เทรนด์ไมโคร เตือนภัย ‘ฟิชชิ่งมือถือ’ พร้อมโจมตีอุปกรณ์พกพาที่หลากหลาย

บริษัท เทรนด์ไมโคร อินคอร์ปอเรท (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านการรักษาความปลอดภัยข้อมูลดิจิทัลสำหรับผู้บริโภค เปิดเผยรายงานล่าสุดจากศูนย์วิจัยเทรนด์แล็บส์เกี่ยวกับฟิชชิ่งมือถือ โดยจากการสังเกตพฤติกรรมของไซต์ฟิชชิ่งในช่วงปี 2555 พบว่ามี URL ฟิชชิ่งมากกว่า 4,000 รายการที่ถูกออกแบบมาในรูปของเว็บมือถือโดยเฉพาะ ซึ่งหมายความว่าอุปกรณ์มือถือ รวมถึงสมาร์ทโฟนและแท็บเล็ต กำลังตกเป็นเป้าหมายของการโจมตีแบบฟิชชิ่งอย่างชัดเจน

จากการวิจัยล่าสุดพบว่า 4 ใน 5 ของผู้ใช้ในประเทศสหรัฐอเมริกาสั่งซื้อสินค้าออนไลน์ผ่านทางสมาร์ทโฟน และ 52% ของผู้ใช้เรียกดูเว็บไซต์ผ่านทางอุปกรณ์พกพาต่างๆ ขณะที่ 39% เข้าเยี่ยมชมไซต์เครือข่ายสังคมออนไลน์หรือบล็อกเป็นประจำ

นายพอล โอลิเวอเรีย นักวิจัยเทรนด์แล็บส์ กล่าวว่า “ผู้ใช้กำลังค่อยๆ เปลี่ยนแปลงพฤติกรรมเกี่ยวกับการใช้อุปกรณ์มือถือของตน เนื่องจากความสะดวกสบายและความมีประสิทธิภาพของสมาร์ทโฟนและแท็บเล็ต ขณะเดียวกัน อาชญากรไซเบอร์ก็กำลังใช้ประโยชน์จากแนวโน้มของผู้บริโภคดังกล่าวผ่านทางเว็บไซต์ฟิชชิ่ง ซึ่งเป็นไซต์หลอกลวงที่มีลักษณะเหมือนกับเว็บไซต์ปกติทั่วไป เพื่อล่อลวงให้ผู้ใช้เปิดเผยข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน และรายละเอียดเกี่ยวกับบัญชีต่างๆ

นอกจากนี้ บริษัทเทรนด์ไมโครยังพบว่าในปี 2555 URL ฟิชชิ่งมือถือในสัดส่วนถึง 75% เป็น เว็บไซต์ลวงที่ปลอมแปลงมาจากเว็บไซต์ผู้ให้บริการทางการเงินและการธนาคารที่มีชื่อเสียง เช่น Barclays ขณะที่เว็บไซต์อีคอมเมิร์ซและเว็บไซต์ชอปปิ้งออนไลน์ ซึ่งรวมถึงผู้ให้บริการชั้นนำ อย่าง PayPal และ eBay ก็มีจำนวนถึง 4% และเมื่อผู้ใช้ถูกลวงให้เปิดเผยข้อมูลประจำตัวในการล็อกอินเข้าสู่เว็บไซต์เหล่านั้น อาชญากรไซเบอร์ก็จะสามารถใช้ข้อมูลที่ขโมยมาดังกล่าวดำเนินธุรกรรมที่ไม่ได้รับอนุญาตและสั่งซื้อสินค้าต่างๆ ผ่านทางบัญชีของเหยื่อได้

นายพอลกล่าวเพิ่มเติมว่า “แนวโน้มของการเปิดฉากโจมตีแบบฟิชชิ่งที่เพิ่มสูงขึ้นบนโทรศัพท์มือถือ เป็นผลมาจากข้อจำกัดบางอย่างของตัวแพลตฟอร์มมือถือเอง โดยหน้าจอที่มีขนาดเล็กของอุปกรณ์ มือถือส่วนใหญ่ทำให้ผู้ใช้ไม่สามารถดำเนินการตรวจสอบเว็บไซต์เพื่อค้นหาองค์ประกอบของความปลอดภัยด้านการป้องกันฟิชชิ่งได้อย่างเต็มที่ นอกจากนี้ อุปกรณ์มือถือส่วนใหญ่มักจะใช้เบราว์เซอร์แบบที่มีการตั้งค่าล่วงหน้าไว้ให้แล้ว (ดีฟอลต์) ดังนั้นจึงทำให้เป็นเรื่องง่ายยิ่งขึ้นสำหรับอาชญากรไซเบอร์ที่จะสร้างรูปแบบการโจมตีที่ตนต้องการด้วยการมุ่งเน้นไปที่เบราว์เซอร์

