลของจะถูกเก็บเอาไว้แบบนั้นบัญชีการใช้งานอาจจะเป็นบัญชีเข้าใช้เว็บไซต์, โปรแกรม หรือแอพพลิเคชั่นต่างๆ ซึ่ง

มีข้อแนะนำดังนี้

1. หากเป็นแอพพลิเคชั่นที่เลิกใช้งานแล้ว ควรลบทิ้งและทำการปิดไอดี

2. หลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัวบนพื้นที่สาธารณะ หากจำเป็นต้องดำเนินการลงบนพื้นที่สาธารณะอย่าลืมมาลบทิ้งหลังจากเสร็จดำเนินการ

3. ตั้งค่าการเข้าถึงข้อมูล พยายามเปิดเผยข้อมูลให้น้อยที่สุดเท่าทีทำได้

ในการรักษาความปลอดภัย นอกจากระวังด้วยตัวเราเองแล้ว ทางที่ดีเราควรหาโปรแกรมรักษาความปลอดภัยเข้ามาช่วยดูแล ซึ่งไม่ใช่แค่ในคอมพิวเตอร์เท่านั้น เดี๋ยวนี้สมาร์ทโฟนก็จำเป็นต้องติดตั้งโปรแกรมแอนตี้ไวรัสเช่นเดียวกัน ซึ่งจะช่วยในการตรวจสอบความปลอดภัยให้เราและดูแลการทำงานของแอพพลิเคชั่นที่มีการทำงานที่เป็นอันตรายให้สมาร์ทโฟนของเราด้วย

หลักการเลือกโปรแกรมหรือแอพพลิเคชั่นแอนตี้ไวรัส

1. เลือกที่สามารถอัพเดตฐานข้อมูลไวรัสได้อัตโนมัติและไม่มีค่าใช้จ่าย

2. ในการซื้ออุปกรณ์ใหม่ อย่าลืมถามถึงโปรแกรมรักษาความปลอดภัยที่มีมาให้

3. เตือนคนรอบข้างให้ตระหนักถึงความปลอดภัย

ที่สุดแล้วสิ่งสำคัญของการรักษาเข้ามาใช้ความปลอดภัยคือต้องใช้อินเตอร์เน็ตอย่างมีสติและไม่ประมาท อย่าได้เห็นว่า ไม่เสียค่าใช้จ่ายแล้วไปคลิกลิงค์ต่างๆ และโปรแกรมแอนตี้ไวรัสก็เป็นอีกสิ่งที่อุปกรณ์ที่มีการเชื่อมต่ออินเตอร์เน็ตขาดไม่ได้ ไม่ว่าจะเป็นคอมพิวเตอร์หรือสมาร์ทโฟน เพื่อการใช้งานให้มีประสิทธิภาพ และดำเนินไปสู่เป้าหมายให้เกิดประโยชน์สูงสุด

เอกสารอ้างอิง

A Trendlabs digital life e-guide: A guide to 2013 new year's resolutions. **[online]** [cite dated 14 January 2013]. Available from internet: http://about-threats.trendmicro.com/ebooks/a-guide-to-2013-new-years-resolutions/#/1/.