SANS SECURITY AWARENESS

คู่มือการสร้างความตระหนักรู้เรื่องความปลอดภัย — ทำงานจากที่บ้านอย่างปลอดภัย

บทสรุปสำหรับผู้บริหาร

องค์กรหลายองค์กรในขณะนี้จำเป็นต้องปรับเปลี่ยนการทำงานของพนักงานของตนเป็นการทำงานจากที่บ้าน อันเนื่องมาจากไวรัสโคโรนา ซึ่งประเด็นนี้อาจจะเป็นเรื่องที่ท้าทายเพราะว่าหลายองค์กรไม่มีนโยบาย เทคโนโลยี รวมถึงการฝึกอบรมเพื่อให้สามารถทำงานจากทางไกลได้อย่างปลอดภัย นอกจากนั้น พนักงานหลายคนยังคงมีความไม่คุ้นเคย หรือไม่สบายใจเกี่ยวกับแนวคิดเรื่องการทำงานจากที่บ้าน จุดประสงค์ของคู่มือฉบับนี้ก็คือ การช่วยให้คุณสามารถฝึกอบรมบุคลากรของคุณให้ตระหนักรู้เรื่องความปลอดภัยให้มากที่สุดเท่าที่จะเป็นไปได้อย่างรวดเร็ว หากคุณมีคำถามเกี่ยวกับการใช้งานคู่มือฉบับนี้ สามารถติดต่อเราได้ที่ support@sans.org

เนื่องจากมีความเป็นไปได้อย่างมากที่บุคลากรของคุณจะต้องประสบกับความตึงเครียดและการเปลี่ยนแปลงอย่างมาก และองค์กรของคุณก็มีโอกาสสูงที่จะประสบกับข้อจำกัดด้านเวลาและทรัพยากร คู่มือเชิงกลยุทธ์ฉบับนี้จะมุ่งเน้นไปที่การทำให้การฝึกอบรมมีความเรียบง่ายมากที่สุดเท่าที่จะเป็นไปได้ เราขอแนะนำให้คุณมุ่งเน้นไปที่ความเสี่ยงที่สำคัญที่สุดที่จะสร้างผลกระทบใหญ่หลวงที่สุด ซึ่งเราจะอธิบายให้รับทราบดังต่อไปนี้ โปรดถือว่านี่คือจุดเริ่มต้น หากมีความเสี่ยงเพิ่มเติมหรือประเด็นอื่นที่คุณอยากจะเพิ่ม โปรดเพิ่มเข้ามา โปรดระลึกไว้ว่า ยิ่งมีพฤติกรรม กระบวนการ หรือเทคโนโลยีที่คุณกำหนดให้พนักงานของคุณดำเนินการมากขึ้นเท่าไร โอกาสที่พนักงานของคุณจะนำมาดำเนินการได้ทั้งหมดก็จะยิ่งน้อยลงเท่านั้น

วิธีการใช้งานคู่มือฉบับนี้

เราขอแนะนำให้คุณเริ่มต้นด้วยการอ่านรายละเอียดที่อยู่ในคู่มือฉบับนี้ และตรวจดูลิงก์ที่เชื่อมต่อไปยังแหล่งข้อมูลอื่น เพื่อที่คุณจะได้เห็นภาพรวมว่ามีข้อมูลอะไรที่สามารถใช้ได้บ้าง คุณจะพบได้ว่า ความเสี่ยงแต่ละประเด็นที่ได้ระบุไว้ เราจะมีการเตรียมแหล่งข้อมูลที่แตกต่างกันไว้อย่างหลากหลาย เพื่อให้คุณสามารถนำไปใช้งานและฝึกอบรมให้องค์กรของคุณได้ สิ่งเหล่านี้จะทำให้คุณสามารถเลือกลักษณะของชุดข้อมูลที่คุณรู้สึกว่ามีประสิทธิภาพมากที่สุดต่อความจำเป็นและวัฒนธรรมองค์กรของคุณได้ หลังจากที่คุณได้อ่านเอกสารฉบับนี้จบแล้ว ให้คุณอ่านแม่แบบการสื่อสารและเอกสารข้อมูลที่เป็นเอกสารประกอบมาพร้อมกับชุดเอกสารชุดนี้ เพื่อให้คุณมีความเข้าใจเกี่ยวกับสิ่งที่คุณต้องการจะบรรลุได้ดียิ่งขึ้น เมื่อคุณได้อ่านเอกสารเสร็จเป็นที่เรียบร้อยแล้ว จะมีกลุ่มงานหลักสำคัญ 2 กลุ่มที่คุณจะต้องร่วมประสานงาน ซึ่งก็คือ

