Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

คู่มือการรักษาความปลอดภัยทางไซเบอร์สำหรับธุรกิจขนาดเล็ก

ความซับซ้อนของเนื้อหา
เรียบง่าย ● ○ ○

cyber.gov.au

คำนำ

สำหรับธุรกิจขนาดเล็ก แม้แต่เหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์เพียงเล็กน้อยก็อาจส่งผลกระทบที่ร้ายแรงได้

คู่มือนี้ประกอบด้วยมาตรการรักษาความปลอดภัยขั้นพื้นฐานเพื่อช่วยปกป้องธุรกิจของคุณจากภัยคุกคามด้านความปลอดภัยทางไซเบอร์ทั่วไป เพื่อเป็นการเริ่มต้น เราขอแนะนำมาตรการสามประการดังนี้

- **เปิดใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย**
- **อัปเดตซอฟต์แวร์ของคุณ**
- **สำรองข้อมูลของคุณ**

คู่มือนี้อาจพูดถึงมาตรการที่ไม่เกี่ยวข้องกับธุรกิจของคุณ หรือธุรกิจของคุณอาจมีความต้องการที่ซับซ้อนมากกว่า หลังจากทำตามคู่มือนี้แล้ว เราขอแนะนำให้ธุรกิจขนาดเล็กนำความสมบูรณ์ระดับหนึ่ง (Maturity Level One) ของหลักการจำเป็นแปดประการมาใช้งานด้วย หากคุณมีคำถามเกี่ยวกับคำแนะนำนี้หรือความปลอดภัยทางไซเบอร์ในเนื้อหาที่ กว้างกว่านี้เราขอแนะนำให้คุณพูดคุยกับผู้เชี่ยวชาญด้านไอที หรือที่ปรึกษาที่เชื่อถือได้

เยี่ยมชมเว็บไซต์ cyber.gov.au เพื่ออ่านคู่มือฉบับเต็มของเรา รวมถึงคำแนะนำวิธีการสำหรับแต่ละมาตรการ

สารบัญ

ภัยคุกคามต่อธุรกิจขนาดเล็ก 4

ข้อความสแกม 4

การโจมตีทางอีเมล 5

ซอฟต์แวร์ที่เป็นอันตราย 6

รักษาความปลอดภัยบัญชีผู้ใช้ของคุณ 7

เปิดใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย 7

ใช้รหัสผ่านหรือข้อความรหัสผ่านที่รัดกุม 7

จัดการบัญชีที่ใช้ร่วมกัน 7

ใช้งานการควบคุมการเข้าถึง 7

ปกป้องอุปกรณ์และข้อมูลของคุณ 8

อัปเดตซอฟต์แวร์ของคุณ 8

สำรองข้อมูลของคุณ 8

ใช้ซอฟต์แวร์รักษาความปลอดภัย 8

รักษาความปลอดภัยเครือข่ายและบริการภายนอกของคุณ 9

ทำให้เว็บไซต์ของคุณยากต่อการโจมตี 9

รีเซ็ตอุปกรณ์ของคุณก่อนขายหรือกำจัดทิ้ง 9

ล็อกและเก็บรักษาอุปกรณ์ของคุณให้ปลอดภัย 10

ปกป้องข้อมูลทางธุรกิจของคุณ 10

เตรียมความพร้อมให้พนักงานของคุณ 11

ให้ความรู้แก่พนักงาน 11

จัดทำแผนฉุกเฉิน 11

คอยติดตามข้อมูลอยู่เสมอ 11

ภัยคุกคามต่อธุรกิจขนาดเล็ก

ข้อความสแกม

สแกมเป็นวิธีทั่วไปที่อาชญากรไซเบอร์มุ่งเป้าไปที่ธุรกิจขนาดเล็ก เป้าหมายของพวกเขาคือการหลอกลวงคุณหรือพนักงานของคุณให้ทำการดังนี้

- การส่งเงินหรือบัตรของขวัญ
- การคลิกที่ลิงก์หรือเอกสารแนบที่เป็นอันตราย
- การให้ข้อมูลที่สำคัญ เช่น รหัสผ่าน

อาชญากรไซเบอร์อาจพยายามหลอกลวงธุรกิจของคุณผ่านอีเมล ข้อความตัวอักษร โทรศัพท์ และโซเชียลมีเดีย สแกมเมอร์มักจะแสร้งทำเป็นบุคคลหรือองค์กรที่คุณไว้วางใจ

การโจมตีแบบฟิชชิ่ง (Phishing Attacks)

สิ่งน่ากังวลโดยเฉพาะสำหรับธุรกิจขนาดเล็กคือ **การโจมตีแบบฟิชชิ่ง** สแกมเหล่านี้มักจะมีลิงก์ไปยังเว็บไซต์ปลอมที่คุณได้รับการชักชวนให้เข้าสู่ระบบบัญชีหรือให้ป้อนรายละเอียดที่เป็นความลับ

โดยปกติแล้ว การโจมตีแบบฟิชชิ่งมักมองหาช่องโหว่เพื่อเข้าถึงรหัสผ่านบัญชีผู้ใช้ของคุณ อาชญากรไซเบอร์มักใช้วิธีนี้ในการ "ครอบครอง" บัญชีโซเชียลมีเดียของธุรกิจขนาดเล็กและยึดไว้เพื่อเรียกค่าไถ่

วิธีการบรรเทาปัญหา

หากมีข้อความมาจากหน่วยงานที่รู้จักและดูน่าสงสัย ให้ใช้ความระมัดระวัง ติดต่อบุคคลหรือธุรกิจทางช่องทางอื่นเพื่อตรวจสอบว่าข้อความนั้นถูกต้องเป็นทางการหรือไม่ ใช้รายละเอียดการติดต่อที่คุณพบผ่านแหล่งที่มาที่ถูกต้อง เช่น โดยการเยี่ยมชมเว็บไซต์อย่างเป็นทางการของธุรกิจ และไม่ใช่ข้อมูลที่อยู่ในข้อความที่น่าสงสัย

เรียนรู้เพิ่มเติมเกี่ยวกับการระบุสแกมและการโจมตีแบบฟิชชิ่งด้วยแหล่งข้อมูลต่อไปนี้

- รู้จักจำแนกและรายงานสแกม
- เรียนรู้วิธีการตรวจจับสแกมแบบฟิชชิ่ง
- การตรวจจับข้อความที่เนื้อหาใช้วิธีวิศวกรรมสังคม

