

ระว่าง 10 ภัยอันตราย

บนโลก

ออนไลน์ปี'54

ใกล้ตัวมากกว่าที่คิด!



[ต่อต้านแฮก]

เนื่องจากการใช้อินเทอร์เน็ต และการใช้เวลาอยู่บนโลกออนไลน์ ในปัจจุบันมีอัตราการเติบโตสูงขึ้นอย่างก้าวกระโดด ตัวอย่างที่เห็นได้ชัดคือ คนไทยได้มีการอ่านข่าวสารผ่านเว็บไซต์เพิ่มมากขึ้น มีการใช้อินเทอร์เน็ตในการสืบค้นข้อมูล หรือแม้แต่การใช้โทรศัพท์เคลื่อนที่ในการเชื่อมต่ออินเทอร์เน็ตก็มีสัดส่วนที่สูงขึ้น

แต่อย่างไรก็ตาม ปัญหาที่ตามมาจากราคาใช้อินเทอร์เน็ตได้เพิ่มมากขึ้นเรื่อยๆ คือ ความปลอดภัยของผู้ใช้อินเทอร์เน็ต

จะเห็นได้ว่าประเด็นเรื่องการป้องกันและแก้ไขปัญหาคาการหลอกลวงบนอินเทอร์เน็ตและอาชญากรรมทางอิเล็กทรอนิกส์เป็นปัญหาที่ผู้ใช้อินเทอร์เน็ตพบอยู่บ่อยๆ มีจรรยาวัที่ได้หาวิธีที่แยบยลมากขึ้น เพื่อใช้เป็นกลลวงและหลอกล่อเหยื่อให้หลงเชื่อ เช่น การส่งอี-เมลที่เป็นอี-เมลปลอม (สแปม) หรือการหลอกล่อให้กรอกข้อมูลส่วนตัวลงแบบฟอร์ม

สิ่งเหล่านี้ก่อให้เกิดผลประโยชน์ทางการเงินแก่เหล่ามิจฉาชีพ หมขอสรูป 10 วายร้ายบนโลกออนไลน์ที่จะเกิดขึ้นปี'54 ดังนี้

อันดับที่ 10

ปัญหาใหญ่บนโลกออนไลน์เองอาจจะไม่เกิดจากปัญหาของอินเทอร์เน็ตหรือปัญหาทางด้านเทคนิค แต่เป็นปัญหาที่เกิดขึ้นจากผู้ใช้เอง ซึ่งผู้ใช้มีแนวโน้มที่จะผูกตัวเองเข้ากับโลกออนไลน์มากขึ้นโดยไม่รู้ตัว เริ่มมีการใช้ชีวิตและสังคมบนโลกออนไลน์ ไม่ว่าจะเป็นการช้อปปิ้ง การพูดคุย พบปะสังสรรค์กับเพื่อนๆ บนโลกออนไลน์ซึ่งสิ่งเหล่านี้ได้เปลี่ยนวิถีการดำเนินชีวิตของผู้คนไป เสมือนเป็นการตัดขาดชีวิตจากโลกภายนอก ลิขวิถีการใช้ชีวิตจริงๆ ไป ซึ่งมีวิัจัยจากหลายหน่วยงานได้สรุปผลออกมาว่าคนในปัจจุบันมีแนวโน้มที่จะมีเพื่อนและพูดคุยกับคนไม่รู้จักบนโลกออนไลน์มากขึ้น และมีความสุขกับการสร้างตัวเองใหม่ ที่เป็นตัวละครบนโลกออนไลน์ เนื่องจากเราจะเป็นใครก็ได้บนโลกออนไลน์ แต่สิ่งนี้กลับทำให้เป็นการตัดขาดจากโลกภายนอกโดยสิ้นเชิง

อันดับที่ 9

จะไม่มี ความลับบนโลกนี้อีกต่อไป โลกของความปลอดภัยนั้นหาได้ยากบนโลกออนไลน์ ข้อมูลต่างๆ ถูกโอนถ่ายจากเว็บหนึ่งสู่อีเว็บหนึ่งทั้งที่เจ้าของข้อมูลรู้ตัวและไม่รู้ตัว การเข้าถึงข้อมูลส่วนบุคคลสามารถทำได้ง่ายขึ้นไม่ว่าจะเป็นการหาชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ข้อมูลเหล่านี้ง่ายต่อการถูกเปิดเผย การที่สมัครเพื่อเป็นสมาชิกเว็บไซต์หนึ่งเว็บไซต์ บัญชีอี-เมลหนึ่งอี-เมล มีข้อมูลส่วนตัวที่จำเป็นที่จะต้องให้ และใครจะรู้ว่าข้อมูลเหล่านั้นจะถูกเก็บหรือถูกส่งต่อไปยังที่ใดต่อไป