1. **ทีมงานรักษาความปลอดภัย:** โปรดประสานงานกับทีมงานรักษาความปลอดภัยของคุณ
   เพื่อที่จะมีความเข้าใจที่ดีขึ้นเกี่ยวกับความเสี่ยงสำคัญที่คุณพยายามจะบริหารจัดการ เราได้ระบุถึงความเสี่ยงที่เราเชื่อว่าเป็นความเสี่ยงที่สำคัญไว้ในคู่มือฉบับนี้ โดยจะเป็นความเสี่ยงที่สามารถพบเห็นได้ทั่วไปในพนักงานที่ทำงานจากที่บ้าน แต่อย่างไรก็ตามความเสี่ยงของคุณอาจจะมีความแตกต่างกันออกไป เราขอแจ้งเตือนไว้ตรงนี้ว่า ความผิดพลาดของทีมงานรักษาความปลอดภัยที่พบได้บ่อยก็คือ การพยายามบริหารจัดการความเสี่ยงทั้งหมดที่มี และการมีนโยบายพร้อมข้อกำหนดจำนวนมากก็จะทำให้บุคลากรมีงานล้นมือ
   ให้พยายามจำกัดความเสี่ยงที่คุณต้องการจะตอบสนองให้เหลือน้อยที่สุดเท่าที่จะเป็นไปได้ เมื่อคุณได้ระบุและจัดลำดับความเสี่ยงของคุณเป็นที่เรียบร้อยแล้ว ให้คุณชี้ชัดไปที่พฤติกรรมที่จะช่วยบริหารจัดการความเสี่ยงนั้น ๆ จากที่เราได้กล่าวไป ในกรณีที่องค์กรของคุณไม่มีความพร้อมด้านเวลาหรือทรัพยากร โปรดใช้ประโยชน์จากสิ่งที่เราจะระบุให้รับทราบดังต่อไปนี้

2. **การสื่อสาร:**
   คุณได้ระบุความเสี่ยงด้านบุคคลที่มีความสำคัญที่สุดของคุณพร้อมกับพฤติกรรมสำคัญที่คุณจะต้องใช้เพื่อบริหารจัดการความเสี่ยงเหล่านั้นเป็นที่เรียบร้อยแล้ว ให้คุณร่วมงานกับทีมงานสื่อสารองค์กรของคุณ เพื่อเข้าหาและฝึกอบรมพนักงานของคุณให้มีพฤติกรรมเหล่านั้น
   แผนงานความตระหนักรู้เรื่องความปลอดภัยที่มีประสิทธิภาพที่สุดนั้น จะเกิดขึ้นได้จากการร่วมมืออย่างขันแข็งกับทีมงานสื่อสารองค์กร หากเป็นไปได้ ให้พิจารณาว่าสามารถนำพนักงานจากทีมงานสื่อสารองค์กรเข้ามาอยู่ในทีมงานรักษาความปลอดภัยของคุณได้หรือไม่ เวลาที่คุณทำการสื่อสารกับพนักงานของคุณ

คำพูดที่กระตุ้นที่มีประสิทธิภาพที่คุณสามารถใช้งานเพื่อให้พนักงานสนใจ คือ
การเน้นย้ำให้ทราบว่าการอบรมครั้งนี้ไม่เพียงแต่จะช่วยทำให้พนักงานของคุณมีความปลอดภัยกับการทำงานเท่านั้น
แต่ยังช่วยทำให้มีความปลอดภัยด้านไซเบอร์ที่บ้านอีกด้วย อันจะช่วยคุ้มครองได้ทั้งตนเองและครอบครัว

เป้าหมายสูงสุดของการร่วมงานกับกลุ่มงานทั้งสองกลุ่มนี้ ก็คือการพยายามทำให้ความปลอดภัยมีความเรียบง่ายที่สุดเท่าที่จะเป็นไปได้เพื่อพนักงานของคุณ และสร้างแรงจูงใจให้แก่พนักงานของคุณ **ทั้ง 2 ประเด็นนี้คือองค์ประกอบสำคัญที่จะทำให้เกิดการเปลี่ยนแปลงพฤติกรรม** นอกจากนั้น เรายังขอแนะนำให้คุณแต่งตั้งคณะกรรมการที่ปรึกษา ที่ประกอบไปด้วยบุคคลสำคัญที่สามารถมอบข้อเสนอแนะและคำติชมที่คุณสามารถนำไปใช้ในแผนงานของคุณได้ นอกจากทีมงานรักษาความปลอดภัยและทีมงานสื่อสารองค์กรของคุณแล้ว หน่วยงานอื่น ๆ ที่คุณควรจะต้องจับมือและร่วมประสานงานได้แก่ ฝ่ายทรัพยากรบุคคล และฝ่ายกฎหมาย