กรณีศึกษา

พนักงานของบริษัทขนส่งได้รับอีเมลจากผู้บริหารคนหนึ่ง โดยขอให้ซื้อบัตรเครดิต MasterCard แบบเติมเงินมูลค่า 6 x 500 ดอลลาร์ ผู้บริหารบอกให้เธอเก็บเรื่องนี้ไว้เป็นความลับ เนื่องจากจะใช้บัตรเหล่านี้เป็นบัตรกำนัลสำหรับพนักงาน เมื่อซื้อแล้ว พนักงานจะต้องถ่ายภาพบัตรทั้งสองด้านและส่งให้ผู้บริหารเพื่อเป็นหลักฐานการซื้อ

ตามที่ได้รับคำสั่งงานมา พนักงานไปยังที่ทำการไปรษณีย์และใช้บัตรเครดิตส่วนตัวของเธอซื้อบัตรของขวัญ เธอตอบกลับอีเมลของผู้บริหารและส่งภาพถ่ายบัตรของขวัญเป็นหลักฐาน

หลังจากกลับมาจากที่ทำการไปรษณีย์ พนักงานได้มอบบัตรตัวจริงให้แก่ผู้บริหาร ซึ่งไม่รู้เรื่องบัตรเหล่านั้นเลย จากการตรวจสอบ **อีเมลทั้งหมดเกี่ยวกับบัตรของขวัญมาจากที่อยู่อีเมลแบบสุ่มและไม่ได้มาจากบัญชีอีเมลที่ถูกต้องเป็นทางการของผู้บริหาร นี่เป็นการสแกมแบบหนึ่ง**

การโจมตีทางอีเมล

นอกจากการสแกมแบบฟิชชิ่งแล้ว การโจมตีทางอีเมลโดยทั่วไปที่กระทำต่อธุรกิจขนาดเล็กเรียกว่า **การโจมตีผ่านอีเมลธุรกิจ** (Business Email Compromise - BEC) อาชญากรอาจปลอมตัวเป็นตัวแทนธุรกิจโดยใช้บัญชีอีเมลที่ถูกโจมตีมาหรือที่ได้รับมาด้วยวิธีอื่น เช่น การใช้ชื่อโดเมนที่ดูคล้ายกับธุรกิจจริง นอกเหนือจากการขโมยข้อมูลแล้ว เป้าหมายของการโจมตีเหล่านี้มักจะเป็นการหลอกลวงเหยื่อให้ส่งเงินไปยังบัญชีธนาคารที่มีสแกมเมอร์เป็นเจ้าของดำเนินการ

วิธีการบรรเทาปัญหา

การป้องกันการโจมตีทางอีเมลที่ดีที่สุดคือการฝึกอบรมและการสร้างความตระหนักให้กับพนักงานของคุณ ตรวจสอบให้แน่ใจว่าพนักงานของคุณทราบอยู่เสมอว่าควรระมัดระวังอีเมลต่อไปนี้

- อีเมลที่ขอให้ชำระเงินโดยเฉพาะหากเร่งด่วนหรือเกินกำหนด
- อีเมลที่มีการเปลี่ยนแปลงรายละเอียดธนาคาร
- ที่อยู่อีเมลที่ดูไม่ถูกต้องนัก เช่น ชื่อโดเมนไม่ตรงกับชื่อบริษัทของซัพพลายเออร์

แม้ว่าการโจมตีเหล่านี้อาจสร้างความเสียหายได้ แต่มาตรการบรรเทาปัญหาก็ทำได้ง่ายและแทบไม่มีค่าใช้จ่ายเลย **เมื่อพนักงานได้รับอีเมลในลักษณะนี้ วิธีบรรเทาปัญหาที่มีประสิทธิผลที่สุดคือ การโทรหาผู้ส่งเพื่อยืนยันว่าอีเมลเหล่านั้นถูกต้องเป็นทางการหรือไม่** อย่าใช้รายละเอียดการติดต่อในข้อความที่คุณได้รับเนื่องจากอาจเป็นการหลอกลวงได้ แนะนำกระบวนการที่เป็นทางการเพื่อให้พนักงานปฏิบัติตามเมื่อได้รับคำขอให้ชำระเงินหรือมีการเปลี่ยนแปลงรายละเอียดธนาคาร

เรียนรู้วิธีปกป้องธุรกิจของคุณจากการสแกมแบบ BEC และการโจมตีผ่านอีเมลด้วยแหล่งข้อมูลต่อไปนี้

- การโจมตีผ่านอีเมลธุรกิจ
- ปกป้องธุรกิจของคุณจากการหลอกลวงและการโจมตีผ่านอีเมล
- สิ่งที่ต้องทำหากธุรกิจของคุณตกเป็นเป้าหมายของการหลอกลวงและการโจมตีผ่านอีเมล

กรณีศึกษา

ธุรกิจก่อสร้างขนาดเล็กได้รับอีเมลจากซัพพลายเออร์โดยแจ้งว่าได้เปลี่ยนธนาคารแล้ว ซัพพลายเออร์ให้รายละเอียดบัญชีใหม่สำหรับการชำระเงินตามใบแจ้งหนี้ เนื่องจากอีเมลดูเหมือนถูกต้องเป็นทางการ **ธุรกิจก่อสร้างจึงไม่ได้โทรหาซัพพลายเออร์เพื่อยืนยันการเปลี่ยนแปลงในรายละเอียดบัญชีธนาคาร**

ธุรกิจได้ชำระเงินตามใบแจ้งหนี้จากซัพพลายเออร์เป็นเงินกว่า 70,000 ดอลลาร์ วันต่อมา พนักงานอีกคนชำระเงินตามใบแจ้งหนี้เดิมอีกครั้งผิดพลาดโดยไม่ได้ตั้งใจเป็นเงินกว่า 70,000 ดอลลาร์ โดยรวมแล้วมีการจ่ายเงินมากกว่า 150,000 ดอลลาร์ไปยังบัญชีธนาคารใหม่

เมื่อธุรกิจโทรหาซัพพลายเออร์เพื่อสอบถามว่าสามารถเรียกคืนเงินที่ชำระซ้ำกันได้หรือไม่ ซัพพลายเออร์แจ้งว่ารายละเอียดธนาคารเหล่านั้นไม่ถูกต้อง จึงมีการเริ่มต้นสอบสวนขึ้นมาทันที และซัพพลายเออร์พบว่าหนึ่งในบัญชีอีเมลของพวกเขาถูกแฮ็กและมีการส่งรายละเอียดบัญชีธนาคารที่หลอกลวงออกไปให้ลูกค้า **เงินที่ชำระไปไม่สามารถกู้คืนได้**