โดยเฉพาะในปัจจุบันโลกของสังคมออนไลน์ (Social Network) ได้ถือว่าเป็นฐานข้อมูลอย่างดีให้กับองค์กรธุรกิจมากมายเพื่อหาผลประโยชน์ในการใช้เป็นฐานข้อมูลลูกค้า

อันดับที่ 8

ในยุคนี้ ภัยธรรมชาติที่เกิดขึ้นบนโลกเราทุกวันนี้มีมากมายเหลือเกิน ซึ่งผู้ประสบภัยต่างๆ ทั่วทุกมุมโลก ต่างได้รับผลกระทบไม่น้อย มีองค์กรทั้งภาครัฐ เอกชน องค์กรอิสระที่ไม่หวังผลกำไรคอยช่วยเหลือและสนับสนุนผู้ประสบภัยธรรมชาติต่างๆ ซึ่งเหล่าอาชญากรไซเบอร์ก็ไม่เว้นที่จะใช้ประโยชน์จากน้ำใจของมวลมนุษยมาเป็นเหยื่อ มีการเกิดขึ้นของเว็บไซต์มากมายที่เป็นเว็บไซต์การ

กุศลจอมปลอมที่สร้างขึ้นเพื่อให้ประชาชนผู้ใจบุญ ที่มีความประสงค์ต้องการช่วยเหลือเพื่อนมนุษย์ที่ได้รับความลำบากทำการบริจาคเงินไปยังองค์กรที่หลอกล่อต้มตุ๋นดังกล่าว

อันดับที่ 7

หลายๆ คนในยุคไซเบอร์นี้นิยมที่จะส่งบัตรอวยพรไปให้เพื่อนๆ ผ่านทางอี-เมล หรือทางบัตรอวยพรอิเล็กทรอนิกส์ (E-Card)

ดังนั้น เหล่าอาชญากรไซเบอร์

จึงอาศัยช่องทางนี้ในการหลอกลวงและเข้าถึงข้อมูลของเหยื่อ อาชญากรไซเบอร์จะใช้วิธีการส่งบัตรอวยพรเทศกาลปลอม (Spam E-Card) ที่แฝงด้วยลิงก์ที่เป็นสแปม (Spam) มาให้เหยื่อทางอี-เมล อาจจะถูกส่งมาจากอี-เมลของอาชญากรไซเบอร์เอง หรือจากเพื่อนของเหยื่อที่อี-เมลนั้นได้ถูกแฮ็ก (Hack) เข้าไปในบัญชีรายชื่อเรียบร้อยแล้ว และทำการส่งต่อไปยังเพื่อนๆ

เมื่อเหยื่อได้รับอี-เมล และเปิดอ่าน จะมีลิงก์ให้เหยื่อทำการกด (Click) เพื่อทำการเปิดบัตรอวยพรอิเล็กทรอนิกส์ดังกล่าว แต่เบื้องหลังแล้วเป็นการทำการสั่งให้สแปมทำงาน

และนั่นทำให้เครื่องคอมพิวเตอร์ของเหยื่อตกอยู่ในอันตราย ทำให้อาชญากรไซเบอร์สามารถเข้าไปดูข้อมูลในคอมพิวเตอร์ของเหยื่อได้ หรือทำให้สามารถดึงข้อมูลรายชื่ออี-เมลของเพื่อนๆ ได้ต่อไป

อันดับที่ 6

โฆษณาแฝงด้วยไวรัส (Malware) สังเกตได้ว่าเว็บไซต์ทุกวันนี้อยู่ได้ด้วย 2 ประการ คือ

หนึ่งการที่มีคนเข้าจำนวนมากๆ โดยเฉพาะผู้ที่เข้าเว็บไซต์เป็นประจำ (unique Visitors)

และ สองคือโฆษณาที่ถือว่าเป็นแหล่งรายได้และทำเงินให้กับเว็บไซต์ต่างๆ อยู่มากได้ ดังนั้น การที่จะมีโฆษณานบนเว็บหรือมีธุรกิจที่สนใจในการลงโฆษณานบนเว็บไว้ได้นั้น ต้องอาศัยตัวแปรที่หนึ่งคือ มีคนเข้าเว็บไซต์จำนวนมากพอสมควรที่จะดึงดูดให้ธุรกิจมาโฆษณากับทางเว็บไซต์ในปัจจุบันเว็บไซต์ที่มีโฆษณาจึงไม่ใช่เรื่องแปลกตาเฉกเช่นกับในอดีต

ดังนั้น อาชญากรไซเบอร์จึงฉวยโอกาสที่ผู้เข้าเว็บไซต์ไม่ทันได้ระวังทำการเผยแพร่โฆษณาที่แฝงด้วยไวรัส เมื่อผู้เป็นเหยื่อทำการคลิกที่โฆษณานั้นแล้ว ตัวไวรัสจะถูกทำงานและฝังตัวอยู่ในเครื่อง

ทำให้เมื่อ

เหยื่อเข้าเว็บไซต์ใดก็ตาม

จะเกิดหน้าต่างเด้งขึ้นมาอย่างต่อเนื่อง ทำให้เกิดความรำคาญของผู้ใช้งาน ซึ่งผู้ใช้งานเองอาจมีความเข้าใจว่า มีโปรแกรมป้องกันไวรัสแล้วสามารถยับยั้งได้

แต่ปัญหาใหญ่คือ โปรแกรมแอนตี้ไวรัสรุ่นเก่าไม่สามารถตรวจพบสไปยาแวร์ได้ ทำให้ต้องใช้โปรแกรมประเภทแอนตี้สไปยาแวร์เพิ่มเติม

อันดับที่ 5

อันตรายจากการใช้โปรแกรมแชต (Instant Messaging) เช่น MSN เหล่าอาชญากรไซเบอร์หาช่องทางในการเจาะและแพร่ไวรัสหรือมัลแวร์ผ่านทางโปรแกรมแชตที่ได้รับความนิยมสูงอย่างต่อเนื่อง

ลักษณะการทำงานคือ เมื่อท่านใช้งานในโปรแกรมแชตกับเพื่อนของท่าน ท่านอาจจะได้รับข้อความให้รับไฟล์ที่ชื่อว่า Image.zip

จากเพื่อนของท่าน ถ้าท่านเผด็จศึกไปแล้ว โปรแกรมไวรัสจะถูกทำงานและทำให้รายชื่อของเพื่อนของท่านถูกลบออกไปหมด และยังเป็นการส่งโปรแกรมไวรัสดังกล่าวไปให้เพื่อนของท่านโดยที่ท่านไม่รู้ตัว

อันดับที่ 4

ภัยจากการโหลดไฟล์ผ่านทางอินเทอร์เน็ต (Bit Torrent) อะไรก็ตามที่มีผู้ใช้จำนวนมาก เป็นที่นิยม จะเป็นช่องที่พวกอาชญากรไซเบอร์ให้ความสนใจ เช่น โปรแกรมที่เหล่านักดาวน์โหลดไฟล์ขนาดใหญ่ ไม่ว่าจะเป็นหนัง หรือโปรแกรมใหญ่ ต่างใช้กันคือ Bit Torrent ที่ถูกออกแบบมาให้มีความสามารถทั้งการดาวน์โหลดและอัปโหลดไฟล์ขนาดใหญ่ๆ ด้วยความเร็วสูง แถมยังสามารถหาไฟล์ที่ต้องการได้อย่างง่ายดาย

เหล่าอาชญากรไซเบอร์จึงทำการปล่อยไฟล์ที่ได้รับความนิยมพร้อมกับการแฝงตัวไวรัสและมัลแวร์มายังเครื่องของเหยื่อผ่านการดาวน์โหลด และทำการส่งต่อไปยังเหยื่อรายต่อไปในขณะที่เหยื่อทำการอัปโหลด ผลกระทบที่เกิดขึ้นเครื่องคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ในองค์กรจะทำงานได้ไม่เต็มประสิทธิภาพ มีความเร็วลดลง และเป็นการเปิดช่องว่างทำให้เหล่าแฮกเกอร์ใช้ในการเจาะเข้าระบบขององค์กรต่อไป

อันดับที่ 3

ภัยจากเว็บไซต์ปลอม (Phishing) ลักษณะของเว็บปลอมนั้น อาชญากรไซเบอร์จะทำการส่งอี-เมลไปยังเหยื่อ โดยอาจจะใช้ที่อยู่และอี-เมลของธนาคาร เมื่อเหยื่อทำการคลิกเข้าไปแล้ว หน้าตาใหม่จะถูกเปิดขึ้น โดยหน้าตาเว็บไซต์ปลอมนั้นจะมีลักษณะเหมือนกับหน้าเว็บไซต์จริงๆ ของธนาคาร และจะมีข้อความแจ้งในทำนองว่า ให้เหยื่อทำการอัปเดตข้อมูลส่วนตัว เพื่อปรับปรุงและสามารถเข้าใช้งานได้ต่อไป เมื่อเหยื่อกรอกข้อมูลแล้ว กดยืนยัน ข้อมูลที่เหยื่อกรอกกับถูกส่งไปที่อาชญากรไซเบอร์ แทนที่จะไปที่เว็บไซต์ของธนาคาร เว็บไซต์ประเภทนี้ยังคงเป็นช่องทางหลักของเหล่าอาชญากรไซเบอร์ที่ใช้ในการหลอกเหยื่อให้หลงกล

ทำให้เหยื่อหลงเชื่อทำการกรอกข้อมูลส่วนตัว รหัสต่างๆ ซึ่งทำให้อาชญากรไซเบอร์เหล่านั้นสามารถนำข้อมูลของเหยื่อไปใช้ประโยชน์ต่อไป

อันดับที่ 2

Wi-Fi ปลอม มีลักษณะเดียวกันกับเว็บไซต์ปลอม (Phishing) แม้ว่าหลักการยังคงเหมือนเดิมแต่รูปแบบของการใช้เว็บปลอมก็ได้มีการพัฒนาให้มีความแยบยลมากขึ้น เช่น การที่เหยื่อเข้าไปนั่งในร้านกาแฟร้านหนึ่ง และค้นหาสัญญาณอินเทอร์เน็ตไร้สาย (โดยเฉพาะที่ฟรี) ซึ่งอาชญากรไซเบอร์รู้ถึงพฤติกรรมนี้ดี ว่าเมื่อคนเราเจอสัญญาณฟรีในที่สาธารณะ เรามักจะลองเข้าเพื่อใช้งาน ซึ่งอาชญากรไซเบอร์ก็ได้เตรียมเว็บไซต์ปลอมสำหรับการให้บริการอินเทอร์เน็ตฟรีขึ้น โดยเมื่อเหยื่อได้ทำการเชื่อมต่อสัญญาณ จะมีหน้าต่างปรากฏในลักษณะที่แจ้งถึงเงื่อนไขการใช้บริการฟรีอินเทอร์เน็ต เพียงแต่ให้เหยื่อกรอกข้อมูลก็สามารถเข้าใช้งานอินเทอร์เน็ตฟรี อาจจะเป็นเพียงการกรอกข้อมูล อี-เมล และตั้งพาสเวิร์ดสำหรับการใช้งาน แต่โดยปกติคนเราก็มักจะใช้พาสเวิร์ดซ้ำๆ กันอยู่แล้ว ทำให้เหล่าอาชญากรไซเบอร์ทำการสุ่ม และเดาได้ว่าจะใช้พาสเวิร์ดที่ได้มาทำอะไรต่อไป และเมื่อเหยื่อกรอกข้อมูลกับเป็นการส่งข้อมูลนั้นไปยังอาชญากรไซเบอร์ แถมยังไม่สามารถเข้าใช้งานได้อีก

อันดับที่ 1

สังคมที่ตกต่ำลง เป็นผลพวงของการเติบโตอย่างรวดเร็วจนดูเหมือนว่ายากที่จะควบคุม ความอันตรายของโลกออนไลน์ ทำให้เกิดพฤติกรรมเลียนแบบมากมาย (โดยเฉพาะในทางไม่ดี) มีการโชว์คลิปต่างๆ ที่เป็นการทำลายจริยธรรมของมนุษย์ผ่านทางเว็บไซต์ที่เผยแพร่คลิป ส่งผลเสียต่อสังคมและวัฒนธรรม ทำให้เด็กและเยาวชนจำนวนมากไม่น้อย สื่อแวมมีพฤติกรรมที่ใช้ความรุนแรง ไม่ว่าจะเป็นการถ่ายคลิปทำร้ายร่างกายกัน การบังคับขืนใจและใช้การถ่ายคลิปเพื่อข่มขู่ การทำร้ายกัน การฆ่าตัวตาย หรือแม้แต่การถ่ายรูปตัวเองในลักษณะที่ยั่วยวนและนำขึ้นไปโพสต์ตามเว็บต่างๆ ทำให้เกิดปัญหาพฤติกรรมทางเพศของเด็กและเยาวชนที่รวดเร็วขึ้น และทำให้เกิดคดีการล่วงละเมิดและเยาวชนที่สูงขึ้นเช่นกัน

อนุพงศ์ อวิรุทธา

anupong.av@spu.ac.th

หัวหน้าสาขาวิชาการจัดการ คณะบริหารธุรกิจ
มหาวิทยาลัยศรีปทุม