ชุดข้อมูลสำหรับดาวน์โหลดทางดิจิทัล MGT433

SANS Institute มีหลักสูตรฝึกอบรมที่ใช้ระยะเวลา 2 วัน ซึ่งก็คือ MGT433: วิธีการสร้าง คงรักษา และวัดผลแผนงานการสร้างความตระหนักรู้เรื่องความปลอดภัยที่มีผลต่อประสิทธิภาพอยู่ในระดับสูง หลักสูตรเร่งรัดนี้จะให้รายละเอียดทฤษฎี ทักษะ กรอบวิธีดำเนินงาน และแหล่งข้อมูลที่จำเป็นต่อการสร้างแผนงานตระหนักรู้เรื่องความปลอดภัยที่มีผลต่อประสิทธิภาพอยู่ในระดับสูง
ที่จะทำให้คุณสามารถบริหารจัดการและวัดผลความเสี่ยงของมนุษย์ได้อย่างมีประสิทธิภาพ นอกจากนั้น
เรายังได้จัดเตรียมข้อมูลแม่แบบและการวางแผนที่เป็นชุดข้อมูลสำหรับดาวน์โหลดทางดิจิทัล ซึ่งเป็นส่วนหนึ่งของคู่มือฉบับนี้ ไว้ให้ใช้งานโดยไม่มีค่าใช้จ่ายอีกด้วย
ถึงแม้ว่าแหล่งข้อมูลเหล่านี้อาจจะมีรายละเอียดการใช้งานที่ลึกซึ้งยิ่งขึ้นเกินกว่าความจำเป็นของแผนงานนี้ก็ตาม
แต่ว่าข้อมูลเหล่านี้อาจจะมีค่าอย่างยิ่งสำหรับองค์กรขนาดใหญ่ หรือในการกำหนดใช้แผนงานที่มีความละเอียดซับซ้อนมากขึ้น

การตอบคำถามของพนักงาน

นอกจากการสื่อสารและการฝึกอบรมให้แก่พนักงานของคุณแล้ว เราขอแนะนำเป็นอย่างยิ่งให้ใช้เทคโนโลยีบางประเภทหรือกระดานสนทนา
เพื่อให้คุณสามารถตอบคำถามพนักงานของคุณ และถ้าทำได้ ให้ตอบคำถามโดยทันที ซึ่งคุณสามารถใช้อีเมลเฉพาะพิเศษ ใช้การสนทนาผ่าน Skype หรือ Slack หรือใช้กระดานสนทนาออนไลน์บางประเภท เช่น Yammer ก็ได้ หรือคุณจะจัดการถ่ายทอดสดเกี่ยวกับการรักษาความปลอดภัยผ่านทางเว็บก็ได้
เพราะจะทำให้คุณสามารถเปิดให้เข้าร่วมรับข้อมูลได้หลายครั้งในแต่ละสัปดาห์
เพื่อให้พนักงานของคุณสามารถเลือกเวลาเข้าร่วมรับชมการถ่ายทอดสดที่เหมาะสมกับตนเองที่สุด รวมถึงอาจจะสามารถถามคำถามสดได้อีกด้วย
เพราะเป้าหมายก็คือทำให้การรักษาความปลอดภัยเป็นสิ่งที่จับต้องได้ง่ายมากที่สุดเท่าที่จะเป็นไปได้ รวมถึงช่วยตอบคำถามที่พนักงานของคุณมี
นี่คือโอกาสอันดีเยี่ยมในการให้พนักงานของคุณมีส่วนร่วม และทำให้การรักษาความปลอดภัยมีความเป็นมิตร โปรดใช้โอกาสจากวิกฤตรงนี้ ขอให้โปรดระลึกไว้เสมอว่า
ในการจะทำให้การดำเนินการนี้มีประสิทธิภาพได้นั้น คุณจะต้องจัดสรรทรัพยากรเป็นการเฉพาะ เพื่อดูแลช่องสื่อสารถ่ายทอดเกี่ยวกับเรื่องการรักษาความปลอดภัย
และตอบคำถามอย่างกระตือรือร้น