ซอฟต์แวร์ที่เป็นอันตราย

มัลแวร์ (Malware) เป็นคำที่ครอบคลุมสำหรับซอฟต์แวร์ที่เป็นอันตรายซึ่งออกแบบมาเพื่อก่อให้เกิดความเสียหาย เช่น แรนซัมแวร์ (Ransomware) ไวรัส (Virus) สปายแวร์ (Spyware) และโทรจัน (Trojan) มัลแวร์สามารถ

- ขโมยหรือล็อกไฟล์บนอุปกรณ์ของคุณ
- ขโมยหมายเลขธนาคารหรือบัตรเครดิตของคุณ
- ขโมยชื่อผู้ใช้และรหัสผ่านของคุณ
- เข้าควบคุมหรือทำการสอดแนมคอมพิวเตอร์ของคุณ

มัลแวร์อาจทำให้อุปกรณ์ของคุณหยุดทำงานอย่างปกติ ลบไฟล์หรือทำให้ไฟล์ของคุณเสียหาย หรืออนุญาตให้คนอื่นเข้าถึงข้อมูลส่วนตัวหรือข้อมูลทางธุรกิจของคุณได้ หากอุปกรณ์ของคุณติดมัลแวร์ คุณอาจเสี่ยงต่อการโจมตีอื่น ๆ มัลแวร์อาจแพร่กระจายไปยังอุปกรณ์อื่น ๆ บนเครือข่ายของคุณได้

อุปกรณ์ของคุณอาจติดมัลแวร์ได้หลายวิธีได้แก่

- การเยี่ยมชมเว็บไซต์ที่ติดมัลแวร์
- การดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่ติดมัลแวร์จากอินเทอร์เน็ต
- การเปิดเอกสารแนบอีเมลที่ติดมัลแวร์

แรนซัมแวร์ (Ransomware)

แรนซัมแวร์เป็นมัลแวร์ที่พบได้ทั่วไปและเป็นอันตราย ซึ่งทำงานโดยการล็อกหรือเข้ารหัสไฟล์ของคุณเพื่อทำให้คุณไม่สามารถเข้าถึงไฟล์ได้อีกต่อไป มีการเรียกค่าไถ่เพื่อคืนสภาพใช้งานได้ให้ไฟล์ ซึ่งโดยปกติแล้วจะเรียกในรูปสกุลเงินดิจิตัล อาชญากรไซเบอร์ยังอาจขู่ว่าจะเผยแพร่หรือขายข้อมูลออนไลน์ เว้นแต่ว่าจะมีการจ่ายเงินค่าไถ่

วิธีการบรรเทาปัญหา

แม้ว่าซอฟต์แวร์ป้องกันไวรัสหรือซอฟต์แวร์รักษาความปลอดภัยจะสามารถช่วยปกป้องคุณจากมัลแวร์ได้ แต่ไม่มีซอฟต์แวร์ใดที่มีประสิทธิผลถึง 100 เปอร์เซ็นต์ พนักงานต้องให้ความระมัดระวังกับอีเมล เว็บไซต์ และการดาวน์โหลดไฟล์ และยังต้องอัปเดตอุปกรณ์ของตนเป็นประจำเพื่อให้ปลอดภัยอยู่เสมอ

ดูแหล่งข้อมูลต่อไปนี้สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการปกป้องธุรกิจของคุณจากแรนซัมแวร์

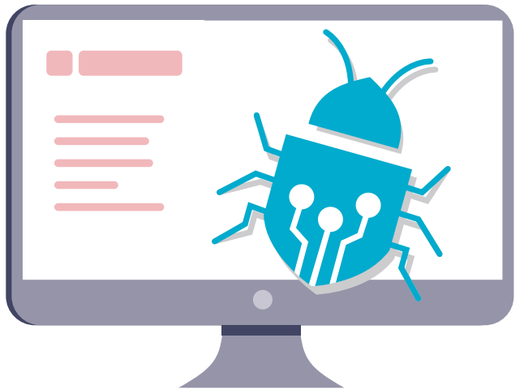
- แรนซัมแวร์ (Ransomware)
- ปกป้องตัวคุณเองจากการโจมตีของแรนซัมแวร์
- จะทำอย่างไรถ้าคุณถูกเรียกค่าไถ่

กรณีศึกษา

พนักงานของร้านอะไหล่รถยนต์มาทำงานในตอนเช้าวันหนึ่งและไม่สามารถบูตคอมพิวเตอร์เซิร์ฟเวอร์ได้ เมื่อผู้ให้บริการไอทีเข้าถึงเซิร์ฟเวอร์ พวกเขาพบหน้าต่างที่เปิดอยู่ ซึ่งระบุว่าข้อมูลคอมพิวเตอร์ทั้งหมดได้รับการเข้ารหัสไว้แล้ว ข้อความนั้นเรียกร้องให้พวกเขาจ่ายเงินค่าไถ่เป็นบิตคอยน์ (Bitcoin) เพื่อปลดล็อกไฟล์

มีไดรฟ์สำรองที่เสียบเข้ากับคอมพิวเตอร์ซึ่งถูกเข้ารหัสไว้ด้วย พวกเขาพยายามเชื่อมต่อกับไดรฟ์สำรองข้อมูลเพิ่มเติม แต่ไฟล์ถูกเข้ารหัสโดยอัตโนมัติภายในไม่กี่วินาที **พวกเขาไม่สามารถลบแรนซัมแวร์ก่อนที่จะพยายามกู้คืนข้อมูลและสูญเสียไฟล์สำรองข้อมูลทุกไฟล์ที่พวกเขามี**

ทางเลือกเดียวที่เหลือคือ การรีเซ็ตเซิร์ฟเวอร์ให้เป็นการตั้งค่าจากโรงงานและเริ่มต้นด้วยระบบใหม่ ธุรกิจของพวกเขาสูญเสียข้อมูลที่สะสมมาหลายปีและต้องเริ่มต้นใหม่ทั้งหมด



รักษาความปลอดภัยบัญชีผู้ใช้ของคุณ

เปิดใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย

การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) ทำให้อาชญากรไซเบอร์เข้าถึงบัญชีผู้ใช้ของคุณได้ยากขึ้น

MFA เป็นการเพิ่มความปลอดภัยอีกชั้นหนึ่งให้กับบัญชีผู้ใช้ของคุณ นี่เป็นหนึ่งในวิธีที่มีประสิทธิผลที่สุดในการปกป้องบัญชีผู้ใช้ของคุณจากการเข้าถึงของบุคคลอื่น ดังนั้นคุณควรใช้วิธีนี้ในทุกที่ที่เป็นไปได้ ใครก็ตามที่เข้าสู่ระบบบัญชีผู้ใช้ของคุณจะต้องให้ข้อมูลอื่นนอกเหนือจากชื่อผู้ใช้และรหัสผ่านของคุณ ซึ่งอาจเป็นรหัสเฉพาะจากข้อความตัวอักษรหรือแอปยืนยันตัวตน สำหรับข้อมูลเพิ่มเติม โปรดอ่านคำแนะนำเกี่ยวกับ MFA ของเราที่ cyber.gov.au/mfa.

