Work From Home ให้ปลอดภัย...รอดพ้นจากภัยไซเบอร์ ตอนที่ 1

HIGHLIGHTS : ในโลกที่เผชิญความเสี่ยงจากภัยโควิด มาตรการสำคัญของการป้องกันคือ การแยกกันอยู่ห่างๆ ไม่ติดต่อกัน การทำงานที่บ้านจึงเป็นมาตรการสำคัญอย่างหนึ่งที่องค์กรนำมาใช้ ซึ่งอีกด้านหนึ่งที่ต้องเผชิญคือความเสี่ยงภัยจากโจรไซเบอร์ ทำให้ต้องเพิ่มมาตรการการบริหารความเสี่ยงให้เข้มงวด แต่มีความยากอยู่ที่ต้องเข้มงวดแบบยืดหยุ่นได้ด้วย ขณะเดียวกันยังต้องปรับตัวอย่างรวดเร็วให้ทันกับการเปลี่ยนแปลงของโลกและคู่แข่ง เพื่อให้ธุรกิจประสบผลสำเร็จตามเป้าหมาย บทความนี้จะบอกเล่าถึงวิธีการทำงานที่บ้านอย่างไร ให้ปลอดภัยกับทั้งตนเองและองค์กร

เวลาในการ 4 นาที

การทำงานที่บ้านเป็นมาตรการป้องกันการติดโควิดที่ดี แต่อีกด้านหนึ่งก็นำมาซึ่งความเสี่ยงที่สูงยิ่งขึ้นจากภัยโจรไซเบอร์ เนื่องจากภายในสำนักงานมักจะมีระบบควบคุมและรักษาความปลอดภัยที่มีมาตรการที่สูงกว่าเข้มงวดกว่าการทำงานจากที่บ้าน

บทความนี้ จึงขอนำเสนอการดูแลพื้นที่ทำงานที่บ้าน อุปกรณ์คอมพิวเตอร์ที่ใช้ เพื่อให้มั่นใจได้ว่า มีการควบคุมที่ดีเพียงพอและเหมาะสม ซึ่งเป็นการถอดความจากการบรรยายของคุณ **Rebecca Herold,** *CDPSE, FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI, Ponemon Institute Fellow CEO The Privacy Professor®, CEO Privacy & Security Brainiacs* ในหัวข้อ Security & Privacy Compliance in Work from Home Situations เมื่อวันที่ 6 สิงหาคม 2563 จัดโดย ISACA https://www.isaca.org/why-isaca/about-us ติดตามคุณรีเบคก้าได้ที่ Twitter ID: http://twitter.com/PrivacyProf

การรักษาความปลอดภัยของการทำงานที่บ้าน และอุปกรณ์ที่ใช้ แบ่งเป็น 12 เรื่อง ดังนี้

1. **การดูแลด้านความปลอดภัยและความเป็นส่วนตัว**

การทำงานที่บ้านไม่สามารถใช้การควบคุมโดยตรงกับพนักงานในพื้นที่ทำงานนอกสำนักงาน นอกจากนั้นในบ้านหรือห้องพัก ก็จะมีคนในครอบครัว รูมเมท เพื่อน เข้ามาใช้พื้นที่หรืออุปกรณ์คอมพิวเตอร์ร่วมกันในการทำงาน หรือ เรียนออนไลน์ แถมยังมีอุปกรณ์สมาร์ท IoT เชื่อมต่อเครือข่าย Wi-Fi ร่วมกัน ซึ่งเพิ่มความเสี่ยงต่อการรักษาความปลอดภัยและความเป็นส่วนตัวให้สูงขึ้น อาจจะมีการเข้าถึงข้อมูลขององค์กร เช่น ข้อมูลลูกค้า ข้อมูลพนักงาน โดยผู้ไม่ได้รับอนุญาต และอาจเกิดการรั่วไหลของข้อมูล รวมถึงความเสี่ยงที่ทำให้ระบบขัดข้องไม่สามารถดำเนินธุรกิจต่อเนื่อง

องค์กรจึงต้องทบทวนหรือกำหนดนโยบายการรักษาความปลอดภัยและความเป็นส่วนตัว ให้พนักงานถือปฏิบัติ ซึ่งรวมไปถึงพนักงานของบริษัทคู่ค้าที่ทำงานที่บ้านด้วย โดยเพิ่มเติมข้อมูลความเสี่ยงที่เกิดขึ้นใหม่จากสภาพแวดล้อมของการทำงานที่บ้านและนอกสำนักงาน นอกจากนั้นยังต้องมีการทบทวนแผนการกู้คืนจากภัยพิบัติและความต่อเนื่องทางธุรกิจ(แผน BCP) ให้ครอบคลุมการทำงานจากที่บ้านด้วย