ใดเบราวเซอร์หนึ่งแทนที่จะเป็นหลายเบราว์เซอร์”

อีกเหตุผลหนึ่งที่ทำให้แนวโน้มของฟิชชิ่งมือถือเพิ่มจำนวนขึ้น ก็คือการรับรู้ของผู้ใช้ ซึ่งจะเห็นได้ว่าผู้ใช้อุปกรณ์มือถือจะต้องเข้าใจว่าสมาร์ทโฟนและอุปกรณ์มือถืออื่นๆ มีขีดความสามารถเหมือนกับเครื่องเดสก์ทอปและจำเป็นที่จะต้องได้รับการคุ้มครองเช่นเดียวกัน อุปกรณ์เหล่านี้ควรจะถูกใช้งานอย่างระมัด ระวังและปลอดภัย มิฉะนั้นผู้ใช้อุปกรณ์มือถือก็อาจจะต้องพบกับภัยคุกคามในแบบเดียวกับที่ผู้ใช้พีซีประสบมาแล้ว

บริษัท เทรนด์ไมโคร มีแนวทางการป้องกันภัยคุกคามที่จะช่วยให้ผู้ใช้สามารถปกป้องตัวเองได้

l เลือกใช้เฉพาะแอพพลิเคชั่นที่เป็นทางการเท่านั้น โดยสามารถค้นหาแอพพลิเคชั่นที่เป็นทางการของเว็บไซต์ชอปปิ้งหรือธนาคารออนไลน์ได้บนเว็บไซต์ทางการของผู้ให้บริการนั้นๆ แล้วจึงทำการ ดาวน์โหลด สิ่งนี้จะช่วยให้การลวงเอาข้อมูลของคุณจากอาชญากรไซเบอร์เป็นเรื่องยากขึ้น

l หลีกเลี่ยงการคลิกลิงก์หรือเปิดสิ่งที่แนบมาในอีเมลจากผู้ส่งที่น่าสงสัย โดยลิงก์และไฟล์ที่แนบมานั้นอาจเป็นอันตรายได้

l ตรวจสอบเว็บเพจและ URL ของเว็บเพจให้แน่ใจ โดยจะต้องมีอีเมลยืนยันที่ขอให้ผู้ใช้ทำการยืนยันอีเมลที่ได้รับ แต่ก็มักจะเป็นรูปแบบที่อีเมลฟิชชิ่งใช้เช่นกัน

l แตะแถบที่อยู่ของเบราเซอร์เพื่อให้แสดงที่อยู่เว็บไซต์แบบเต็ม จากนั้นตรวจดูข้อผิดพลาดในการพิมพ์หรืออักขระที่อาจถูกเพิ่มเข้ามาในที่อยู่เว็บไซต์นั้นๆ

l บุ๊คมาร์กเว็บไซต์ที่เข้าเยี่ยมชมเป็นประจำ ซึ่งจะช่วยลดโอกาสในการถูกนำไปยังเว็บไซต์ฟิชชิ่งอันเนื่องมาจากการข้อผิดพลาดในการสะกดชื่อเว็บผิด

l ใช้โซลูชั่นรักษาความปลอดภัยสำหรับอุปกรณ์มือถือ โดยโซลูชั่นเทรนด์ไมโคร โมบาย ซิเคียวริตี้ (Trend Micro™ Mobile Security) จะช่วยรักษาความปลอดภัยให้กับอุปกรณ์มือถือและข้อมูลในอุปกรณ์ดังกล่าว ด้วยการระบุและสกัดกั้นภัยคุกคามแบบฟิชชิ่ง รวมถึงภัยคุกตามบนเว็บอื่นๆ เช่น URL และแอพพลิเคชั่นที่มีความเสี่ยงสูงหรือเป็นอันตราย