✓ **เปิดใช้งาน MFA ทุกครั้งที่ทำได้ โดยเริ่มจากบัญชีผู้ใช้ที่สำคัญที่สุดของคุณก่อน**

ใช้งานการควบคุมการเข้าถึง

การจำกัดการเข้าถึงของผู้ใช้สามารถจำกัดความเสียหายที่เกิดจากเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ได้

การควบคุมการเข้าถึงเป็นวิธีหนึ่งในการจำกัดการเข้าถึงไฟล์และระบบบางอย่าง โดยทั่วไป พนักงานไม่จำเป็นต้องเข้าถึงข้อมูล บัญชี และระบบทั้งหมดในธุรกิจอย่างเต็มรูปแบบ พวกเขาควรได้รับอนุญาตให้เข้าถึงเฉพาะสิ่งที่จำเป็นต่อการปฏิบัติหน้าที่เท่านั้น

การจำกัดการเข้าถึงจะช่วยจำกัดความเสียหายที่เกิดจากเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ ตัวอย่าง เช่น ด้วยการควบคุมการเข้าถึงที่เหมาะสม หากคอมพิวเตอร์ของพนักงานติดมัลแวร์เรียกค่าไถ่ อาจส่งผลกระทบต่อไฟล์จำนวนน้อยแทนที่จะส่งผลกระทบต่อธุรกิจทั้งหมด

✓ **ตรวจสอบให้แน่ใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงเฉพาะสิ่งที่จำเป็นสำหรับหน้าที่ของตนเท่านั้น**

ใช้รหัสผ่านหรือข้อความรหัสผ่านที่รัดกุม

ปกป้องบัญชีผู้ใช้ของคุณจากอาชญากรไซเบอร์ด้วยรหัสผ่านหรือข้อความรหัสผ่านที่ปลอดภัย

ธุรกิจขนาดเล็กจำนวนมากต้องเผชิญกับการโจมตีทางไซเบอร์อันเป็นผลมาจากพฤติกรรมการใช้รหัสผ่านที่ไม่ปลอดภัยพอ ตัวอย่างเช่น การใช้รหัสผ่านชุดเดียวซ้ำกันหลายบัญชี คุณสามารถใช้แอปจัดการรหัสผ่านและข้อความรหัสผ่านเพื่อสร้างรหัสผ่านที่รัดกุมได้

แอปจัดการรหัสผ่านทำหน้าที่เป็นตู้เซฟเสมือนจริงให้กับรหัสผ่านของคุณ คุณสามารถใช้มันเพื่อสร้างและจัดเก็บรหัสผ่านที่รัดกุมและ**ไม่ซ้ำกัน**สำหรับแต่ละบัญชีของคุณ หากคุณมีบัญชีจำนวนมาก การทำเช่นนี้จะเป็นการขจัดภาระในการจดจำรหัสผ่านที่ไม่ซ้ำกัน คุณไม่จำเป็นต้องจดจำรหัสผ่านหรือบัญชีที่เป็นของรหัสผ่านนั้น ๆ เนื่องจากรหัสผ่านจะถูกบันทึกไว้ในแอปจัดการรหัสผ่านของคุณ

สำหรับบัญชีที่คุณลงชื่อเข้าใช้เป็นประจำหรือที่คุณไม่ต้องการเก็บไว้ในแอปจัดการรหัสผ่าน ให้คุณพิจารณาใช้ข้อความรหัสผ่านเป็นรหัสผ่านของคุณแทน ข้อความรหัสผ่านคือการรวมกันของคำแบบสุ่ม เช่น 'crystal onion clay pretzel' ซึ่งจะมีประโยชน์เมื่อคุณต้องการรหัสผ่านที่ปลอดภัยซึ่งจำได้ง่าย ใช้การผสมคำแบบสุ่มตั้งแต่สี่คำขึ้นไปและเป็นเอกลักษณ์ไม่ซ้ำกัน - **อย่าใช้ข้อความรหัสผ่านชุดเดิม**ซ้ำกันหลายบัญชี สำหรับข้อมูลเพิ่มเติมโปรดอ่านคำแนะนำของเราเกี่ยวกับแอปจัดการรหัสผ่านและข้อความรหัสผ่านได้ที่ cyber.gov.au/passphrases

✓ **ใช้แอปจัดการรหัสผ่านเพื่อสร้างและจัดเก็บรหัสผ่านให้เป็นเอกลักษณ์ไม่ซ้ำกันสำหรับแต่ละบัญชีที่สำคัญของคุณ**

จัดการบัญชีที่ใช้ร่วมกัน

การใช้บัญชีร่วมกันอาจส่งผลกระทบต่อความปลอดภัยและทำให้ยากต่อการติดตามกิจกรรมที่เป็นอันตรายได้

ในธุรกิจขนาดเล็กอาจมีเหตุผลที่สมควรที่ทำให้พนักงานต้องใช้บัญชีร่วมกัน แต่ควรหลีกเลี่ยงการทำเช่นนี้ให้มากที่สุดเท่าที่จะเป็นไปได้ เมื่อพนักงานหลายคนใช้บัญชีเดียวกัน อาจเป็นเรื่องยากที่จะติดตามกิจกรรมกลับไปหาพนักงานคนใดคนหนึ่งได้ และเป็นเรื่องที่ยากกว่าที่จะติดตามอาชญากรไซเบอร์ที่จะโจมตีเข้ามา นอกจากนี้ ยกเว้นคุณจะเปลี่ยนรหัสผ่าน พนักงานยังสามารถเข้าถึงบัญชีต่อไปได้แม้หลังจากที่ออกจากธุรกิจไปแล้ว

✓ **จำกัดการใช้บัญชีที่ใช้ร่วมกันและรักษาความปลอดภัยให้กับบัญชีใด ๆ ในธุรกิจของคุณ**