2. ความท้าทายในการปฏิบัติให้ถูกต้อง

การให้ความรู้และฝึกอบรมถึงความเสี่ยงของการทำงานที่บ้าน นโยบายและวิธีปฏิบัติที่ถูกต้อง การส่งนโยบายให้พนักงานอ่านเอง โดยหวังว่าพนักงานจะเข้าใจ ปฏิบัติตามได้ มันอาจจะยากในโลกความจริง องค์กรจึงต้องให้ความสำคัญในการฝึกอบรมให้พนักงานเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและความเป็นส่วนตัว โดยอาจจะใช้การฝึกอบรมออนไลน์ การทำคลิปวิดีโอที่เข้าใจง่าย โดยทำเป็นประจำสม่ำเสมอและต่อเนื่อง

ในกรณีที่พบเหตุการณ์ที่ไม่ปฏิบัติตามนโยบาย ควรที่จะทำคลิปวิดีโอสั้นๆ หรือ การประชุมออนไลน์ หรือ ส่งข้อความ เพื่อแจ้งเตือนให้พนักงานทราบ เข้าใจและปฏิบัติตามนโยบายการรักษาความปลอดภัยและความเป็นส่วนตัวได้

นโยบายการทำงานที่บ้านนั้นรวมถึง การกำกับดูแลคู่ค้า ผู้ให้บริการบุคคลที่สาม และ supply chain เพราะบริษัทเหล่านี้ก็อาจให้พนักงานทำงานจากที่บ้านเช่นกัน ซึ่งมีความเสี่ยงต่อบริษัทเช่นเดียวกับการทำงานจากที่บ้านของพนักงาน

จำกัดการเข้าถึงข้อมูลให้เป็น "ขั้นต่ำที่จำเป็น" ดูแลให้การเข้าใช้งาน ใน Share file ให้เหมาะสม สิ่งที่น่ากังวลอย่างมากก็คือ มีการใช้พื้นที่และอุปกรณ์ร่วมกัน ซึ่งอาจทำให้ข้อมูลสำคัญรั่วไหลได้

การกู้คืนจากภัยพิบัติและความต่อเนื่องทางธุรกิจ อาจจะไม่มีการสำรองข้อมูลหรือไม่ได้ทำตามนโยบาย ซึ่งจะทำให้เกิดความเสี่ยงทำให้ระบบขัดข้องและธุรกิจขาดความต่อเนื่อง

ฝ่ายตรวจสอบภายใน ควรมีการตรวจสอบการปฏิบัติตามนโยบายการทำงานที่บ้าน

เคล็ดลับ!

ทำวิดีโอสั้น ๆ เพื่อแจ้งเตือน เกี่ยวกับนโยบายและขั้นตอนของความปลอดภัยและความเป็นส่วนตัวของการทำงานที่บ้าน

3. การเข้าถึงจากนอกสำนักงานและ Wi-Fi

นโยบายความปลอดภัยในการทำงานที่บ้าน ต้องระบุเกี่ยวกับ Wi-Fi ที่บ้าน ต้องมีการรักษาความปลอดภัยที่**เพียงพอ** ได้แก่

- ติดตั้ง Firewalls ให้ถูกต้อง
- การตั้งค่ามีความปลอดภัยและปฏิบัติตามนโยบายความปลอดภัย โดยเคร่งครัด
- มีการเข้ารหัส (encryption) หรือ ตั้งรหัสผ่านที่เดาได้ยาก (Strong Password)
- มีการควบคุมการเข้าถึง

  แฮ๊คเกอร์สามารถเจาะเข้าผ่าน Wi-fi ที่ตั้งค่าไม่ปลอดภัย เพื่อหาข้อมูล เช่น Operating System ที่ใช้ ประเภทของการเข้ารหัสที่ใช้ หรือ สามารถทราบด้วยว่า ข้อมูลไหนที่ส่งโดยไม่ใช้การเข้ารหัส ซึ่งแฮ๊คเกอร์สามารถใช้ข้อมูลเหล่านี้ไปใช้ประโยชน์และสร้างความเสียหายให้องค์กรได้

- Wi-Fi สาธารณะ
  - อย่าใช้ เว้นแต่จำเป็นจริงๆเท่านั้น
  - เมื่อจำเป็นให้ใช้การเข้ารหัสที่เข้าถึงได้ยาก(Strong Password)

- หลีกเลี่ยงการชาร์จไฟสาธารณะ ซึ่งอันตราย โจรไซเบอร์สามารถแฮ๊คข้อมูลผ่านสายที่เสียบชาร์จได้ ในกรณีจำเป็นต้องชาร์จไฟสาธารณะ ซึ่งบางครั้งจำเป็นจริงๆเลี่ยงไม่ได้ แนะนำให้ลงทุนซื้อ USB Data Blocker ซึ่งราคาไม่แพง ช่วยป้องกันโจรแฮ๊คเกอร์ ไวรัสมัลแวร์ และการขโมยข้อมูลได้

