



การรักษาความปลอดภัยขององค์กรของท่านทางออนไลน์

เหตุใดความปลอดภัยทางไซเบอร์จึงสำคัญต่อกลุ่มชุมชนและองค์กรต่าง ๆ?

หน้านี้มีคำแนะนำและขั้นตอนบางส่วนที่ท่านสามารถดำเนินการเพื่อปกป้องกลุ่มชุมชนหรือองค์กรของท่านจากภัยคุกคามความปลอดภัยทางไซเบอร์ นอกจากนี้ยังมีคำแนะนำเป็นการเฉพาะสำหรับบุคคลในการรักษาความปลอดภัยทางออนไลน์อีกด้วย

คำแนะนำนี้เนื่องจากภัยคุกคามที่พบเห็นได้บ่อยและร้ายแรงอย่างยิ่ง

การอัปเดต

อัปเดตซอฟต์แวร์อุปกรณ์สื่อสารอิเล็กทรอนิกส์ของท่านให้เป็นปัจจุบันเพื่ออุดช่องโหว่ด้านความปลอดภัย

- อัปเดตอุปกรณ์ของกลุ่มชุมชนหรือองค์กรของท่าน ได้แก่ โทรศัพท์ คอมพิวเตอร์ เราเตอร์ WiFi และอุปกรณ์อื่นใดที่สามารถเชื่อมต่ออินเทอร์เน็ต รวมถึงอุปกรณ์อัจฉริยะต่างๆ
- ถ้าเป็นไปได้ควรใช้การอัปเดตอัตโนมัติ

การตรวจสอบสองชั้น (2FA)

เพิ่มความปลอดภัยให้กับบัญชีของท่านโดยการใส่รหัสผ่านและเพิ่มเติมอีกหนึ่งขั้นตอน เช่น รหัสแอปในโทรศัพท์ของท่าน

- หมายเหตุ: เรียกอีกอย่างว่าการตรวจสอบสิทธิ์หลายชั้น (MFA) การยืนยันสองขั้นตอน (2SV) และเรียกขานแบบอื่นๆอีกหลายชื่อ
- เปิด 2FA ในบัญชีของกลุ่มชุมชนหรือองค์กรทั้งหมดของท่าน
- หากเป็นไปได้ ลองใช้ 2FA ที่ป้องกันการหลอกลวงทางออนไลน์ ซึ่งหมายความว่าท่านจะไม่หลงกลตกเป็นเหยื่อได้ อาจเป็นกุญแจความปลอดภัยทางกายภาพหรืออย่างอื่น เช่น ลายนิ้วมือหรือใบหน้าพิสูจน์ตัวตน

ติดตามบัญชีออนไลน์ของท่าน

ให้แน่ใจว่าติดตามสมาชิกไม่ได้รักษาสิทธิ์การเข้าถึงบัญชีของตนไว้หลังจากออกจากกลุ่มชุมชนหรือองค์กรแล้ว

- หากท่านมีมากกว่าหนึ่งบุคคลเข้าใช้บัญชีเดียวกัน ตรวจสอบให้แน่ใจว่าแต่ละบุคคลมีการเข้าสู่ระบบที่แตกต่างกันและทุกคนเปิดใช้งาน 2FA ด้วย
- จัดทำรายชื่อบัญชีผู้ใช้ทั้งหมด และปิดใช้งานบัญชีผู้ใช้ที่ไม่เกี่ยวข้อง เช่น เมื่อพนักงานลาออก
- จัดบันทึกอุปกรณ์ใดๆ ที่ท่านได้มอบให้แก่สมาชิกของท่าน และอย่าลืมรับคืนอุปกรณ์เหล่านั้นพร้อมกับรีเซ็ตเป็นค่าเดิมจากโรงงานที่ผลิต หากบุคคลนั้นออกจากองค์กร ท่านอาจจำเป็นต้องเปลี่ยนรหัสทางกายภาพในการเข้าออกอาคารด้วย

ตรวจสอบว่าบุคคลใดมีสิทธิ์เข้าถึงบัญชีออนไลน์ของท่าน

บุคคลในกลุ่มชุมชนหรือองค์กรของท่านควรจะสามารถเข้าถึงได้เฉพาะในสิ่งที่บุคคลดังกล่าวต้องการเท่านั้น