ปกป้องอุปกรณ์และข้อมูลของคุณ

อัปเดตซอฟต์แวร์ของคุณ

การอัปเดตซอฟต์แวร์ของคุณให้เป็นปัจจุบันอยู่เสมอเป็นหนึ่งในวิธีที่ดีที่สุดในการปกป้องธุรกิจของคุณจากการโจมตีทางไซเบอร์

การอัปเดตสามารถแก้ไขข้อบกพร่องด้านความปลอดภัยในระบบปฏิบัติการและซอฟต์แวร์อื่น ๆ ของคุณซึ่งทำให้อาชญากรไซเบอร์โจมตีเข้าระบบได้ยากขึ้น มีการค้นพบข้อบกพร่องใหม่ ๆ อยู่ตลอดเวลา ดังนั้นอย่าละเลยการแจ้งเตือนให้อัปเดต การอัปเดตซอฟต์แวร์ของคุณเป็นประจำจะช่วยลดโอกาสที่อาชญากรไซเบอร์จะใช้จุดอ่อนที่รู้จักเพื่อเรียกใช้มัลแวร์หรือแฮ็กอุปกรณ์ของคุณ หากคุณต้องการความช่วยเหลือ ดูคำแนะนำที่ ACSC เผยแพร่เกี่ยวกับการอัปเดตได้

หากอุปกรณ์หรือซอฟต์แวร์ของคุณเก่าเกินไป อาจไม่มีการอัปเดตที่สามารถนำมาใช้ได้ หากผู้ผลิตหยุดสนับสนุนผลิตภัณฑ์ด้วยการอัปเดตแล้ว คุณควรพิจารณาอัปเกรดเป็นผลิตภัณฑ์ใหม่เพื่อให้มีความปลอดภัยอยู่เสมอ ตัวอย่างของระบบที่ไม่ได้รับการอัปเดตที่สำคัญอีกต่อไป ได้แก่ iPhone 7 และ Microsoft Windows 7

สำหรับข้อมูลเพิ่มเติมโปรดอ่าน คำแนะนำเกี่ยวกับการอัปเดตของเราที่ cyber.gov.au/updates

✓ **เปิดการอัปเดตอัตโนมัติสำหรับอุปกรณ์และซอฟต์แวร์ของคุณ**

ใช้ซอฟต์แวร์รักษาความปลอดภัย

ซอฟต์แวร์รักษาความปลอดภัย เช่น ซอฟต์แวร์ป้องกันไวรัสและแรนซัมแวร์สามารถช่วยปกป้องอุปกรณ์ของคุณได้

ใช้ซอฟต์แวร์รักษาความปลอดภัยเพื่อตรวจจับและลบมัลแวร์ออกจากอุปกรณ์ของคุณ ซอฟต์แวร์ป้องกันไวรัสสามารถตั้งค่าให้สแกนหาไฟล์และโปรแกรมที่น่าสงสัยเป็นประจำได้ เมื่อพบการคุกคาม คุณจะได้รับการแจ้งเตือนและไฟล์ที่น่าสงสัยจะถูกกักกันไว้หรือลบออกไป

ธุรกิจขนาดเล็กจำนวนมากสามารถใช้**การรักษาความปลอดภัยของ Windows** เพื่อป้องกันตนเองจากไวรัสและมัลแวร์ได้ Windows Security มีให้มาอยู่แล้วภายในอุปกรณ์ Windows 10 และ Windows 11 และมีการป้องกันไวรัสและภัยคุกคามให้ฟรี คุณยังสามารถใช้เพื่อเปิดคุณสมบัติการป้องกันแรนซัมแวร์บนอุปกรณ์ของคุณได้อีกด้วย

สำหรับผลิตภัณฑ์ทางเลือกและตัวเลือกอื่น ๆ อ่านคำแนะนำเกี่ยวกับซอฟต์แวร์ป้องกันไวรัส โดยการค้นหาคำว่า *antivirus* ที่เว็บไซต์ cyber.gov.au

✓ **ตั้งค่าซอฟต์แวร์รักษาความปลอดภัยเพื่อทำการสแกนบนอุปกรณ์ของคุณให้เสร็จสมบูรณ์เป็นประจำ**

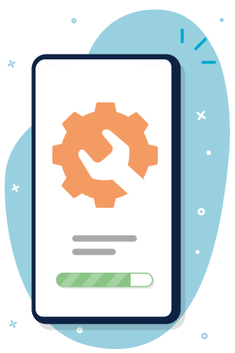
สำรองข้อมูลของคุณ

การสำรองข้อมูลเป็นประจำจะช่วยให้คุณสามารถกู้คืนข้อมูลของคุณได้หากข้อมูลสูญหายหรือถูกโจมตี

การสำรองข้อมูลสำคัญควรกระทำเป็นประจำหรือโดยอัตโนมัติในธุรกิจของคุณ หากไม่มีการสำรองข้อมูลเป็นประจำ อาจเป็นไปไม่ได้ที่คุณจะกู้คืนข้อมูลของคุณหลังจากถูกโจมตีทางไซเบอร์

มีวิธีการและผลิตภัณฑ์มากมายที่คุณสามารถใช้เพื่อสำรองข้อมูลของคุณได้ สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการสำรองข้อมูลทางธุรกิจของคุณ โปรดอ่านคำแนะนำเกี่ยวกับการสำรองข้อมูลของเราที่ cyber.gov.au/backups ตัวเลือกที่ดีที่สุดจะแตกต่างกันไปในแต่ละธุรกิจ ดังนั้นโปรดปรึกษาผู้เชี่ยวชาญด้านไอทีหากคุณไม่แน่ใจ

✓ **จัดทำแผนและดำเนินการตามแผนเพื่อสำรองข้อมูลของคุณเป็นประจำ**



รักษาความปลอดภัยเครือข่ายและบริการภายนอกของคุณ

ปกป้องธุรกิจของคุณจากการโจมตีทางไซเบอร์โดยการรับมือกับจุดอ่อนที่อาจเกิดขึ้นในเครือข่ายของคุณ

อุปกรณ์และบริการในเครือข่ายของคุณอาจเป็นเป้าหมายหลักสำหรับอาชญากรไซเบอร์ ระบบเหล่านี้หลายระบบอาจมีความซับซ้อนในการรักษาความปลอดภัย ดังนั้นจึงควรปรึกษาคำแนะนำต่อไปนี้กับผู้เชี่ยวชาญด้านไอที