ความเสี่ยงและแหล่งข้อมูลเพื่อการฝึกอบรม

เราได้ระบุถึงความเสี่ยงหลัก 3 ประการที่คุณควรจะต้องบริหารจัดการให้กับพนักงานที่ทำงานจากทางไกลของคุณ นี่คือจุดเริ่มต้น
และเป็นประเด็นที่น่าจะมีคุณค่าที่สุดสำหรับคุณ ความเสี่ยงแต่ละประเด็นตามรายละเอียดด้านล่างนี้ จะมีลิงก์เชื่อมต่อไปหาแหล่งข้อมูลหลายแหล่ง
เพื่อช่วยในการสื่อสารและฝึกอบรมหัวข้อนั้น ๆ
เราได้จัดเตรียมสื่อเพื่อการสื่อสารองค์กรที่หลากหลายซึ่งคุณสามารถเลือกใช้ได้เพื่อให้เกิดผลประโยชน์สูงสุดสำหรับวัฒนธรรมองค์กรของคุณ นอกจากนั้น
ข้อมูลเกือบทั้งหมดที่เตรียมไว้จะพร้อมใช้งานในหลายภาษา ถ้าหากทั้งหมดที่กล่าวมานี้รู้สึกว่ามีความลำบากในการรับมือ และคุณมีเวลาที่จำกัดเป็นอย่างยิ่ง
หากเป็นเช่นนั้นเราขอแนะนำให้คุณใช้งานสื่อข้อมูล 2 ชุดที่เราได้ให้รายการไว้ด้านล่างนี้

1. เอกสารข้อมูลเพื่อการทำงานจากที่บ้านอย่างปลอดภัย (รวมไว้แล้วอยู่ในชุดเอกสารใช้งานของคุณ)
2. วิดีโอการสร้างความปลอดภัยทางไซเบอร์ที่บ้าน (ภาษาอังกฤษ) และพร้อมใช้งาน ในภาษาอื่น ๆ ที่นี่

วิศวกรรมสังคม

หนึ่งในความเสี่ยงที่สำคัญที่สุดที่พนักงานผู้ทำงานจากทางไกลจะประสบ โดยเฉพาะอย่างยิ่งในช่วงเวลาที่มีการเปลี่ยนแปลงใหญ่หลวงและมีสภาพแวดล้อมของความเร่งด่วน ก็คือการถูกโจมตีทางวิศวกรรมสังคม วิศวกรรมสังคมเป็นการโจมตีเชิงจิตวิทยา ที่ผู้โจมตีจะใช้กลเม็ดหรือหลอกให้เหยื่อของตนเองหลงกลที่จะทำสิ่งที่ผิดพลาด ซึ่งในช่วงเวลาที่มีการเปลี่ยนแปลงและมีความสับสนนั้น กรณีเช่นนี้ก็จะทำให้การโจมตีง่ายยิ่งขึ้น กุญแจสำคัญก็คือการฝึกอบรมพนักงานให้รู้จักว่าวิศวกรรมสังคมคืออะไร รู้จักถึงวิธีการสังเกตเห็นตัวบ่งชี้วิศวกรรมสังคมที่พบเจอได้บ่อยที่สุด และรู้จักถึงสิ่งที่จะต้องดำเนินการเมื่อสังเกตพบแล้ว
ต้องดำเนินการให้มั่นใจว่าเราไม่ได้มุ่งเน้นไปที่เพียงแค่การโจมตีอีเมลฟิชชิ่งเท่านั้น เรายังต้องมุ่งเน้นถึงกระบวนวิธีการอื่นอีกด้วย เช่น การโทรศัพท์ การส่งข้อความโซเชียลมีเดียต่าง ๆ และข่าวปลอมหรือที่รู้จักกันว่าเฟกนิวส์ คุณสามารถหาสื่อข้อมูลที่คุณจำเป็นต้องใช้ในการฝึกอบรมและเน้นย้ำเกี่ยวกับประเด็นนี้ได้จากโฟลเดอร์ สื่อข้อมูลช่วยเหลือเรื่องวิศวกรรมสังคม นอกจากนั้น วิดีโอดังต่อไปนี้ คือ วิดีโอการสร้างความตระหนักรู้เรื่องความปลอดภัยของ 2 วิดีโอ ที่คุณสามารถลิงก์เข้ามาหาได้และพร้อมให้ใช้งานในหลายภาษา

- วิศวกรรมสังคม (ภาษาอังกฤษ) และพร้อมใช้งานใน ภาษาอื่น ๆ ที่นี่
- ฟิชชิ่ง (ภาษาอังกฤษ) และพร้อมใช้งานใน ภาษาอื่น ๆ ที่นี่

รหัสผ่านที่มีความแข็งแรง

ตามที่ได้ระบุในงานสัมมนา Verizon DBIR ประจำปี รหัสผ่านที่มีความอ่อนแอยังคงเป็นหนึ่งในประเด็นหลักสำคัญที่ทำให้เกิดการเจาะเข้าระบบได้ในระดับโลก มีพฤติกรรมสำคัญอยู่ 4 ประการด้วยกันที่จะช่วยบริหารจัดการความเสี่ยงนี้ได้ โดยมีรายละเอียดดังต่อไปนี้
คุณสามารถหาสื่อข้อมูลที่คุณจำเป็นต้องใช้ในการฝึกอบรมและเสริมทักษะเกี่ยวกับประเด็นนี้ได้จากโฟลเดอร์ รหัสผ่าน

- ข้อความรหัสผ่าน (ขอโปรดให้ทราบด้วยว่า ทั้งรหัสผ่านที่มีความซับซ้อน และ รหัสผ่านที่หมดอายุ ไม่สามารถใช้งานได้อย่างมีประสิทธิภาพอีกต่อไปแล้ว)
- ใช้รหัสผ่านที่ไม่ซ้ำกันกับแต่ละบัญชี
- ใช้โปรแกรมจัดการรหัสผ่าน
- ใช้การยืนยันตัวตนหลายขั้นตอน หรือที่รู้จักกันในอีกชื่อหนึ่งว่าการยืนยันตัวตนสองขั้นตอน หรือการตรวจสอบความถูกต้องสองขั้นตอน

อัปเดตระบบ

ความเสี่ยงประการที่สาม คือการที่จะต้องดำเนินการให้มั่นใจว่า เทคโนโลยีต่าง ๆ ที่บุคลากรของคนใช้งานนั้นเป็นเวอร์ชันล่าสุด ไม่ว่าจะเป็นระบบปฏิบัติการ แอปพลิเคชันต่าง ๆ หรือโมบายแอพก็ตาม สำหรับบุคลากรที่ใช้งานอุปกรณ์ส่วนบุคคล ก็อาจจะจำเป็นที่จะต้องเปิดการอัปเดตอัตโนมัติ
คุณสามารถหาสื่อข้อมูลที่คุณจำเป็นต้องใช้ในการฝึกอบรมและเสริมทักษะเกี่ยวกับประเด็นนี้ได้จากโฟลเดอร์มัลแวร์หรือการสร้างบ้านที่มีความปลอดภัยทางไซเบอร์

หัวข้อประเด็นอื่นที่ควรพิจารณา

- **Wi-Fi**: การสร้างความปลอดภัยให้จุดเชื่อมต่อ Wi-Fi ประเด็นนี้จะถูกครอบคลุมอยู่ในสื่อข้อมูล การสร้างบ้านที่มีความปลอดภัยทางไซเบอร์ นอกจากนั้น โปรดพิจารณาดูวิดีโอนี้ การสร้างบ้านที่มีความปลอดภัยทางไซเบอร์ (ภาษาอังกฤษ) และพร้อมใช้งานใน ภาษาอื่น ๆ ที่นี่.

- **VPN's**: VPN คืออะไรและเพราะเหตุใดจึงควรใช้ เราขอแนะนำ จดหมายข่าว OUCH เกี่ยวกับ VPN.

- **การทำงานจากระยะไกล:** ประเด็นนี้มีไว้สำหรับบุคคลที่ทำงานจากระยะไกล แต่ "ไม่ได้" ทำงานจากที่บ้าน เช่น การทำงานในร้านกาแฟ ที่ท่าอากาศยาน หรือที่โรงแรม เป็นต้น โปรดพิจารณาดู วิดีโอฝึกอบรม การทำงานจากระยะไกล (ภาษาอังกฤษ) และพร้อมใช้งานใน ภาษาอื่น ๆ ที่นี่.

- **บุตรหลาน / ผู้มาเยือน:** เพื่อเป็นการเน้นย้ำแนวคิดว่า สมาชิกในครอบครัว/ผู้มาเยือน ไม่ควรเข้าถึงอุปกรณ์ที่เกี่ยวกับการทำงานได้ โปรดพิจารณาดู วิดีโอฝึกอบรม การทำงานจากระยะไกล (ภาษาอังกฤษ) และพร้อมใช้งานใน ภาษาอื่น ๆ ที่นี่.

- **การตรวจจับ / การตอบสนอง:**

  คุณต้องการให้พนักงานของคุณรายงานเมื่อพนักงานของคุณเชื่อว่ามีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นมาในขณะที่ทำงานจากที่บ้านหรือไม่? หากคุณต้องการ คุณจะให้พนักงานของคุณแจ้งรายงานเกี่ยวกับอะไร และแจ้งเมื่อใด? ประเด็นนี้ได้รับการครอบคลุมอยู่ในข้อมูลการถูกเจาะเข้าโปรแกรม

จดหมายข่าว OUCH

นอกจากนั้น โปรดพิจารณาใช้งานจดหมายข่าว OUCH ที่เปิดให้เข้าใช้งานได้โดยสาธารณะ เพื่อช่วยในการสนับสนุนแผนงานของคุณ แต่ละฉบับได้รับการแปลเป็นภาษาอื่นมากกว่า 20 ภาษา รายการด้านล่างดังต่อไปนี้ เป็นจดหมายข่าว OUCH ที่เราเชื่อว่าจะสามารถช่วยเหลือแผนงานการทำงานจากที่บ้านอย่างปลอดภัยของคุณได้เป็นอย่างดี คุณสามารถดูจดหมายข่าวทุกฉบับผ่านทางออนไลน์ได้ที่ คลังข้อมูลจดหมายข่าวการตระหนักรู้เรื่องความปลอดภัยของ OUCH.

ภาพรวม

Four Steps to Staying Secure (4 ขั้นตอนในการรักษาไว้ซึ่งความปลอดภัย)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (การสร้างบ้านที่มีความปลอดภัยทางไซเบอร์)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

วิศวกรรมสังคม

Social Engineering (วิศวกรรมสังคม)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (ส่งข้อความ / สมิชชิ่ง)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (การหลอกลวงประเภทเจาะจงรายตัว)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (การหลอกลวง CEO)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (การโจมตี / หลอกลวงผ่านทางการเรียกสายโทรศัพท์)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (หยุดฟิชชิ่งนั่นเสีย)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (การหลอกลวงคุณผ่านทางโซเชียลมีเดีย)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

รหัสผ่าน

Making Passwords Simple (ทำให้รหัสผ่านเป็นเรื่องง่าย)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (ติดล็อคให้ล็อกอินของคุณ)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

ข้อมูลเพิ่มเติม

Yes, You Are a Target (ใช่ คุณนั่นแหละคือเป้าหมาย)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (อุปกรณ์สมาร์ตโฮม)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

คำแนะนำฉบับเร่งด่วน

คำแนะนำและเคล็ดลับที่คุณสามารถแบ่งปันให้รับทราบได้ อยู่ในรูปแบบที่ใช้งานง่าย

- ขั้นตอนที่มีประสิทธิภาพที่สุดที่คุณสามารถใช้เพื่อคุ้มครองความปลอดภัยให้กับเครือข่ายไร้สายที่บ้านของคุณก็คือ การเปลี่ยนรหัสผ่านมาตรฐาน เปิดใช้งานการเข้ารหัส WPA2 และใช้งานรหัสผ่านที่มีความแข็งแรงให้แก่เครือข่ายไร้สายของคุณ
- ให้พึงระวังสังเกตอุปกรณ์ทุกชิ้นที่เชื่อมต่อเข้ากับเครือข่ายในบ้านของคุณ ซึ่งรวมถึงกล้องดูทารก เครื่องเกมคอนโซล โทรทัศน์ เครื่องใช้ไฟฟ้าต่าง ๆ หรือแม้กระทั่งรถของคุณ ต้องดำเนินการให้มั่นใจว่ามีการปกป้องอุปกรณ์ทั้งหมดด้วยรหัสผ่านที่มีความแข็งแรง และ/หรือ ใช้งานระบบปฏิบัติการเวอร์ชันล่าสุด
- หนึ่งในวิธีการที่มีประสิทธิภาพมากที่สุดในการปกป้องเครื่องคอมพิวเตอร์ที่บ้านของคุณก็คือ การดำเนินการให้มั่นใจว่าได้แพตช์และอัปเดตระบบปฏิบัติการกับแอปพลิเคชันต่าง ๆ ของคุณเป็นที่เรียบร้อยแล้ว เปิดการใช้งานการอัปเดตโดยอัตโนมัติในเวลาที่สามารถทำได้
- และท้ายที่สุด สามัญสำนึกก็คือสิ่งที่จะคุ้มครองตัวคุณได้ดีที่สุด หากอีเมล สายเรียกโทรศัพท์ หรือข้อความออนไลน์ดูแปลก น่าสงสัย หรือดูดีเกินไป นั่นอาจจะเป็นการโจมตี
- ต้องดำเนินการให้มั่นใจว่า คุณได้ใช้รหัสผ่านที่ไม่ซ้ำกันในแต่ละบัญชีของคุณ หากคุณไม่สามารถจดจำรหัสผ่าน/ข้อความรหัสผ่านของตนเองได้ทุกรหัส โปรดพิจารณาใช้งานโปรแกรมบริหารจัดการรหัสผ่าน เพื่อการจัดเก็บรหัสผ่านของคุณทั้งหมดอย่างปลอดภัย
- การตรวจสอบ 2 ขั้นตอน ถือเป็นหนึ่งในขั้นตอนที่ดีที่สุดที่คุณสามารถใช้ในการรักษาความปลอดภัยให้แก่บัญชีของคุณ ไม่ว่าจะเป็นบัญชีใดก็ตาม การตรวจสอบ 2 ขั้นตอน คือการกำหนดให้ใช้ทั้งรหัสผ่าน และรหัสที่ส่งไปหาหรือสร้างขึ้นมาจากอุปกรณ์เคลื่อนที่ของคุณ ตัวอย่างของบริการที่ให้การรองรับการตรวจสอบ 2 ขั้นตอนก็คือ Gmail, Dropbox และ Twitter
- ฟิชชิ่งก็คือเวลาที่ผู้โจมตีพยายามจะหลอกให้คุณคลิกลงไปบนลิงก์ประสงค์ร้าย หรือเปิดสิ่งที่แนบมาด้วยในอีเมล ต้องระมัดระวังอีเมลหรือข้อความที่ได้รับทางออนไลน์ ที่สร้างให้เกิดความรู้สึกจำเป็นเร่งด่วน มีการสะกดผิด หรือขึ้นต้นด้วยคำว่า "เรียนคุณลูกค้า"

มาตรวัดข้อมูล

ในสถานการณ์เช่นนี้ การใช้มาตรวัดข้อมูลพฤติกรรมเป็นสิ่งที่ทำได้ยากลำบาก เพราะเป็นการยากที่จะวัดความประพฤติของพนักงานที่บ้าน นอกจากนั้น พฤติกรรมเหล่านี้บางประการก็ไม่ได้จำกัดอยู่เฉพาะการทำงานอีกด้วย (เช่น การคุ้มครองความปลอดภัยให้แก่อุปกรณ์ Wi-Fi เป็นต้น) แต่อย่างไรก็ตามคุณสามารถวัดค่าความมีส่วนร่วมได้ เราพบว่าประเด็นเรื่องความเป็นส่วนตัวหรือประเด็นที่เต็มเปี่ยมไปด้วยอารมณ์เช่นนี้ สามารถสร้างความมีส่วนร่วมได้อย่างสูงมาก และเป็นที่น่าสนใจกว่าประเด็นอื่นอย่างมากอีกด้วย เช่นนี้แล้ว มาตรวัดข้อมูลดังต่อไปนี้ อาจจะมีประโยชน์ได้

- **ปฏิสัมพันธ์:** พนักงานของคุณถามคำถามบ่อยเพียงใด นำเสนอความคิดหรือขอความช่วยเหลือผ่านทางช่องทางความปลอดภัยหรือกระดานสนทนาที่คุณเป็นผู้ดำเนินการบ่อยเพียงใด?
- **การจำลองสถานการณ์:** ให้จำลองสถานการณ์ว่ามีการโจมตีทางวิศวกรรมสังคมบางประเภท เช่น ฟิชชิ่ง การส่งข้อความ หรือการโจมตีผ่านทางโทรศัพท์ เป็นต้น

สำหรับรายการมาตรวัดข้อมูลครอบคลุมอย่างละเอียด โปรดดาวน์โหลดตารางมาตรวัดข้อมูลการสร้างความตระหนักรู้เรื่องความปลอดภัยเชิงปฏิสัมพันธ์จาก ชุดข้อมูลสำหรับดาวน์โหลดทางดิจิทัล MGT433.

การอนุญาตให้ใช้งาน

สงวนลิขสิทธิ์ © 2020 SANS Institute สงวนลิขสิทธิ์ทั้งหมดโดย SANS Institute ห้ามไม่ให้ผู้ใช้งานคัดลอก ทำซ้ำ เผยแพร่ซ้ำ จัดจำหน่าย แสดงผล หรือสร้างผลงานสืบเนื่องโดยอิงกับส่วนใดส่วนหนึ่งหรือทุกส่วนของเอกสาร ไม่ว่าจะเป็นสื่อประเภทใดก็ตาม ไม่ว่าจะเป็นสื่อพิมพ์ สื่ออิเล็กทรอนิกส์ หรือด้วยวิธีอื่นใดก็ตาม ไม่ว่าเพื่อจุดประสงค์ใดก็ตาม โดยไม่ได้รับความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรจาก SANS Institute นอกจากนั้น ห้ามไม่ให้ผู้ใช้งานขาย ให้เช่า ให้เช่าซื้อ แลกเปลี่ยน หรือโอนถ่ายเอกสารเหล่านี้ไม่ว่าจะด้วยวิธีใดก็ตาม ด้วยรูปลักษณะใดก็ตาม หรือด้วยรูปแบบก็ตาม โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจาก SANS Institute

ผู้ประพันธ์ชุดใช้งาน

Lance Spitzner มีประสบการณ์ด้านความปลอดภัยมากกว่า 20 ปีเกี่ยวกับการวิจัยภัยคุกคามทางไซเบอร์ สถาปัตยกรรมและความตระหนักรู้เรื่องความปลอดภัยและการฝึกอบรม รวมทั้งได้ช่วยเหลือบุกเบิกแขนงวิชาเกี่ยวกับการหลอกลวงและความฉลาดทางไซเบอร์ ด้วยการสร้าง honeynets และการก่อตั้งโครงการ Honeynet ในฐานะที่เป็นวิทยากรของ SANS เขาได้เป็นผู้พัฒนาหลักสูตร MGT433: การตระหนักรู้เรื่องความปลอดภัย และ MGT521: วัฒนธรรมความปลอดภัย นอกจากนั้น Lance ได้ตีพิมพ์หนังสือเกี่ยวกับความปลอดภัย 3 เล่ม เป็นที่ปรึกษาในประเทศต่าง ๆ มากกว่า 25 ประเทศ และได้ช่วยเหลือให้องค์กรกว่า 350 แห่งสร้างแผนงานความตระหนักรู้และวัฒนธรรมความปลอดภัยเพื่อบริหารจัดการความเสี่ยงทางมนุษย์ขององค์กร Lance เป็นวิทยากรที่มีผลงานนำเสนออยู่เป็นประจำ เป็นผู้ชื่นชอบการทวีต (@lspitzner) และได้ร่วมงานโครงการความปลอดภัยชุมชนหลากหลายโครงการด้วยกัน ก่อนที่จะเข้ามาสู่แวดวงความปลอดภัยข้อมูลนั้น Lance ได้ทำงานเป็นนายทหารสัญญาบัตรอยู่ในกองเคลื่อนกำลังพลเร็วแห่งกองทัพบก (Army's Rapid Deployment Force) และได้รับ MBA จาก University of Illinois

เกี่ยวกับ SANS Institute

SANS Institute ก่อตั้งขึ้นมาในปี 1989 โดยก่อตั้งขึ้นมาเป็นองค์กรให้ความร่วมมือทางการวิจัยและการศึกษา SANS เป็นองค์กรที่ได้รับความไว้ใจสูงที่สุด และในขณะนี้ก็เป็นผู้ให้การอบรมเกี่ยวกับความปลอดภัยไซเบอร์ที่ใหญ่ที่สุด และให้การรับรองบุคลากรมืออาชีพทั้งในองค์กรรัฐบาลและองค์กรพาณิชย์ทั่วโลก วิทยากรของ SANS สอนหลักสูตรที่แตกต่างกันกว่า 60 หลักสูตรในงานฝึกอบรมความปลอดภัยไซเบอร์ กว่า 200 งานรวมถึงทางออนไลน์ GIAC เป็นกิจการในเครือของ SANS Institute ที่เป็นผู้ให้การรับรองคุณสมบัติของผู้ปฏิบัติการ ผ่านทางประกาศนียบัตรรับรองด้านความปลอดภัยทางไซเบอร์ ทางเทคนิคด้วยการใช้งานจริงกว่า 35 ฉบับ SANS Technology Institute ที่เป็นหน่วยงานย่อยอิสระในระดับภูมิภาคที่ให้ใบรับรองวุฒิได้ เป็นผู้เปิดสอนหลักสูตรปริญญามหาบัณฑิตด้านความปลอดภัยทางไซเบอร์ SANS นำเสนอแหล่งข้อมูลที่ไม่เสียค่าใช้จ่ายหลากหลายประเภทให้แก่ชุมชน InfoSec ซึ่งรวมถึงโครงการร่วม งานวิจัย รายงาน และจดหมายข่าว รวมทั้งยังเป็นผู้ปฏิบัติการระบบแจ้งเตือนล่วงหน้าของอินเตอร์เน็ต ซึ่งก็คือ Internet Storm Center ศูนย์กลางของ SANS ก็คือผู้ปฏิบัติการด้านความปลอดภัย เป็นตัวแทนขององค์กรต่าง ๆ ทั่วโลก นับตั้งแต่บริษัทไปจนถึงมหาวิทยาลัย ที่ร่วมกันทำงานเพื่อช่วยเหลือชุมชนความปลอดภัยข้อมูลทั้งหมด (https://www.sans.org)