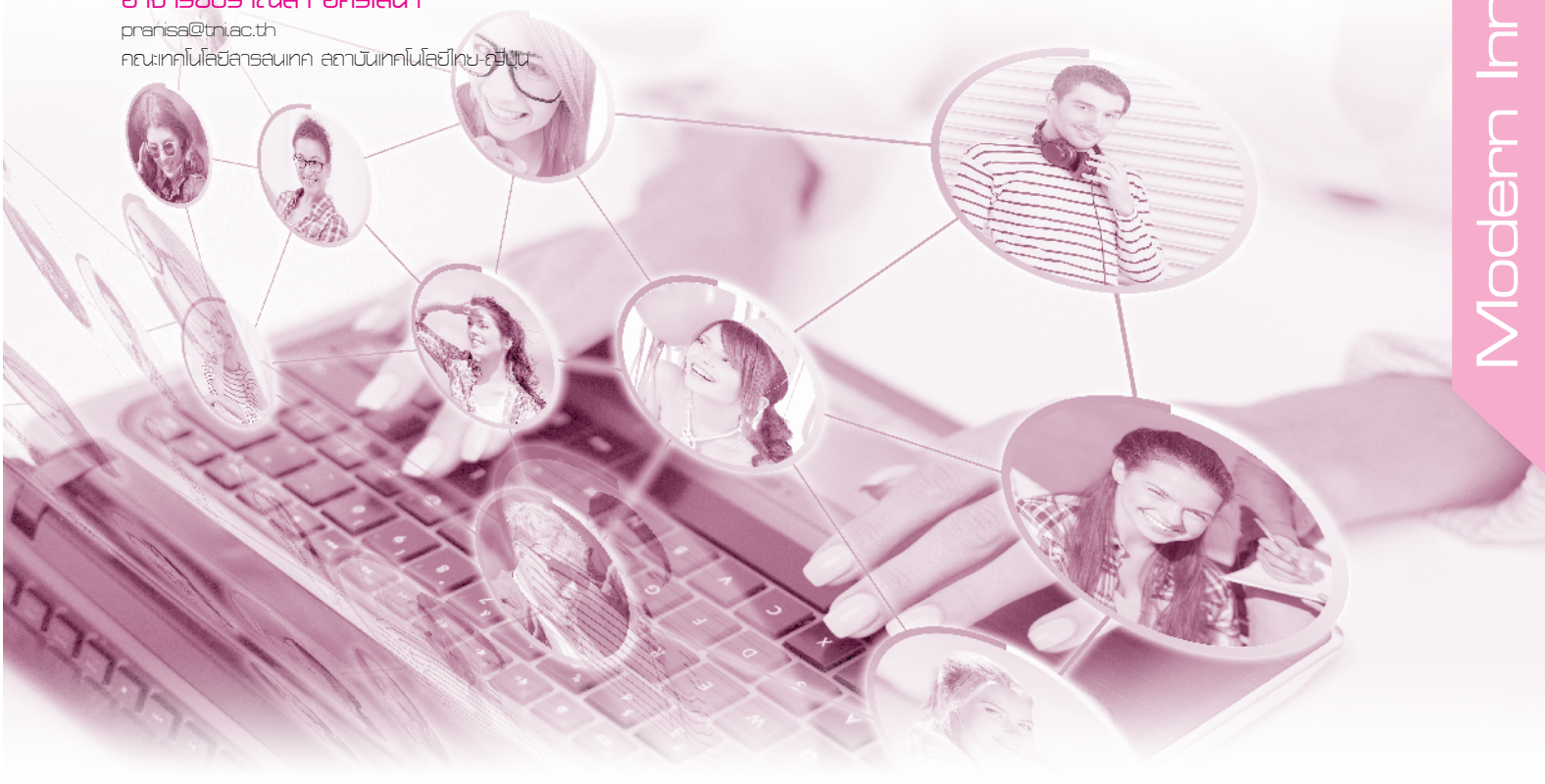
รู้ทัน ข้อความลวงออนไลน์

อาจารย์ปราณิสา อิศรเสนา
pranisa@tni.ac.th
คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น