- **รักษาความปลอดภัยเซิร์ฟเวอร์ของคุณ** หากคุณใช้ NAS หรือเซิร์ฟเวอร์อื่นในบ้านหรือธุรกิจของคุณ โปรดใช้ความระมัดระวังเป็นพิเศษในการรักษาความปลอดภัย อุปกรณ์เหล่านี้เป็นเป้าหมายทั่วไปของอาชญากรไซเบอร์ เนื่องจากอุปกรณ์มักเป็นที่จัดเก็บไฟล์สำคัญหรือทำหน้าที่สำคัญ มีกลยุทธ์การบรรเทาปัญหาหลายอย่างที่จำเป็นในการปกป้องอุปกรณ์เหล่านี้ ตัวอย่าง เช่น สิ่งสำคัญคือต้องแน่ใจว่าเซิร์ฟเวอร์หรืออุปกรณ์ NAS ได้รับการอัปเดตเป็นประจำ บัญชีผู้ใช้สำหรับการดูแลระบบควรได้รับการรักษาความปลอดภัยด้วยข้อความรหัสผ่านที่รัดกุมหรือการยืนยันตัวตนโดยใช้หลากหลายปัจจัย
- **ลดร่องรอยให้เหลือน้อยที่สุด ตรวจสอบและรักษา** ความปลอดภัยของบริการที่มีการเปิดเผยทางอินเทอร์เน็ตบนเครือข่ายของคุณ ซึ่งอาจรวมถึงรีโมทเดสทอป (Remote Desktop) ไฟล์แชร์ (File Shares) เว็บเมล (Webmail) และบริการการดูแลระบบระยะไกล
- **โยกย้ายไปยังบริการคลาวด์** พิจารณาใช้บริการทางออนไลน์หรือบริการคลาวด์ที่มีการรักษาความปลอดภัยในตัวแทนที่จะจัดการด้วยตัวเอง ตัวอย่างเช่น เรียกใช้บริการทางออนไลน์สำหรับสิ่งต่าง ๆ เช่น อีเมลหรือการโฮสเว็บไซต์ แทนที่จะใช้งานและรักษาความปลอดภัยของบริการเหล่านี้ด้วยตัวคุณเอง
- **ปรับปรุงความปลอดภัยของเราเตอร์** (Router) ของคุณ ปฏิบัติตามคำแนะนำของเราเกี่ยวกับวิธีการรักษาความปลอดภัยเราเตอร์ (Router) ของคุณ รวมถึงการอัปเดตรหัสผ่านเริ่มต้น การเปิด Wi-Fi สำหรับ “แขก” ให้ลูกค้าหรือผู้เยี่ยมชม และการใช้โปรโตคอลการเข้ารหัสที่รัดกุมที่สุด ค้นหาโดยใช้คำว่า Router บนเว็บไซต์ cyber.gov.au สำหรับข้อมูลเพิ่มเติม
- **ทำความเข้าใจกับซัพพลายเชนทางไซเบอร์ของคุณ** ธุรกิจสมัยใหม่มักเรียกใช้บริการจากภายนอกหลายบริการ ตัวอย่างเช่น การใช้ผู้ให้บริการบุคคลที่สาม (Managed Service Provider) เพื่อให้ดูแลระบบไอทีของตน ปัญหาด้านความปลอดภัยของบริการหรือผู้ให้บริการเหล่านี้ อาจส่งผลกระทบอย่างมีนัยสำคัญต่อธุรกิจของคุณ สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการจัดการความเสี่ยงของซัพพลายเชนทางไซเบอร์ โปรดอ่านคำแนะนำเกี่ยวกับซัพพลายเชนทางไซเบอร์ ที่เว็บไซต์ cyber.gov.au

✓ **พูดคุยกับผู้เชี่ยวชาญด้านไอทีเกี่ยวกับวิธีการรักษาความปลอดภัยเครือข่ายของคุณ**

ทำให้เว็บไซต์ของคุณยากต่อการโจมตี

เว็บไซต์เป็นเป้าหมายหลักสำหรับการโจมตีทางไซเบอร์

ปกป้องเว็บไซต์ของคุณจากการถูกจี้ปลันโดยทำตามมาตรการรักษาความปลอดภัยพื้นฐานบางประการดังนี้

- รักษาความปลอดภัยการเข้าสู่ระบบเว็บไซต์ของคุณด้วยการยืนยันตัวตนโดยใช้หลากหลายปัจจัย หรือรหัสผ่านที่รัดกุม
- อัปเดตระบบการจัดการเนื้อหาและปลั๊กอินของเว็บไซต์ของคุณเป็นประจำ
- สำรองข้อมูลเว็บไซต์ของคุณเป็นประจำเพื่อให้คุณสามารถกู้คืนข้อมูลได้หลังจากการโจมตีทางไซเบอร์

ACSC มีแหล่งข้อมูลเพิ่มเติมสำหรับเจ้าของเว็บไซต์ ค้นหาแหล่งข้อมูลเหล่านี้ได้ที่ cyber.gov.au

- ชัยชนะที่รวดเร็วสำหรับเว็บไซต์ของคุณ
- การนำระบบเหล่านี้ออกใช้งาน ใบรับรอง ทีแอลเอส เฮชทีทีพีเอส และกลไกการเข้ารหัสที่ฉวยโอกาส
- ความปลอดภัยของระบบชื่อโดเมนสำหรับเจ้าของโดเมน
- การเตรียมพร้อมและการตอบสนองต่อการโจมตีโดยปฏิเสธการให้บริการ

✓ **อ่านแหล่งข้อมูล ACSC เกี่ยวกับการรักษาความปลอดภัยเว็บไซต์**

รีเซ็ตอุปกรณ์ของคุณก่อนการขายหรือกำจัดทิ้ง

ข้อมูลบนอุปกรณ์เครื่องเก่าของคุณอาจจะเข้าถึงได้โดยคนแปลกหน้า

หากคุณไม่กำจัดอุปกรณ์ของคุณอย่างปลอดภัย อาชญากรไซเบอร์สามารถเข้าถึงข้อมูลบนอุปกรณ์ได้ ซึ่งอาจรวมถึงอีเมล ไฟล์ และข้อมูลทางธุรกิจอื่น ๆ ลบข้อมูลทั้งหมดออกจากอุปกรณ์ทางธุรกิจของคุณก่อนที่จะขาย แลกเปลี่ยนซื้อขาย หรือขจัดทิ้งไป ตัวอย่างเช่น โดยการทำการรีเซ็ตให้เป็นการตั้งค่าจากโรงงาน ซึ่งจะช่วยล้างข้อมูลและคืนค่าอุปกรณ์ให้กลับเป็น การตั้งค่าดั้งเดิม

สำหรับคำแนะนำเกี่ยวกับการรีเซ็ตอุปกรณ์ของคุณ โปรดอ่านคำแนะนำของเราเกี่ยวกับวิธีการกำจัดอุปกรณ์ของคุณอย่างปลอดภัย ค้นหาคำว่า *dispose* บนเว็บไซต์ cyber.gov.au.