- หากบัญชีของบุคคลหนึ่งถูกเจาะข้อมูล ขั้นตอนเหล่านี้จะช่วยบรรเทาอันตรายที่ผู้ร้ายอาจก่อขึ้นได้
- ตรวจสอบและลบสิทธิ์ที่ไม่จำเป็นอย่างสม่ำเสมอ
- หากท่านมีบัญชี "ผู้ดูแลระบบ" บัญชีเดียวที่ผู้ใช้หลายคนใช้ ควรตรวจสอบกิจกรรมที่ผิดปกติ พยายามหลีกเลี่ยงการใช้บัญชีประเภทนี้ โดยเฉพาะสำหรับการใช้งานรายวัน
- กฎเหล่านี้ยังใช้ได้กับการเข้าถึงอุปกรณ์ของผู้ดูแลระบบ เช่น เราเตอร์

ตรวจสอบสัญญาของท่านกับผู้ให้บริการ

หากท่านได้จ้างบุคคลใดๆดูแลบริการไอทีแก่ท่าน

- ตรวจสอบให้แน่ใจว่ามีการป้องกันความปลอดภัยทางไซเบอร์เพื่อตอบสนองความต้องการของกลุ่มชุมชนหรือองค์กรของท่าน

พิจารณาว่าบัญชีและระบบทั้งหมดของท่านทำงานร่วมกันอย่างไร

ความเข้าใจการเชื่อมต่อจะช่วยให้ท่านทราบว่าผู้ร้ายสามารถเจาะข้อมูลทางใดได้บ้าง

- ตรวจสอบการเชื่อมต่อระหว่างระบบของท่าน เช่น อีเมล คลังเก็บข้อมูลในคลาวด์ และแพลตฟอร์มบัญชี
- พิจารณาใช้เครือข่ายส่วนตัวเสมือน (VPN) เพื่อความปลอดภัยทางออนไลน์เป็นพิเศษ การใช้ VPN จะช่วยซ่อนกิจกรรมออนไลน์ของท่านจากบุคคลใดก็ตามที่อาจพยายามติดตามท่าน ถือเป็นเรื่องดีอย่างยิ่งหากสมาชิกในกลุ่มชุมชนหรือองค์กรของท่านเชื่อมต่อจากระยะไกล

รณรงค์ให้บุคลากรของท่านมีความ "ชาญฉลาดในโลกไซเบอร์"

สมาชิกในกลุ่มชุมชนหรือองค์กรของท่านมีแนวโน้มที่จะตกเป็นเป้าหมายการโจมตีมากกว่าระบบของท่าน

- ฝึกอบรมพนักงานทุกคนเกี่ยวกับความปลอดภัยทางไซเบอร์ขั้นพื้นฐาน เว็บไซต์ [Own Your Online](#) เว็บไซต์ [Own Your Online | NCSC](#) มีคำแนะนำและเคล็ดลับมากมายเพื่อช่วยให้ท่านปลอดภัยในโลกออนไลน์และวิธีการตรวจจับการหลอกลวง
- เดือนบุคลากรว่ามีความสำคัญต่อบัญชีส่วนบุคคลของจนรวมถึงบัญชีที่บุคคลเหล่านั้นใช้ในองค์กรของท่านด้วย

- [เรายังมีคำแนะนำสำหรับรายบุคคลในการรักษาความปลอดภัยทางออนไลน์อีกด้วย](#)

วางแผนรับมือกับเหตุการณ์

การมีแผนรองรับถือเป็นสิ่งสำคัญเพื่อป้องกันมิให้บุคคลตื่นตระหนกเมื่อเกิดเหตุการณ์ขึ้น

- แผนรองรับเหตุการณ์จะระบุว่าใครมีหน้าที่ใดบ้างในระหว่างเกิดเหตุการณ์ มีเทมเพลตบริการที่ [การจัดการกับเหตุการณ์ | NCSC](#)
- รวมแผนว่าจะต้องปฏิบัติอย่างไรหากโทรศัพท์ คอมพิวเตอร์ หรือระบบอื่น ๆ ล้มเหลว อัปเดตแผนดังกล่าวอยู่เสมอ
- เก็บรายละเอียดการติดต่อของทุกคนที่จำเป็นและสำรองรายละเอียดไว้หากช่องทางหลักในการติดต่อใช้งานไม่ได้ (เช่น อีเมล)
- เก็บแผนไว้ ณ ที่หนึ่งที่ไม่โดนระบบของท่านด้วย ในกรณีที่ท่านไม่สามารถเข้าถึงได้