หลอกโอนเงินจากเว็บหาคู่ แล้วไม่ได้แต่ง... หลอกลงทุนแล้วเชิดหนี ...หลอกว่าได้รางวัลใหญ่ สุดท้ายมีแต่เสียตังค์ฟรีค่ามัดจำ... เรื่องราวคุ้นๆ แบบนี้อยู่รอบๆ ตัวเราจนบางทีเราอาจคิดไปว่า รู้เท่าทันหมดแล้วลูกไม้เก่าๆ แบบนี้ แต่จะเป็นความจริงหรือไม่ประการใดลองศึกษาบทความนี้กันนะคะ

ปัจจุบันนี้ อีเมล์ เฟสบุ๊ค หรือสื่อออนไลน์รอบๆ ตัวเรามีมากมาย บางทีเข้าไปดูอินสตาแกรมดารา ก็มักเจอข้อความฝากร้านชวนทำงานจากบ้านได้เงินง่ายๆ ทีนี้จะเชื่อได้อย่างไรล่ะว่าเรื่องเหล่านี้เป็นความจริง สมมติว่าเราได้อีเมล์แนะนำชวนทำบุญช่วยเด็กยากจนมาจากแอดเดรสของเพื่อนเราล่ะ จะเป็นไปได้ไหมที่คนอื่นเป็นคนปลอมอีเมล์ของเพื่อนมาชวนต่างหาก ส่วนเงินก็เข้าบัญชีนายอะไรก็ไม่รู้สักคนหนึ่ง คำตอบคือเป็นไปได้แน่นอนที่จะปลอมแหล่งส่งอีเมล์ โดยที่ตัวจริงไม่รู้เรื่องอะไรด้วยเลย หากจะย้อนกลับไป อีเมล์โฆษณาหรือสแปมนี่นับว่าเป็นบรรพบุรุษของข้อความลวงประเภทอื่นๆ อีกมากมาย เมื่อก่อนหากจะตุ๋นใครหลอกใคร คนหลอกก็ต้องลงทุนโทรศัพท์บ้าง ส่งไปรษณีย์บ้าง หรือแม้แต่เสี่ยงมาเจอเหยื่อให้ตายใจคือต้องพยายามพอควรกว่าจะให้เหยื่อหลงกล แต่ด้วยการสื่อสารออนไลน์ทำให้การโกงทำได้สบายๆ มากขึ้น ปกปิดตัวจนได้ สมบูรณ์แบบ แค่มีคนหลงเชื่อสัก 1% จากที่ส่งไปพันๆ คน ก็ได้ผลเกินคุ้มแล้ว

กลลวงคลาสสิค “สูตรดั้งเดิม”

แม้จะมีข้อความลวงลักษณะนี้มาหลายปี แต่ก็ยังมีคนหลงกลอยู่เรื่อยๆ ผู้สูงอายุถูกหลอกลงทุน เอาเงินเก็บทั้งชีวิตให้คนแปลกหน้า เสร็จแล้วมาร้องไห้ออกสื่อ ก็มีให้เห็นประจำ ดังนั้นบทความนี้จะขอแนะนำ รูปแบบข้อความลวงคลาสสิค ตามข้อมูลจากศูนย์เฝ้าระวังภัยคุกคาม CERT ของอเมริกากันนะคะ (United States Computer Security Readiness TEAM www.us-cert.gov)

- โอกาสทองทางธุรกิจ
- จดหมายลูกโซ่ (ส่งต่อไปจะโชคดี, น้องจะได้เงินบริจาคจากเฟสบุ๊ค หนึ่งบาทต่อหนึ่งฟอร์เวิร์ด, ไม่ส่งต่อจะโชคร้ายทั้งปี ฯลฯ)
- ทำงานง่ายๆ จากบ้านคุณ
- เพื่อสุขภาพดี ช่วยลดน้ำหนัก
- ได้เงินใช้สบายๆ
- สินค้าแจกฟรี
- นาทีทองการลงทุน
- รับประกันผลกู้เงิน มีปัญหาเครดิต ติดแบลคลิสท์ก็กู้ได้

ส่วนใหญ่ข้อความประเภทนี้จะเสนอผลตอบแทนมหาศาลจากความพยายามแค่นิดหน่อย เช่น “งานพิเศษแค่อาทิตย์ละชั่วโมงเปลี่ยนชีวิต” “มาเป็นนายตัวเองกันเถอะ” “เลือกเวลาทำงานได้

ตามใจ” และข้อความกระตุ้นต่อมโลภ เพิ่มเติม เช่น

- ประมูลออนไลน์ รายได้แน่นอน
- รวยเร็ว คลิกเลย
- ให้คอมพ์ที่บ้านทำงานแทนคุณ
- ให้อินเทอร์เน็ตช่วยหาเงินกันดีกว่า
- ความลับอีเบย์

หากสังเกตสักนิด เราจะพบว่า **ข้อความลวงพวกนี้จะไม่บอกชัดๆ ว่า ธุรกิจที่ว่ารวยว่าดีนั้นคืออะไร** บางครั้งก็จะแนะนำงานสัมมนาฟรี หรือแนะนำเว็บไซต์ต่อที่หากอยากได้คำแนะนำมากกว่านี้ต้องเสียค่าสมัครขั้นต้นก่อน แต่พอหลงโอนเงินไปจริง ก็จะได้แต่คำแนะนำพื้นๆ หรือให้เราไปหาเหยื่อคนอื่นเพิ่มเติมเพื่อให้ได้ส่วนแบ่งค่าสมัคร อาจเรียกสวยๆ ว่าเพิ่มโอกาสทางธุรกิจ ของดีๆ ต้องบอกต่อ แต่ไม่ว่าคำพูดจะสวยหรูอย่างไรสุดท้ายก็เหมือนแชร์ลูกโซ่ ที่พร้อมจะล้มได้ทุกเมื่อหากไม่มีคนหลงหลให้หลอกต่ออีกต่อไป เหมือนทะเลที่ไม่มีปลาให้จับนั่นเอง

การใช้ความไม่มั่นใจ ความอ่อนแอของผู้อื่น เช่น “อยากผอมสวยไวๆ ไม่ต้องอดอาหารเราช่วยได้ “ก็เป็นอีกตัวอย่างคลาสสิคเหยื่อเองมักจะอายหรือลังเลที่จะปรึกษากับผู้เชี่ยวชาญ เช่นแพทย์อยู่แล้วหรือไม่มีกำลังทรัพย์พอใช้ซื้อสินค้าหรือบริการจริง ข้อความลวงพวกนี้ มักจะสัญญาว่าจะหายเร็ว เห็นผลทันที ราคาไม่แพง ไม่ต้องยุ่งยากให้แพทย์สั่ง และมีแพ็คเกจสวยงามให้ดูมีคุณค่ากว่าตัวสินค้าจริง เช่น ครีมหน้าขาวผสมปรอทในกล่องขอบทอง เป็นต้น บางทีก็มีคำให้การของผู้เคยใช้แล้วเห็นผล ให้ชื่อให้นามสกุลมา ถามว่าเราจะรู้ได้อย่างไรว่าคนเหล่านั้นไม่ใช่พวกเดียวกับผู้ขาย หรือหากใช้แล้วไม่ได้ผลตามโฆษณา ก็ตรวจสอบไม่ได้

Phishing E-mail

คือ อีเมล์ที่ออกแบบให้เหมือนกับมาจากผู้ส่งตัวจริง จากนั้นก็จะล่อลวงเหยื่อให้ไปที่เว็บปลอม หรือให้ดาวน์โหลด Malware