✓ **ทำการรีเซ็ตให้เป็นการตั้งค่าจากโรงงานก่อนขาย หรือกำจัดอุปกรณ์ทางธุรกิจ**

ล็อกอุปกรณ์ของคุณไว้และเก็บรักษาให้ปลอดภัย

การจำกัดการเข้าถึงอุปกรณ์ทางธุรกิจของคุณจะลดโอกาสของกิจกรรมที่เป็นอันตราย

การจำกัดการเข้าถึงอุปกรณ์ทางธุรกิจของคุณเป็นวิธีง่าย ๆ ที่จะป้องกันไม่ให้ข้อมูลถูกขโมยหรือป้องกันกิจกรรมที่เป็นอันตรายอื่น ๆ ไม่ควรเก็บอุปกรณ์ทางธุรกิจไว้ในที่ที่พนักงานหรือบุคคลทั่วไปที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

ใช้การควบคุมการรักษาความปลอดภัยเพื่อปกป้องอุปกรณ์ทางธุรกิจของคุณเพิ่มเติม อย่างน้อยที่สุดอุปกรณ์ควรได้รับการล็อกด้วยข้อความรหัสผ่าน รหัสประจำตัว (PIN) หรือการยันยันตัวตนด้วยข้อมูลชีวภาพ (Biometrics) ตรวจสอบให้แน่ใจว่าอุปกรณ์เหล่านี้ได้รับการกำหนดค่าให้ล็อกโดยอัตโนมัติหลังจาก ไม่มีการใช้งานเป็นระยะเวลาสั้น ๆ

✓ **ตั้งค่าอุปกรณ์ให้ล็อกโดยอัตโนมัติหลังจากไม่มีการใช้งานเป็นเวลาสั้น ๆ**

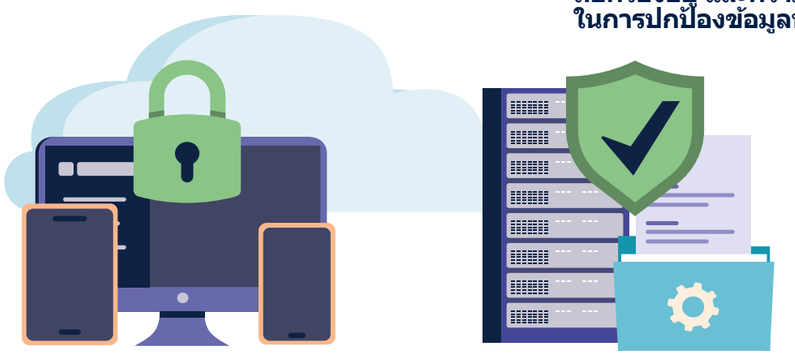
ปกป้องข้อมูลทางธุรกิจของคุณ

ข้อมูลทางธุรกิจที่คุณถือครองเป็นเป้าหมายที่อาชญากรไซเบอร์ให้ความสนใจ

การละเมิดข้อมูลกำลังเพิ่มขึ้นเรื่อย ๆ อย่าปล่อยให้ธุรกิจของคุณตกเป็นเหยื่อ เป็นสิ่งสำคัญที่จะต้องเข้าใจว่าข้อมูลใดบ้างที่ธุรกิจของคุณถือครองและอยู่ในสถานที่ตั้งใด เมื่อคุณทราบแล้ว ให้ใช้คำแนะนำในคู่มือนี้เพื่อช่วยปกป้องข้อมูลของคุณจากการเข้าถึงโดยอาชญากรไซเบอร์ ธุรกิจขนาดเล็กบางแห่งอาจมีภาระผูกพันเพิ่มเติมภายใต้กฎหมายอีกด้วย

- **รวบรวมข้อมูลทางธุรกิจของคุณไว้ที่เดียวกัน** คุณอาจมีข้อมูลที่จัดเก็บไว้ในอุปกรณ์หรือบริการต่าง ๆ มากมายหลายจุด เมื่อมีการกระจายข้อมูลจากตำแหน่งศูนย์กลาง จำนวนระบบที่คุณต้องรักษาความปลอดภัยและสำรองข้อมูลก็จะเพิ่มตามระบบจำนวนมากยังสามารถสร้างโอกาสให้อาชญากรไซเบอร์โจมตีได้มากขึ้นอีกด้วย หากเป็นไปได้ ให้จัดเก็บข้อมูลทางธุรกิจของคุณไว้ในตำแหน่งศูนย์กลางที่มีการรักษาความปลอดภัยและการสำรองข้อมูลเป็นประจำ การรวมศูนย์ข้อมูลของคุณอาจเปิดเป็นช่องโหว่ที่ใหญ่กว่าได้ หากระบบของคุณถูกโจมตี ดังนั้น ตรวจสอบให้แน่ใจว่าตำแหน่งศูนย์กลางนี้ได้รับการปกป้องอย่างเพียงพอด้วยการกำหนดตั้งค่าที่ปลอดภัยและการจำกัดการเข้าถึง พูดคุยกับผู้เชี่ยวชาญด้านไอทีหรือความปลอดภัยทางไซเบอร์เพื่อขอคำแนะนำ
- **ทราบภาระผูกพันของคุณในการปกป้องข้อมูล ธุรกิจขนาดเล็กบางแห่งอาจมีภาระผูกพัน** ทางกฎหมายในการจัดการข้อมูลส่วนบุคคลที่พวกเขาเก็บรวบรวม อ่านคำแนะนำของสำนักงานกรรมาธิการข้อมูลออสเตรเลีย (Office of the Australian Information Commissioner) เพื่อเรียนรู้เพิ่มเติมจากคู่มือสำหรับธุรกิจขนาดเล็กได้ที่ oaic.gov.au ปรึกษาผู้เชี่ยวชาญด้านกฎหมายหากคุณไม่แน่ใจ

✓ **ทำความเข้าใจข้อมูลที่ธุรกิจของคุณถือครองอยู่ และความรับผิดชอบของคุณในการปกป้องข้อมูลนั้น**