การตั้งค่าต่างๆที่ใช้ความรู้ทางเทคนิค

ควรมอบหมายให้ IT Support ทำหน้าที่ช่วยเหลือพนักงานให้เข้าใจและปฏิบัติได้ถูกต้อง และฝ่ายตรวจสอบภายในควรทำ Wi-fi Audit เพื่อให้มั่นใจว่า มีการปฏิบัติตามนโยบายการรักษาความปลอดภัย มาตรการบริหารความเสี่ยงที่ควรทำคือ พนักงานที่มีหน้าที่ดูแลข้อมูลที่มีความเสี่ยงสูง ต้องติดตั้ง Wi-Fi Business สำหรับใช้ทำงาน และแยกต่างหากจาก Wi-Fi บ้าน และแยกอุปกรณ์ IoT ที่ชาญฉลาด ไปใช้ Wi-Fi บ้าน เพื่อป้องกันไม่ให้แฮ๊คเกอร์เข้าถึงระบบของธุรกิจผ่านอุปกรณ์ IoT

โปรดให้ความสำคัญ และแจ้งเตือนพนักงานที่ทำงานที่บ้านที่อาจจะไปทำงานในห้องสมุด ร้านกาแฟ หรือ บางบริษัทอาจจะเช่าสำนักงานชั่วคราว หรือ Working space หรือ โรงแรม และให้พนักงานกระจายเข้าทำงานเพื่อลดความหนาแน่นในสำนักงาน โดยพนักงานต้องระวังไม่ใช้ Free Wi-Fi หรือ Wi-Fi ที่ใช้ ไอดี พาสเวิร์ด ร่วมกัน

เคล็ดลับ!

สำหรับโฮมออฟฟิศให้ตั้งค่าเครือข่าย wi-fi บ้านแยกต่างหาก จาก wi-fi ที่ใช้สำหรับธุรกิจ

4. การตรวจสอบยืนยันตัวตน

สภาพแวดล้อมในการทำงานที่บ้าน อาจจะทำให้พนักงานละเลย หลงลืม ไม่ได้ปฏิบัติตามการควบคุมที่เหมาะสม ปลอดภัย คิดว่าง่าย เร็วดี เพราะเชื่อว่าบ้านปลอดภัย ซึ่งเป็นความเสี่ยงขององค์กรเพราะไม่สามารถควบคุมโดยตรงได้ เหมือนกับในพื้นที่สำนักงาน สิ่งที่อาจเกิดขึ้น เช่น

- ไม่มีการฝึกอบรมที่ครอบคลุมการตรวจสอบและยืนยันตัวตน
- ไม่ได้กำหนดให้มีการตรวจสอบยืนยันตัวตน หรือ ตรวจสอบไม่เข้มงวดพอ ทำให้มีความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาตจากผู้ไม่หวังดี
- ใช้รหัสผ่านที่คาดเดาได้ (weak)
- มีการใช้รหัสผ่านร่วมกันกับคนที่บ้าน ไม่ว่าจะเป็นครอบครัว เพื่อนร่วมห้อง ที่ใช้งานพื้นที่หรืออุปกรณ์ร่วมกัน
- ขาดการรักษาความปลอดภัยของรหัสผ่าน แปะรหัสผ่านบนโต๊ะ ตู้เย็น บนเครื่องคอมพิวเตอร์
- ไม่ได้จำกัดจำนวนครั้งของการใส่รหัสผิด เพื่อป้องกันการพยายามเข้าสู่ระบบ
- ใช้รหัสผ่านเรื่องงานกับเรื่องส่วนตัวเป็นรหัสเดียวกัน ซื้อของออนไลน์ ดูหนัง บัญชีโซเชี่ยลมีเดียต่างๆ

- ช่องโหว่ของคนในการใช้ปัจจัยหลายๆอย่างตรวจสอบและยืนยันตัวบุคคล (Multi-Factor Authentication: MFA) MFA ยืนยันตัวตนโดยการใช้ปัจจัยหลายอย่าง ซึ่งน่าจะปลอดภัยขึ้น แต่ความเสี่ยงกลับเป็นเรื่องเดิม คือ ถูกหลอกให้บอกรหัสกับโจร ถูกโจรตก Phishing รหัสไป หลายท่านคงเคยได้อ่านข่าวที่คนถูกแฮ็คบัญชีไลน์ เฟสบุ๊ค ไอจี เหตุเกิดจากเมื่อได้รับข้อความจากเพื่อนในไลน์หรือเฟสบุ๊ค ขอเบอร์มือถือ บอกทำหายไป และสักพักก็บอกว่า มีข้อความเข้าในมือถือ ช่วยถ่ายรูปส่งมาให้หน่อย ผู้รับเห็นว่าเป็นเพื่อน กำลังยุ่งไม่ทันอ่านว่า ข้อความอะไร แต่เพื่อนต้องการใช้ด่วน ก็ส่งให้ ถึงตรงนี้ คงทายได้ว่า เพื่อนนั้นถูกแฮ็ค คนที่คุยนั้นเป็นโจรแฮ็คเกอร์ ข้อมูลส่งให้โจรคือ เบอร์มือถือ และ OTP ซึ่งทำให้มีข่าว เฟสบุ๊ค ไลน์ ไอจีถูกโจรแฮ็ค แล้วโจรปลอมตัวไปขอยืมเงินเพื่อนๆ ในเฟสบุ๊ค ไลน์ ไอจี และประกาศเตือนว่า บัญชีนี้ถูกแฮ็ค อย่าหลงเชื่อให้เงินไป

นโยบายการรักษาความปลอดภัยของการทำงานที่บ้าน ต้องกำหนดเรื่องการตรวจสอบยืนยันตัวตนข้างต้นเป็นมาตรฐานเดียวกับการทำงานในพื้นที่สำนักงาน มีการฝึกอบรมให้พนักงานเข้าใจและถือปฏิบัติตามได้ถูกต้อง

เคล็ดลับ!

กำหนดนโยบาย: ห้ามใช้รหัสผ่านของธุรกิจบนอุปกรณ์ภายในบ้าน ห้ามให้ครอบครัวหรือเพื่อนใช้รหัสผ่านของธุรกิจ ห้าม save รหัสบนเบราว์เซอร์ ห้ามเขียนรหัสผ่านกันลืมติดไว้ตามที่ต่างๆ

5. ซอฟต์แวร์และระบบปฏิบัติการการรักษาความปลอดภัย

นโยบายการรักษาความปลอดภัยของการทำงานที่บ้าน ต้องกำหนดให้ครอบคลุมถึงเรื่อง

- อัปเดตไฟร์วอลล์ Operating System ให้เป็นเวอร์ชั่นล่าสุด
- ลงโปรแกรมป้องกันมัลแวร์ที่ทำให้ธุรกิจหยุดชะงัก
- มาตรการป้องกันความเสี่ยงที่อุปกรณ์ IoT ที่หลากหลายเข้ากันไม่ได้ คุยกันไม่รู้เรื่อง ไม่เข้าใจ อาจทำให้ธุรกิจหยุดชะงักเนื่องจากความเข้ากันไม่ได้และการหยุดชะงักของ IoT

เคล็ดลับ!

ตรวจสอบให้แน่ใจว่าสิ่งต่อไปนี้ได้รับการอัปเดตให้เป็น version ล่าสุด:

- เว็บเบราว์เซอร์
- บัญชีการสนทนาออนไลน์ (Instant messaging clients)
- ซอฟต์แวร์การใช้ไฟล์ร่วมกัน
- แอพพลิเคชั่นของธุรกิจ
- แพลตฟอร์มการประชุมออนไลน์
- Email clients*
- Office productivity software
- โปรแกรมป้องกันไวรัส
- ไฟร์วอลล์ส่วนบุคคล

*Email Client เป็นโปรแกรมสำหรับจัดการข้อความเพื่อเปิดเช็คดูข้อมูลต่างๆ จากการ รับ/ส่งอีเมล์ จากผู้ให้บริการต่างๆ แทนตัวของ Web Browser โดยมีการทำงานคือ จะทำการโหลดอีเมล์ทุกฉบับที่มีการ รับ/ส่ง มาไว้ที่ตัวของโปรแกรม อีเมล์จะถูกจัดเก็บไว้ที่ตัวของโปรแกรม สามารถเปิดอ่านได้เมื่อเข้าใช้โปรแกรม โดยโปรแกรมจะมีฟังชั่นการจัดการ Email ในรูปแบบต่างๆ ต่างกันออกไปตามความเหมาะสม

5 เรื่องที่กล่าวไปแล้วนี้ ล้วนเป็นเรื่องสำคัญที่เกี่ยวข้องกับความปลอดภัยของการทำงานจากที่บ้าน และบางเรื่องเป็นสิ่งที่เราอาจคิดไม่ถึง หรือบางอย่างเราอาจละเลยไม่ได้ปฏิบัติอย่างเคร่งครัด ในตอนต่อไปจะกล่าวถึงอีก 7 เรื่อง มีเรื่องอะไรบางนั้น ติดตามกันต่อได้เลยค่ะ

ถอดความโดย วิภา ลี้ตระกูลนำชัย CIA CISA