(ไวรัสหรือโปรแกรมที่ทำให้คนร้ายเข้ามาควบคุมเครื่องเรา) เปิดเผยข้อมูลส่วนตัว ตัวอย่างที่เห็นได้ชัดเจนคงไม่พ้นหน้าเว็บปลอมของธนาคารออนไลน์ติดต่อมาว่าบัญชีผู้ใช้ของท่านมีปัญหา และให้ยืนยันตัวตนโดยการคลิกลิ้งค์ และกรอกแบบฟอร์มออนไลน์ เมื่อคลิกลิงค์ที่ดูเหมือน URL ธนาคาร แต่จริงๆ โอนไปที่เว็บหลอก ทุกข้อมูลที่กรอกไป ชื่อผู้ใช้ พาสเวิร์ด ข้อมูลการเงินก็จะเป็นของคนร้ายไปได้ง่ายๆ ที่นี้จะระวังได้อย่างไร จำไว้ว่าธนาคารจะไม่ส่งอีเมล์มาให้ลูกค้ายืนยันตัวตนออนไลน์เด็ดขาด **อะไรก็ตามที่เราไม่ได้พิมพ์ URL เอง ห้ามคลิกเด็ดขาด** นอกจากนี้ปกติธนาคารจะยืนยันตัวตนด้วยหลายปัจจัย เช่น ให้ยืนยันตัวตนด้วยโทรศัพท์ OTP (one time password) ที่หมดอายุในสองสามนาที นอกเหนือจากชื่อผู้ใช้และรหัสผ่าน ก็จะช่วยป้องกันได้มาก

นอกจากเรื่องธนาคารแล้ว ข้อความลวงยังอาจมาจากแผนกไอทีของท่าน ผู้ให้บริการอินเทอร์เน็ตของท่าน (คนร้ายปลอมต้นทางมา) ดังนั้น เมื่อไรก็ตามที่ไม่แน่ใจก็ขอให้ใช้วิธีติดต่อกลับไปที่ call center หรือช่องทางติดต่ออย่างเป็นทางการของผู้ให้บริการนั้นเอง อย่าไปคลิกลิงค์ที่คนอื่นส่งมา

สุดท้ายนี้ก็คือ การจะรู้เท่าทันข้อความลวง ขอให้ระวังข้อความที่เสนออะไรดีเกินจริงจากผู้ที่ไม่รู้จัก หัดสังเกตอีเมล์ที่แนบไฟล์โปสการ์ดแปลกๆ ให้ระวังว่าอีเมล์จากบริษัทแอนตี้ไวรัสที่ชี้ชวนให้อัพเดทฐานข้อมูลไวรัส โดยคลิกลิ้งค์ดาวน์โหลดจากในอีเมล์นั่นแหละมักเป็นไวรัสเสียเอง (ปกติแอนตี้ไวรัสจะอัพเดทผ่านโปรแกรมเฉพาะอยู่แล้ว) เรื่องตลก รูปสาวสวยเซ็กซี่ ที่ถูกฟอร์เวิร์ดมาจนหาที่มาไม่ได้ โปรแกรมที่ไม่ต้องคลิกก็เปิดเมล์ให้อัตโนมัติก็ปิดฟีเจอร์นี้เสีย เพราะมีความเสี่ยงสูงมากที่จะมาจากผู้ไม่ประสงค์ดี หรือการกำหนดค่าอีเมล์ไคลแอนท์ เช่น outlook ให้กรองสแปม แบบละเอียดก็ช่วยได้มาก ใช้สัญชาติญาณว่าโลกนี้ไม่มีอะไรได้มาง่ายๆ ฟรีๆ และหมั่นติดตามข่าวสารสม่ำเสมอให้รู้เท่าทัน ก็จะเป็นประโยชน์ สุดท้ายนี้ ขอให้ทุกท่านอยู่รอดปลอดภัยในยุคไซเบอร์กันนะคะ และอย่าลืมติดตามคอร์สอบรม IT ดีๆ ได้ที่ Website คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย-ญี่ปุ่น http://it.tni.ac.th ยินดีต้อนรับทุกท่านค่ะ TPA news