เตรียมความพร้อมให้พนักงานของคุณ

ให้ความรู้แก่พนักงาน

พนักงานที่มีแนวปฏิบัติด้านการรักษาความปลอดภัยทางไซเบอร์ที่ดีเป็นแนวป้องกันด่านแรกของคุณจากการโจมตีทางไซเบอร์

พนักงานของคุณควรมีความตระหนักเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ ซึ่งรวมถึงหัวข้อต่อไปนี้

- ภัยคุกคามด้านการรักษาความปลอดภัยทางไซเบอร์ที่พบบ่อย ได้แก่ การโจมตีผ่านอีเมลธุรกิจและแรนซัมแวร์
- มาตรการป้องกัน รวมถึงรหัสผ่านหรือข้อความรหัสผ่านที่รัดกุม การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) และการอัปเดตซอฟต์แวร์
- วิธีการตรวจจับสแกมและการโจมตีแบบฟิชชิ่ง
- นโยบายเฉพาะทางธุรกิจ (ตัวอย่างเช่น กระบวนการรายงานอีเมลที่น่าสงสัย หรือการตรวจสอบใบแจ้งหนี้ว่าเป็นของแท้ก่อนชำระเงิน)
- สิ่งที่ต้องทำในกรณีฉุกเฉิน

เว็บไซต์ ACSC มีแหล่งข้อมูลสำหรับหัวข้อส่วนใหญ่เหล่านี้ที่เว็บไซต์ cyber.gov.au/learn คุณอาจพิจารณาวิธีการอื่นในการให้ความรู้แก่พนักงานได้ เช่น สอนหลักสูตรที่เป็นทางการ หรือให้การฝึกอบรมภายในองค์กร ไม่ว่าคุณจะตัดสินใจอย่างไร โปรดจำไว้ว่าการฝึกอบรมด้านการรักษาความปลอดภัยทางไซเบอร์ไม่ใช่ข้อกำหนดที่จะทำเพียงครั้งเดียว และควรได้รับการรื้อฟื้นความรู้เป็นระยะ ๆ

✓ **กำหนดวิธีการสอนความตระหนักด้านการรักษาความปลอดภัยทางไซเบอร์ในธุรกิจของคุณ**

จัดทำแผนฉุกเฉิน

แผนฉุกเฉินสามารถลดผลกระทบจากการโจมตีทางไซเบอร์ในธุรกิจของคุณได้

เมื่อต้องตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ ทุกนาทีเป็นเวลาวิกฤต การมีแผนฉุกเฉินหมายความว่าพนักงานของคุณสามารถใช้เวลาน้อยลงในการคิดหาสิ่งที่ต้องทำและมีเวลาลงมือดำเนินการมากขึ้น

พิจารณาคำถามต่อไปนี้เมื่อจัดทำแผนฉุกเฉินของคุณ

- กระบวนการที่พนักงานของคุณใช้ในการรายงานเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นมีอะไรบ้าง?
- คุณติดต่อใครเพื่อขอความช่วยเหลือ? ตัวอย่างเช่น ผู้เชี่ยวชาญด้านไอทีและธนาคารของคุณ
- คุณจะสื่อสารกับพนักงาน ผู้ถือผลประโยชน์ร่วม หรือลูกค้าของคุณเกี่ยวกับเหตุการณ์ที่เกิดขึ้นได้อย่างไร?
- คุณจะจัดการธุรกิจตามปกติอย่างไร หากระบบที่สำคัญใด ๆ ออฟไลน์อยู่?

ตรวจสอบให้แน่ใจว่าพนักงานของคุณคุ้นเคยกับแผนฉุกเฉิน รวมถึงบทบาทหรือความรับผิดชอบที่พวกเขาอาจมี เก็บรักษาสำเนาของแผนเป็นฉบับกระดาษไว้ด้วย ในกรณีที่ระบบของคุณออฟไลน์เมื่อคุณต้องการใช้แผน

✓ **จัดทำแผนฉุกเฉินไว้สำหรับเหตุการณ์ด้านการรักษาความปลอดภัยทางไซเบอร์**

คอยติดตามข้อมูลอยู่เสมอ

ร่วมเป็นพันธมิตรกับ ACSC เพื่อรับข้อมูลล่าสุดจาก ACSC

คอยติดตามข้อมูลเกี่ยวกับภัยคุกคามและจุดอ่อนทางไซเบอร์ที่ล่าสุดอยู่เสมอด้วยการเป็นพันธมิตรกับ ACSC บริการนี้จะส่งจดหมายข่าวและการแจ้งเตือนรายเดือนถึงคุณเมื่อมีการระบุภัยคุกคามทางไซเบอร์แบบใหม่ขึ้นมา

การรักษาความปลอดภัยทางไซเบอร์เป็นสาขาความรู้ที่มีการพัฒนาอย่างรวดเร็ว อาชญากรไซเบอร์ใช้ประโยชน์จากจุดอ่อนอย่างไม่รอช้าภายในไม่กี่นาทีหลังจากที่มีการค้นพบจุดอ่อน การติดตามข้อมูลเกี่ยวกับสถานการณ์การรักษาความปลอดภัยทางไซเบอร์อยู่เสมอจะช่วยให้ธุรกิจของคุณเข้าใจถึงภัยคุกคามที่มีแนวโน้มต้องเผชิญและวิธีการป้องกันภัยคุกคามเหล่านั้น

✓ **ลงทะเบียนธุรกิจของคุณกับ โครงการพันธมิตร ACSC (ACSC Partnership Program)**

ข้อจำกัดความรับผิดชอบ (Disclaimer)
เนื้อหาในคู่มือนี้มีลักษณะทั่วไปและไม่ควรยึดถือว่าเป็นคำแนะนำทางกฎหมายหรือเป็นที่พึ่งสำหรับความช่วยเหลือในสถานการณ์เฉพาะหรือสถานการณ์ฉุกเฉินใด ๆ ในเรื่องที่สำคัญใด ๆ คุณควรขอคำแนะนำจากผู้เชี่ยวชาญอิสระที่เหมาะสมกับสถานการณ์ของคุณเอง

เครือรัฐจะไม่รับผิดชอบหรือมีส่วนรับผิดต่อความเสียหาย การสูญเสีย หรือค่าใช้จ่ายที่เกิดขึ้นจากการพึ่งพาข้อมูลที่มีอยู่ในคู่มือนี้

สำหรับข้อมูลเพิ่มเติมหรือรายงานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ ติดต่อเราที่
cyber.gov.au | 1300 CYBER1 (1300 292 371)
หมายเลขนี้มีไว้สำหรับใช้ภายในออสเตรเลียเท่านั้น

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre