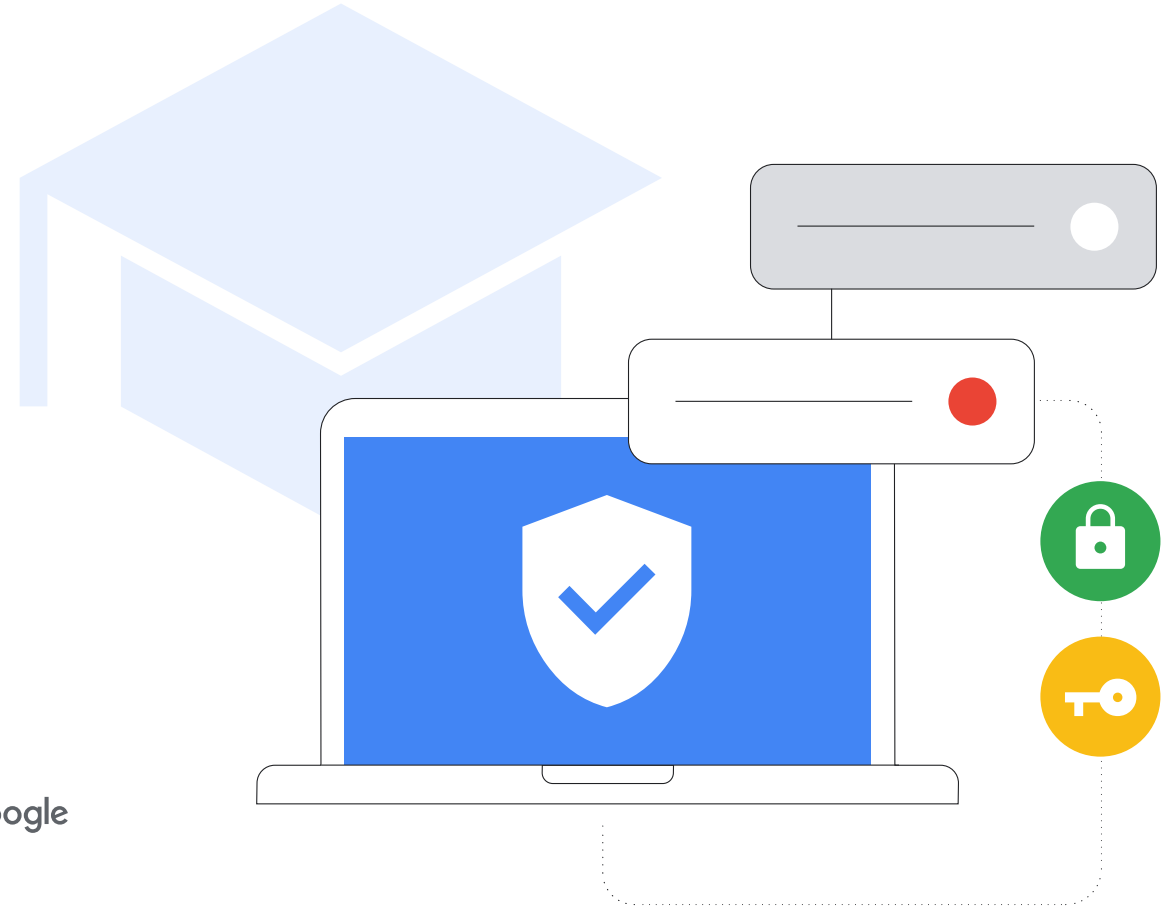
Google for Education

คู่มือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอนุบาลถึงมัธยมศึกษาตอนปลาย (K12)

ที่อัปเดตเดือนสิงหาคม 2023



Safer with Google

ข้อมูลสรุป

เพื่อให้สามารถปฏิบัติตามประเด็นที่ได้รับการเน้นย้ำจากในรายงานของ CISA เรื่องการปกป้องอนาคตของเรา (Protecting Our Future) ได้บรรลุผล สถาบันการศึกษาระดับอนุบาลถึงมัธยมศึกษาตอนปลาย (K-12) จำเป็นอย่างยิ่งที่จะต้องลงทุนกับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อปกป้องนักเรียน ครอบครัวของนักเรียน ครู เจ้าหน้าที่ และชุมชน เอกสารนี้จะให้คำแนะนำและแนวทางปฏิบัติแนะนำสำหรับผู้ดูแลระบบไอทีของโรงเรียนเกี่ยวกับการตั้งค่าและกำหนดค่าฮาร์ดแวร์และซอฟต์แวร์ในสถาบันการศึกษาระดับ K-12 เพื่อเสริมความแข็งแกร่งให้กับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีทั้งแนวทางปฏิบัติแนะนำทั่วไป รวมถึงคำแนะนำที่เฉพาะเจาะจงสำหรับผลิตภัณฑ์และบริการของ Google ปัจจุบันพันธกิจของ Google การจัดระเบียบข้อมูลบนโลก ตลอดจนทำให้ข้อมูลนั้นเป็นประโยชน์และทำให้ทุกคนทั่วโลกเข้าถึงได้ ซึ่ง เป็นแรงผลักดันสำคัญของ Google for Education เช่น กัน งานของเรา คือการสร้างเครื่องมือที่ออกแบบมาเพื่อการเรียนการสอน ในคู่มือนี้เราจะขอแสดง ข้อมูลที่เราได้เรียนรู้จากสถานศึกษาต่างๆ ให้คุณได้รับทราบร่วมกัน

แนวทางปฏิบัติแนะนำด้านการรักษาความปลอดภัยจะแยกออกเป็นหัวข้อต่างๆ พร้อม รายละเอียดเพิ่มเติมเกี่ยวกับกลยุทธ์การกำหนดค่า การตั้งค่า และการลดความเสี่ยง นอกจากนี้ยังมีคำ อธิบายแนวทางการให้บริการของ Google ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะสำหรับเครื่องมือทางการศึกษา และถึงแม้ ราจะให้คำแนะนำอย่างละเอียดไว้ในเอกสารนี้โดยไม่ได้อ้างอิงถึงผลิตภัณฑ์หรือบริการอื่นใด แต่เราก็เชื่อมั่นว่าผลิตภัณฑ์ของเรา สามารถป้องกันการโจมตีทางไซเบอร์ที่เกิดขึ้นเป็นประจำได้ตั้งแต่เปิดใช้งานครั้งแรกอย่างมีประสิทธิภาพกว่า

ความเสี่ยง

สถาบันการศึกษาเป็นเป้าหมายอันดับต้นๆ ของการโจมตีทางไซเบอร์เพราะมีข้อมูลส่วนบุคคลจำนวนมาก ผู้ไม่ประสงค์ดีจึงมักหาทางเจาะช่องโหว่นี้เพื่อขโมย ข้อมูลไปใช้เ พื่อประโยชน์ของตนเอง 46% ของโรงเรียนที่ยังไม่ตกเป็นเป้าหมาย การโจมตีเชื่อว่าตนจะถูกโจมตีในที่สุด ปัจจุบัน การโจมตีโดยแรนซัมแวร์มีความซับซ้อนมากขึ้นเรื่อยๆ ทำให้หยุดยั้งได้ยากกว่าเดิม ในจำนวนนี้ 42% ที่คิดว่าแรนซัมแวร์แพร่หลายมากจนถือเป็นภัยคุกคามที่ หลีกเลี่ยงไม่ได้ ส่วนสำคัญที่ทำให้โรงเรียนเกิดจุดอ่อนในการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การที่โรงเรียนจำเป็นต้องเปลี่ยนมาใช้การเรียนรู้ทางไกลในปี 2020 อย่างกะทันหันจึงทำให้เกิด ช่องโหว่ที่จะถูกโจมตีได้จำนวนมาก

การป้องกัน

เราลดการโจมตีเหล่านี้ได้ แม้ว่าจะไม่มีเทคโนโลยีใดที่กำจัดความเสี่ยงได้ทั้งหมด แต่หากภาคส่วนการศึกษาและผู้ให้บริการเทคโนโลยีด้านการศึกษา (EdTech) ร่วมมือกันเพื่อใช้งานและผสานรวมแนวทางปฏิบัติแนะนำก็จะสามารถ ซึ่งจะสร้างแนวทางที่ปลอดภัย มั่นคง และครอบคลุมในการลดความเสี่ยงได้อย่างมีประสิทธิภาพ สถาบันการศึกษาก็จะสามารถจัดการความเสี่ยงและลดจำนวนการโจมตีได้มากขึ้นหา มีมาตรการป้องกันและนโยบายที่เหมาะสมใน การปกป้องผู้ใช้ การรักษาความปลอดภัยให้อุปกรณ์ และรับประกันความเป็นส่วนตัวของข้อมูล

คำแนะนำสำคัญ

- **ใช้การตรวจสอบสิทธิ์ที่มีความปลอดภัย** เพื่อปกป้องข้อมูลที่ละเอียดอ่อน รวมไปถึงอีเมล ไฟล์ และเนื้อหาอื่นๆ ตลอดจนป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงระบบการศึกษา ใช้แนวทางปฏิบัติแนะนำสำหรับการตรวจสอบสิทธิ์ผู้ใช้ รวมถึงรหัสผ่านที่รัดกุมและการยืนยันแบบ 2 ขั้นตอน (2SV), พาสคีย์ และเครื่องมือจัดการรหัสผ่าน หากทำได้ โดยเฉพาะสำหรับผู้ดูแลระบบไอทีและเจ้าหน้าที่ซึ่งทำงานกับข้อมูลที่ละเอียดอ่อน
- **ใช้การตั้งค่าความปลอดภัยที่เหมาะสม** เพื่อปกป้องผู้ใช้ ข้อมูล และสภาพแวดล้อมให้ปลอดภัย แม้ว่าผลิตภัณฑ์ของ Google จะสร้างมาอย่างปลอดภัยตั้งแต่ต้น แต่ผู้ดูแลระบบก็จำเป็นต้องใช้งานและกำหนดค่าเครือข่ายและระบบอย่างเหมาะสมเพื่อช่วยให้การรักษาความปลอดภัยรัดกุมยิ่งขึ้น คุณควรใช้หลักการ Zero Trust และสิทธิ์ขั้นต่ำที่สุดเพื่อความมั่นคงปลอดภัยของโรงเรียน กล่าวคือ ผู้ใช้ควรมีสิทธิ์เข้าถึงเฉพาะซอฟต์แวร์ ข้อมูล แอปพลิเคชัน และระบบที่จำเป็นต่อการทำงานของตนเองอย่างมีประสิทธิภาพเท่านั้น
- **อัปเดตและอัปเกรดระบบของคุณ** เพื่อให้มั่นใจว่าผู้ใช้จะได้รับการปกป้องจากภัยคุกคามล่าสุด โปรดใช้ระบบปฏิบัติการ (OS) และเบราว์เซอร์ที่ทันสมัย รวมถึงตรวจสอบว่าผู้ใช้กำลัง ใช้ซอฟต์แวร์เวอร์ชันล่าสุดบนอุปกรณ์ทุกเครื่อง (หรือเวอร์ชันเสถียรระยะยาวที่ผ่านการอนุมัติ) และมีการอัปเดตระบบดังกล่าวโดยอัตโนมัติ การอัปเกรดไปใช้โซลูชันที่ปลอดภัยกว่า เช่น Chromebook ก็ช่วยยกระดับการรักษาความปลอดภัยได้ ทั้งนี้ เราไม่เคยตรวจพบแรนซัมแวร์บนอุปกรณ์ ChromeOS แม้แต่ครั้งเดียว
- **ใช้ระบบแจ้งเตือนและตรวจสอบแบบเรียลไทม์** เพื่อเสริมระดับความปลอดภัยและลดปัญหาที่อาจเกิดขึ้นอย่างรวดเร็ว คุณสามารถใช้ฟีเจอร์ต่างๆ ที่มาพร้อมซอฟต์แวร์การทำงานร่วมกันและการสื่อสารที่คุณใช้เป็นหลัก เช่น Google Workspace for Education หรือจะใช้โซลูชันการบันทึกและตรวจสอบเพื่อความปลอดภัยแยกต่างหากก็ได้ ตรวจสอบว่ามีการติดตามกิจกรรมที่ครอบคลุมทั่วเครือข่าย อุปกรณ์ แอปพลิเคชัน ผู้ใช้ และข้อมูลของโรงเรียน ตรวจสอบการเข้าสู่ระบบบัญชี การแชร์ไฟล์ จำนวนอีเมล (โดยเฉพาะความพยายามในการฟิชชิงและส่งมัลแวร์) กิจกรรมในอุปกรณ์ และการเปลี่ยนแปลงการกำหนดค่า อัปเดตโซลูชันการแจ้งเตือนและการตรวจสอบให้เป็นปัจจุบันเสมอ เพื่อรับการแจ้งเตือนเกี่ยวกับภัยคุกคาม เหตุการณ์สำคัญ และการเปลี่ยนแปลงของระบบ
- **ฝึกอบรมครู เจ้าหน้าที่ และนักเรียน** ให้รู้วิธีใช้อุปกรณ์และซอฟต์แวร์อย่างปลอดภัย สังเกตและรายงานสิ่งที่อาจเป็นภัยคุกคาม รวมถึงแชร์ข้อมูลอย่างเหมาะสมเพื่อช่วยป้องกันการโจมตีที่พบได้บ่อยที่สุด โรงเรียนหรือเขตการศึกษาสามารถสร้างสื่อการฝึกอบรมเฉพาะ ควบคู่ไปกับการใช้สื่อสำเร็จรูปที่ไม่มีค่าใช้จ่าย เพื่อเป็นชุดเครื่องมือที่ครอบคลุมสำหรับโรงเรียน

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

คำแนะนำสำหรับผู้ใช้ผลิตภัณฑ์ของ Google โดยเฉพาะ : ผลิตภัณฑ์ของ Google เช่น Google Workspace for Education และ Chromebook สามารถยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงเรียนและช่วยให้สามารถปฏิบัติตามคำแนะนำข้างต้นได้ง่ายขึ้น หากสามารถใช้งานได้ทั้งสองอย่างก็จะ เป็นโซลูชันที่ครอบคลุมในการปกป้องความเป็นส่วนตัวของผู้ใช้ และมอบการรักษาความปลอดภัยที่ดีที่สุดให้แก่สถาบันของคุณ

กลยุทธ์เหล่านี้และ คำแนะนำเพิ่มเติมในเอกสารนี้ถือเป็นรากฐานที่ยอดเยี่ยมสำหรับการรักษาความปลอดภัยของสถาบันการศึกษาระดับ K-12

แนวทางของ Google ด้านการศึกษา

พันธกิจของ Google คือในการจัดระเบียบข้อมูลบนโลก ตลอดจนทำให้ข้อมูลนั้นเป็นประโยชน์และทำให้ทุกคนทั่วโลกเข้าถึงได้ ซึ่งถือเป็นพันธกิจของเราในภาคส่วนการศึกษาด้วย ทีม Google for Education มุ่งมั่น าทำตามพันธกิจนี้โดยการสร้างเครื่องมืออย่าง Chromebook และ Google Classroom เพื่อช่วย ให้นักเรียนและครูสามารถสร้าง แชร์ และจัดระเบียบเนื้อหาของตนเอง ตลอดจนเข้าถึงและใช้ทรัพยากรทางการศึกษาและเครื่องมือออนไลน์ได้อย่างสะดวกสบายและปลอดภัย

โรงเรียนต่างๆ ควรมีเทคโนโลยีที่ปลอดภัยตั้งแต่เริ่ม ต้น ออกแบบมาเพื่อความเป็นส่วนตัว ให้สิทธิคุณในการควบคุม รวมถึงมีเนื้อหาและข้อมูลที่เชื่อถือได้ เมื่อใช้ผลิตภัณฑ์เช่น Chromebooks และ Google Workspace for Education โรงเรียนจะได้รับ การรักษาความปลอดภัยที่ดีที่สุดซึ่งเป็นไปตามมาตรฐานสูงสุดระดับโลกในด้านการศึกษา ส่วนผู้ดูแลระบบไอทีก็จะได้รับ การเข้าถึงอย่างเต็มรูปแบบ รวมถึงการควบคุมข้อมูลและนโยบายความปลอดภัยที่ไม่ยุ่งยาก ด้านนักเรียนก็จะสามารถจดจ่อกับการเรียนรู้ได้อย่างเต็มที่ในสภาพแวดล้อมดิจิทัลที่ปลอดภัย ซึ่งแสดงเนื้อหาตามอายุ รวมถึงลดจำนวนสแปมและภัยคุกคามทางไซเบอร์

เรา ให้ความสำคัญกับฟีเจอร์ความปลอดภัยและการควบคุมในตัว มาตรฐานความเป็นส่วนตัวระดับสูงสุด และตัวเลือกเครื่องมือรักษาความปลอดภัยในเชิงรุกที่มากขึ้นเพื่อสร้างการเรียนรู้ที่ปลอดภัยสำหรับทุกคน อุปกรณ์ ChromeOS ช่วยลดภัยคุกคามที่โรงเรียนต้องเผชิญ และเป็นแนวป้องกันที่ดีที่สุดต่อภัยคุกคามอันดับหนึ่งของโรงเรียนอย่างแรนซัมแวร์ ซึ่งไม่เคยโจมตี Chromebook ได้สำเร็จเลยสักครั้ง

ในขณะเดียวกัน Google Workspace for Education ก็เป็นชุดโปรแกรมสำหรับการสื่อสารและการทำงานร่วมกันในระบบคลาวด์ที่มีความปลอดภัย อีกทั้งยังได้รับความนิยมมากที่สุดในโลก โปรดดูข้อมูลเพิ่มเติมเกี่ยวกับวิธีที่ผลิตภัณฑ์แต่ละรายการช่วยรักษาความมั่นคงปลอดภัยไซเบอร์ตามคำแนะนำที่ระบุไว้ ณ ที่นี้ได้ในส่วนสุดท้าย

เอกสารนี้แบ่งออกเป็น 2 ส่วน โดยส่วนแรกจะกล่าวถึงคำแนะนำด้านความปลอดภัยทั่วไปซึ่งสามารถนำไปปฏิบัติได้จริงสำหรับสถาบันการศึกษาระดับ K-12 ไม่ว่าจะใช้ผลิตภัณฑ์ใดก็ตาม ส่วนที่ 2 จะเป็นคำแนะนำในการกำหนดค่าที่เฉพาะเจาะจงสำหรับสถาบันที่ใช้ผลิตภัณฑ์ Google for Education เช่น Google Workspace for Education และ Chromebook หากสามารถใช้งานร่วมกันได้ 2 ส่วน ก็จะช่วยให้คุณและนักเรียนปลอดภัยบนโลกออนไลน์มากยิ่งขึ้น

บทนำ

ทั้งอุปกรณ์และเครือข่ายของสถาบันการศึกษาระดับ K-12 ต่างก็มีความเสี่ยงสูงในการตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ สถาบันการศึกษาระดับ K-12 จึงจำเป็นต้องใช้การรักษาความปลอดภัยที่ดีที่สุดเพื่อปกป้องนักเรียน รวมถึงปกป้องข้อมูล บริการ ทรัพยากร เวลา และเงินที่อาจสูญเสียไปเมื่อเกิดการโจมตีเหล่านี้ (แหล่งที่มา)

คู่มือนี้เป็นเครื่องมือสนับสนุนแนวทางปฏิบัติแนะนำด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผู้ดูแลระบบและระบบของโรงเรียนสามารถนำไปใช้เพื่อรักษาสภาพแวดล้อมให้ปลอดภัยยิ่งขึ้น การนำแนวทางปฏิบัติแนะนำเหล่านี้ไปใช้จะช่วยให้สถาบันการศึกษาระดับ K-12 สามารถลดหรือป้องกันการโจมตีทางไซเบอร์ที่รุนแรงและทำให้เสียค่าใช้จ่ายสูงซึ่งอาจเกิดขึ้นกับระบบการศึกษาตลอดจนปกป้องนักเรียน ครอบครัว ครู และเจ้าหน้าที

การโจมตีทางไซเบอร์ที่พุ่งเป้าไปยังโรงเรียนมีให้เห็นบ่อยขึ้นและรุนแรงขึ้นเรื่อยๆ ศูนย์แหล่งข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับช่วง K-12 (K-12 Cybersecurity Resource Center) ระบุว่าระหว่างปี 2016 ถึง 2021 มีเหตุการณ์ทาง ไซเบอร์ที่เปิดเผยต่อสาธารณะเกี่ยวข้องกับองค์กรการศึกษามากกว่า 1,300 ครั้ง ซึ่งเกิดขึ้นทั่วทั้ง 50 รัฐในสหรัฐอเมริกา ผู้นำทางการศึกษาในปัจจุบันต้องปกป้องข้อมูลและข้อมูลส่วนบุคคลของนักเรียน ครู และเจ้าหน้าที รวมถึงระบบและข้อมูลของสถาบัน ซึ่งถือเป็นงานหนักสำหรับภาคการศึกษาที่จะต้องพยายามอัปเดตตนเองให้ทันต่อ การเปลี่ยนแปลงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่เสมอเมื่อเทียบกับภาคส่วนอื่นๆ

การโจมตีทางไซเบอร์ที่ประสบความสำเร็จ เช่น แรนซัมแวร์ ฟิชชิง มัลแวร์ และอื่นๆ อาจทำให้เกิดการละเมิดข้อมูลส่วนบุคคลที่ระบุตัวบุคคลนั้นได้ (PII) ซึ่งจะส่งผลกระทบในวงกว้าง สร้างความเสียหายมูลค่าสูง (ค่าใช้จ่ายในกรณีที่ถูกโจมตีโดยแรนซัมแวร์โดยเฉลี่ยเพิ่มขึ้นถึง 5 เท่าตั้งแต่ปี 2020 เป็น $812,260) รวมถึงทำให้การสอนและการดำเนินงานอื่นๆ ของโรงเรียนต้องหยุดชะงักเป็นเวลานาน เมื่อเร็วๆ นี้ การโจมตีด้วยแรนซัมแวร์ที่ประสบความสำเร็จสามารถ ปิดระบบโรงเรียน ได้ทั้งหมด ซึ่ง ซึ่งส่งผลกระทบต่อทั้งชุมชนเพราะนักเรียนไม่สามารถเข้าชั้นเรียนได้เป็นเวลาหลายวันต่อเนื่อง การมีทรัพยากรและเงินทุนที่จำกัดทำให้องค์กรระดับ K-12 ยังคงเป็นเป้าหมายสำคัญของการโจมตีต่อไป เว้นแต่จะมีการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น

การรักษาความมั่นคงปลอดภัยไซเบอร์จะสร้างผลลัพธ์ที่ดีที่สุดได้ก็ต่อเมื่อมีการสื่อสาร การทำงานร่วมกัน และความร่วมมือ เอกสารนี้ได้รวบรวมเคล็ดลับความปลอดภัยของ Google, เฟรมเวิร์กการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute for Standards and Technology: NIST) รวมถึงชุดเครื่องมือและคำแนะนำเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับช่วง K-12 ปี 2023 ของ CISA ซึ่งเป็นแหล่งข้อมูลเกี่ยวกับแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยอมรับในวงกว้าง โดยเอกสารนี้จะกล่าวถึงขั้นตอนทั่วไปที่ผู้ดูแลระบบไอทีควรดำเนินการหรือพิจารณา แนวทางปฏิบัติแนะนำของ Google และคำแนะนำสำหรับผลิตภัณฑ์ของเราตลอดจนการอ้างอิงถึงเคล็ดลับความปลอดภัยและบริการต่างๆ ที่บริษัทอื่นนำเสนอ ผู้ดูแลระบบควรอ่านคำแนะนำด้านความปลอดภัยทั้งหมดที่ได้รับจากบริษัทที่เกี่ยวข้องและนำคำแนะนำล่าสุดไปใช้ เนื่องจากบริษัทที่รับผิดชอบจะสามารถอธิบายผลิตภัณฑ์ของตนเองและการเปลี่ยนแปลงใดๆ ที่อาจเกิดขึ้นได้ดีที่สุด

ก่อนดำเนินการตามคำแนะนำที่ระบุด้านล่าง คุณควรคำนึงถึงปัจจัยต่อไปนี้

ข้อควรพิจารณามีดังนี้

1. **การปกป้องนักเรียนของคุณ**
   ความต้องการของแต่ละโรงเรียนนั้นแตกต่างกันไป สำหรับนักเรียนบางกลุ่มอาจจำเป็นต้องมีขั้นตอนเพิ่มเติมในการรักษาความปลอดภัยและปกป้องความเป็นส่วนตัว เครื่องมือ EdTech หลายอย่างมีฟีเจอร์ที่ช่วยในเรื่องการเข้าถึงตามอายุ เช่น การจำกัดเนื้อหาไม่เหมาะสมหรือการเก็บตำแหน่งและข้อมูลติดต่อให้เป็นส่วนตัว
2. **ประเภทของข้อมูลที่จัดเก็บ**
   หากจัดเก็บข้อมูลที่ละเอียดอ่อน เราแนะนำให้คุณเข้ารหัสข้อมูลหรือจัดเก็บข้อมูลในตำแหน่งอื่น
3. **ประเภทอุปกรณ์ที่ใช้และรูปแบบการใช้งาน**
   อุปกรณ์และแอปพลิเคชันควรได้รับการอัปเดตอัตโนมัติเพื่อความปลอดภัยสูงสุด โปรดเข้ารหัสข้อมูลและแยกบัญชีเพื่อให้แน่ใจว่าผู้ใช้จะเข้าถึงข้อมูลของตนเองได้เท่านั้น
4. **นโยบายของโรงเรียน เขตการศึกษา หรือภูมิภาค**
   โรงเรียนของคุณอาจมีนโยบายเฉพาะเกี่ยวกับการใช้เทคโนโลยี คุณจึงจำเป็นต้องตรวจสอบว่ามาตรการป้องกันทั้งหมดเป็นไปตามนโยบายของโรงเรียนหรือไม่

ทุกๆ วัน Gmail สามารถบล็อกฟิชชิงที่พยายามเจาะระบบได้กว่า
100 ล้านครั้ง

ทุกๆ สัปดาห์ Google ตรวจพบเว็บไซต์ที่ไม่ปลอดภัย
300,000 เว็บ

ทุกๆ วัน ผู้ใช้
74 ล้าน
คนได้รับความช่วยเหลือจากเครื่องมือจัดการรหัสผ่านของ Google

ทุกๆ ปี ผู้คน
700 ล้าน
คนเพิ่มความปลอดภัยให้ตัวเองโดยใช้เว็บไซต์การตรวจสอบความปลอดภัย

คำแนะนำด้านความปลอดภัยทั่วไป

ใช้การตรวจสอบสิทธิ์ที่มีความปลอดภัย

การตรวจสอบสิทธิ์ที่มีความปลอดภัยจำเป็นต้องเป็นสิ่งสำคัญอันดับแรกสุดสำหรับโรงเรียนและสถาบันการศึกษา ในไตรมาส 4 ของปี 2022 บัญชีที่มีความเสี่ยงหรือไม่มีการกำหนดข้อมูลเข้าสู่ระบบคิดเป็น 48% ของปัจจัยเสี่ยงทั้งหมดที่นำไปสู่การหลุดรั่วของข้อมูล หากสามารถนำคำแนะนำที่สำคัญไปปฏิบัติได้จะช่วยตรวจสอบได้ว่ามีผู้สวมรอยเป็นผู้ใช้หรือไม่ และจำกัดการเข้าถึงข้อมูลที่เหมาะสมกับบทบาทของผู้ใช้แต่ละคนได้

ผู้ดูแลระบบไอทีควรบังคับใช้การยืนยันแบบ 2 ขั้นตอน (2SV) (หรือที่เรียกอีกอย่างว่าการตรวจสอบสิทธิ์แบบ 2 ปัจจัย (2FA)) และเปลี่ยนไปใช้การตรวจสอบสิทธิ์แบบไม่ใช้รหัสผ่าน (เช่น พาสคีย์) ทุกครั้งที่เป็นไปได้ โดยเฉพาะอย่างยิ่งเมื่อมีคนเข้าถึงระบบของสถาบันการศึกษาจากระยะไกล การยืนยันแบบ 2 ขั้นตอนจะเพิ่มการรักษาความปลอดภัยให้กับบัญชีออนไลน์มากขึ้นอีกขั้น ซึ่งทำให้ผู้โจมตีเข้าถึงได้ยากขึ้นมาก

ปัจจุบัน โรงเรียนใช้อุปกรณ์และรูปแบบการใช้งานหลายประเภท ความสามารถทางเทคนิคของผู้ใช้ในสภาพแวดล้อมระดับ K-12 ก็แตกต่างกันไปอีกด้วย ความปลอดภัยของบัญชีและอุปกรณ์จะแตกต่างกันไปตามบทบาทและประเภทผู้ใช้โดยมีแนวทางปฏิบัติแนะนำที่กำหนดไว้ ไม่ว่าจะเป็นผู้ดูแลระบบไอที ครูและเจ้าหน้าที่ นักเรียนที่โตกว่าซึ่งใช้อุปกรณ์ที่ได้รับมอบหมาย ไปจนถึงนักเรียนอายุน้อยซึ่งใช้อุปกรณ์ร่วมกัน เราจะพูดถึงคำแนะนำเฉพาะสำหรับแต่ละกลุ่มต่อไป

วิธีการตรวจสอบสิทธิ์ซึ่งเป็นแนวทางปฏิบัติแนะนำในสถานการณ์ส่วนใหญ่มีอยู่หลายวิธี ดังนี้

- **รหัสผ่านที่รัดกุม:**
แจ้งให้ผู้ใช้สร้างรหัสผ่านของตนเองเมื่อลงชื่อเข้าใช้ครั้งแรก โดยรหัสผ่านต้องมีความยาวและความซับซ้อนขั้นต่ำตามข้อกำหนดทางเทคนิค รหัสผ่านที่ยาวขึ้นจะช่วยเพิ่มความปลอดภัยเนื่องจากมีความยาวและการใช้อักขระที่ซับซ้อน ผู้ใช้ไม่ควรต้องเปลี่ยนรหัสผ่านเป็นประจำ เนื่องจากจะทำให้ผู้ใช้เลือกใช้รหัสผ่านที่ง่ายกว่าหรือเปลี่ยนรหัสผ่านเพียงเล็กน้อย (เช่น การเปลี่ยนอักขระเพียงตัวเดียว)
- **การยืนยันแบบ 2 ขั้นตอน (2SV):**
การยืนยันแบบ 2 ขั้นตอนจะปกป้องบัญชีด้วยขั้นตอนที่ 2 ซึ่งมักเป็นสิ่งที่ผู้ใช้มีติดตัว เช่น คีย์ความปลอดภัยหรือแอปบนโทรศัพท์มือถือที่สร้างรหัสยืนยันแบบครั้งเดียว แม้ว่าการยืนยันแบบ 2 ขั้นตอนทุกรูปแบบจะเพิ่มความปลอดภัยของบัญชีได้ แต่ผู้ดูแลระบบก็ควรหลีกเลี่ยงการใช้รหัสยืนยันที่ส่งผ่านข้อความหรือการโทร ซึ่งอาจเสี่ยงต่อการโจมตีที่ใช้หมายเลขโทรศัพท์
- **การตรวจสอบสิทธิ์แบบไม่ใช้รหัสผ่าน:**
พาสคีย์ปลอดภัยกว่าและใช้งานง่ายกว่าเมื่อเทียบกับรหัสผ่าน ผู้ใช้สามารถลงชื่อเข้าใช้แอปและเว็บไซต์ด้วย PIN, รูปแบบ, เซ็นเซอร์ข้อมูลไบโอเมตริก (เช่น ลายนิ้วมือหรือการจดจำใบหน้า) หรือ การแตะคีย์ความปลอดภัย ผู้ใช้จึงไม่ต้องจำและจัดการรหัสผ่าน สิ่งเหล่านี้กำลังเข้ามาแทนที่การตรวจสอบสิทธิ์รูปแบบเดิมมากขึ้นเรื่อยๆ และทำให้การลงชื่อเข้าใช้ปลอดภัยและรวดเร็วยิ่งขึ้น แม้ว่าอาจจะไม่เหมาะสมกับบริบททางการศึกษาทั้งหมดก็ตามแต่ พาสคีย์จะช่วยปกป้องผู้ใช้จากการโจมตีแบบฟิชชิงเพราะ ทำงานได้บนเว็บไซต์และแอปที่ลงทะเบียนเท่านั้น
- **การลงชื่อเพียงครั้งเดียว (SSO):**
SSO ช่วยให้ผู้ใช้เข้าถึงแอปพลิเคชันและเว็บไซต์ต่างๆ ได้ด้วยข้อมูลเข้าสู่ระบบเพียงชุดเดียว เมื่อต้องจำข้อมูลเข้าสู่ระบบเพียงชุดเดียว โอกาสที่ผู้ใช้จะจดบันทึกข้อมูลนั้นก็น้อยลง นอกจากนี้ เมื่อโรงเรียนไม่จำเป็นต้องจัดการข้อมูลเข้าสู่ระบบของผู้ใช้หลายชุด โรงเรียนก็สามารถประหยัดเงินสำหรับการสนับสนุนด้านไอทีและค่าใช้จ่ายของฝ่ายช่วยเหลือ Google Workspace for Education รองรับ SSO อยู่แล้ว ผู้ใช้จึงสามารถใช้ข้อมูลเข้าสู่ระบบของบัญชี Google เพื่อเข้าสู่ระบบบนแอปพลิเคชันของบุคคลที่สาม หรือใช้ข้อมูลเข้าสู่ระบบของผู้ให้บริการรายอื่นในการเข้าสู่บัญชี Google
- **เครื่องมือจัดการรหัสผ่าน:**
เครื่องมือจัดการรหัสผ่านจะช่วยให้ผู้ใช้สร้างรหัสผ่านที่รัดกุมและไม่ซ้ำกันสำหรับบัญชีและบริการต่างๆ ที่ใช้ในการเรียนหรือการทำงาน (เมื่อไม่ได้ใช้ SSO) เครื่องมือเหล่านี้ไม่มีส่วนช่วยในการเข้าสู่ระบบปฏิบัติการของอุปกรณ์ แต่จะช่วยจัดการรหัสผ่านได้เมื่อผู้ใช้เข้าสู่ระบบแล้ว ส่วนผู้ใช้ Google จะสามารถใช้เครื่องมือจัดการรหัสผ่านใน Chrome บนแพลตฟอร์มต่างๆ รวมถึง ChromeOS และ Android

กลุ่มต่างๆ ที่มีความต้องการเฉพาะจะได้ประโยชน์จากรูปแบบย่อยเฉพาะทางหรือการผสมผสานแนวทางการตรวจสอบสิทธิ์เหล่านี้เข้าด้วยกัน ทั้งนี้จะขึ้นอยู่กับบทบาทของผู้ใช้ภายในสถาบันการศึกษา ประเภทของระบบและข้อมูลที่เข้าถึง ตลอดจนอายุของผู้ใช้

ผู้ดูแลระบบไอทีของโรงเรียน

ผู้ดูแลระบบมีหน้าที่ควบคุมระบบและข้อมูลส่วนใหญ่ของสถาบันระดับ K-12 การปกป้องบัญชีจึงเป็นกุญแจสำคัญในการรักษาความปลอดภัยของระบบทั้งหมด ตั้งแต่โครงสร้างพื้นฐาน ข้อมูลบัญชี ไปจนถึงอุปกรณ์ที่สถาบันดูแล ดังนั้น ผู้ดูแลระบบจึงควรใช้มาตรฐานสูงสุดสำหรับการตรวจสอบสิทธิ์ รวมถึงการใช้รหัสผ่านที่รัดกุม เครื่องมือจัดการรหัสผ่านที่มีประสิทธิภาพ และการยืนยันแบบ 2 ขั้นตอน แต่ละวิธีจะช่วยเพิ่มการป้องกันอีกชั้นหนึ่ง และเมื่อนำมาใช้ร่วมกันก็จะมอบความปลอดภัยที่แข็งแกร่งที่สุดให้กับบัญชีผู้ดูแลระบบและบริการระดับองค์กร

- ผู้ดูแลระบบควรใช้อุปกรณ์คีย์ความปลอดภัยหรือวิธีการยืนยันแบบ 2 ขั้นตอนที่เข้ารหัสอย่างปลอดภัยซึ่งต้องใช้อุปกรณ์และพรอมต์ที่เชื่อถือได้ โดยอาจรวมถึงต้องใช้บริการจาก Google Authenticator หรือแอปอื่นเพื่อสร้างรหัสยืนยันแบบครั้งเดียว นอกจากนี้ Chromebook ที่เปิดตัวหลังปี 2019 พร้อมชิป TPM จะมีปุ่มเปิด/ปิดซึ่งใช้ในการตรวจสอบสิทธิ์แบบ 2 ปัจจัยได้
- ผู้ดูแลระบบควรใช้เครื่องมือจัดการรหัสผ่านที่เชื่อถือได้ซึ่งรองรับการยืนยันแบบ 2 ขั้นตอนในการจัดเก็บรหัสผ่านสำหรับบริการต่างๆ

ครูและเจ้าหน้าที่ซึ่งใช้อุปกรณ์ที่ได้รับมอบหมาย

ครูและเจ้าหน้าที่มีสิทธิ์เข้าถึงข้อมูลที่ละเอียดอ่อนเช่นเดียวกันกับผู้ดูแลระบบ แต่ไม่ได้ควบคุมโครงสร้างพื้นฐานทางดิจิทัลและมีความสามารถทางเทคนิคที่แตกต่างกันมากกว่า

- ครูและเจ้าหน้าที่ที่ใช้ Chromebook ควรมีตัวเลือกในการลงชื่อเข้าใช้ด้วยการยืนยันข้อมูลไบโอเมตริก เช่น ลายนิ้วมือ ในกรณีที่กฎหมายอนุญาต
- ผู้ดูแลระบบควรบังคับให้มีการใช้การยืนยันแบบ 2 ขั้นตอนและเปลี่ยนไปใช้การตรวจสอบสิทธิ์แบบไม่ใช้รหัสผ่านทุกครั้งที่เป็นไปได้ และเมื่อใดก็ตามที่เจ้าหน้าที่เข้าถึงระบบของสถาบันการศึกษาจากระยะไกล

นักเรียนที่โตกว่าซึ่งใช้อุปกรณ์ที่ได้รับมอบหมาย

(มักเป็นชั้นประถมศึกษาปีที่ 4 ขึ้นไป)

นักเรียนที่โตกว่าจะมีความรู้มากกว่าในการปกป้องตนเอง และมักจะสามารถใช้กลไกการตรวจสอบสิทธิ์ที่มีการป้องกันมากกว่าซึ่งเหมาะสมกับประเภทของบริการที่นักเรียนเหล่านี้อาจจำเป็นต้องใช้งานซึ่งนักเรียนควรมีสิทธิ์เข้าถึงเฉพาะบัญชีของตนเองและข้อมูลที่แชร์กับนักเรียนโดยตรงเท่านั้น

- นักเรียนที่ใช้ Chromebook ควรมีตัวเลือกในการสร้าง PIN สำหรับอุปกรณ์โดยเฉพาะเพื่อให้ลงชื่อเข้าใช้ได้เร็วขึ้น การใช้ข้อมูลไบโอเมตริกอาจไม่เหมาะสมกับสภาพแวดล้อมที่หลากหลายของโรงเรียน
- นักเรียนทุกคนควรได้รับการสนับสนุนให้สร้างรหัสผ่านที่ไม่ซ้ำซึ่งไม่มีข้อมูลส่วนบุคคล (เช่น ชื่อ ห้องเรียนประจำหรือวันเกิด) และได้รับการสอนให้เข้าใจว่าเหตุใดการใช้ข้อความรหัสผ่านจึงช่วยเพิ่มความปลอดภัยและทำให้จำรหัสผ่านได้ง่ายขึ้น

นักเรียนอายุน้อยซึ่งใช้อุปกรณ์ร่วมกัน (มักเป็นระดับ K-3l)

นักเรียนอายุน้อยยังคงเรียนรู้วิธีใช้เทคโนโลยีทางการศึกษาอยู่ และจะได้ประโยชน์จากการตรวจสอบสิทธิ์แบบง่ายๆ ซึ่งเหมาะสำหรับการใช้งานกับบริการและข้อมูลที่จำกัด

- โรงเรียนที่ใช้ตัวเลือกรหัสผ่านของบุคคลที่สาม เช่น คิวอาร์โค้ดหรือการเข้าสู่ระบบด้วยภาพสำหรับนักเรียนอายุน้อยและ ผู้ที่ไม่สามารถเข้าสู่ระบบด้วยรหัสผ่าน ควรวางมาตรการป้องกันเพื่อความปลอดภัย เนื่องจากตัวเลือกเหล่านี้มีความปลอดภัยน้อยกว่า ผู้ดูแลระบบควรแก้ไขรหัสผ่านของนักเรียนและอัปเดตรหัสทุกครั้งหากเกิดการสูญหายหรือถูกเปิดเผยต่อผู้อื่น
- โรงเรียนควรให้ความรู้แก่ทั้งนักเรียนและผู้ปกครองเกี่ยวกับความสำคัญของการเก็บรหัสผ่านเป็นความลับและการจัดเก็บข้อมูลเข้าสู่ระบบอื่นๆ อย่างปลอดภัย เช่น คิวอาร์โค้ด
- PIN สำหรับอุปกรณ์โดยเฉพาะเป็นวิธีการตรวจสอบสิทธิ์ที่ปลอดภัยอีกทางหนึ่งสำหรับอุปกรณ์ที่มอบหมายอย่างแท็บเล็ต

ใช้การตั้งค่าความปลอดภัยที่เหมาะสม

อุปกรณ์และเครือข่ายของโรงเรียนเป็นเป้าหมายที่ชัดเจนและมีมูลค่าสูงในสายตาของผู้โจมตีทั่วโลก จึงจำเป็นอย่างยิ่งที่จะต้องรักษาความปลอดภัยให้ดีที่สุดเท่าที่จะเป็นไปได้เพื่อป้องกันไม่ให้เกิดการสูญเสียบริการ ทรัพยากร เวลา และเงิน ผู้ดูแลระบบควรใช้ฟีเจอร์ความปลอดภัยที่มีประสิทธิภาพและเหมาะสมซึ่งมาพร้อมกับผลิตภัณฑ์ที่สถาบันใช้และต้องพิจารณาด้วยว่าครู เจ้าหน้าที่ และนักเรียนสามารถใช้งานระบบเหล่านี้ได้อย่างสะดวกหรือไม่ ดังนั้น ควรกำหนดการตั้งค่าความปลอดภัยและความเป็นส่วนตัวที่สำคัญเพื่อให้ผู้ใช้แต่ละรายไม่สามารถปิดใช้งานหรือแก้ไขการตั้งค่าเหล่านี้ได้ด้วยตนเอง นอกจากนี้ การตั้งค่าอื่นๆ ก็ควรได้รับการป้องกันที่เป็นค่าเริ่มต้นซึ่งกำหนดโดยผู้ดูแลระบบด้วย การใช้การรักษาความปลอดภัยที่ดีที่สุดเท่าที่จะเป็นไปได้จึงสำคัญอย่างยิ่งต่อการป้องกันการสูญเสียบริการ ทรัพยากร เวลา และเงิน หากใช้ Chromebook คุณสามารถดูคำแนะนำในการกำหนดนโยบายด้านอุปกรณ์ได้ในส่วนสุดท้าย

สุดท้าย เราขอแนะนำให้สร้าง "ขอบเขตการใช้ข้อมูล" ไว้ในแนวทางปฏิบัติ โดยจำกัดวัตถุประสงค์ ตลอดจนวิธีรวบรวม ใช้งาน และเปิดเผยข้อมูลส่วนบุคคลของแต่ละคนให้เหลือเท่าที่จำเป็นอย่างสมเหตุสมผลและอยู่ในสัดส่วนที่เหมาะสมสำหรับการให้บริการ หรือสอดคล้องกับบริบทของความสัมพันธ์

แอปพลิเคชันและการอัปเดต

จำกัดและลดจำนวนแอปที่ผู้ใช้ติดตั้งได้เองเพราะแอปพลิเคชันแต่ละรายการที่ติดตั้งบนอุปกรณ์ถือเป็นเวกเตอร์การโจมตีที่อาจทำให้เกิดช่องโหว่ หากเป็นไปได้ ให้ใช้แอปพลิเคชันจากแหล่งที่มาที่เชื่อถือได้ ตัวอย่างเช่น แนะนำให้ผู้ใช้ตรวจสอบป้ายสถานะการยืนยันบน Google Play Store เพื่อให้แน่ใจว่ากำลังดาวน์โหลดแอปพลิเคชันอย่างเป็นทางการที่ผ่านการตรวจสอบความปลอดภัยแล้ว การปรับเปลี่ยนระบบปฏิบัติการหรือฮาร์ดแวร์ (การเจลเบรกหรือการรูท) จะทำให้เกิดข้อบกพร่องด้านความปลอดภัยที่สำคัญและเป็นสิ่งที่ควรหลีกเลี่ยง

การเข้าถึงและระดับการแชร์ข้อมูล

ผู้ดูแลระบบควรตรวจสอบว่าผู้ใช้มีสิทธิเข้าถึงข้อมูล ซอฟต์แวร์ บริการ และระบบที่จำเป็นต่อการปฏิบัติหน้าที่หรือเรียนรู้อย่างมีประสิทธิภาพเท่านั้น ซึ่งจะช่วยจำกัดการเข้าถึงโดยไม่ตั้งใจและติดตามได้ว่าใครมีสิทธิเข้าถึงทรัพยากรใดบ้าง สิ่งที่ต้องใส่ใจเป็นพิเศษคือข้อมูลที่ละเอียดอ่อนมากอย่าง PII ของผู้ใช้และระบบต่างๆ (เช่น ทรัพยากรบุคคล เงินเดือน การให้คะแนน ความปลอดภัย และการกำหนดค่า) ซึ่งควรตรวจสอบว่าผู้ใช้รายใดเข้าถึงข้อมูลได้บ้างและภายใต้สถานการณ์ใดด้วยการจำกัดการเข้าถึงอุปกรณ์ของโรงเรียนและกำหนดให้มีเพียงเจ้าหน้าที่บางรายเท่านั้นที่มีสิทธิเข้าถึง

อ่านนโยบายการแชร์ข้อมูลในเครื่องมือการทำงานร่วมกันเพื่อป้องกันการแชร์ข้อมูลที่ไม่เหมาะสมหรือมากเกินความจำเป็น และการเข้าถึงที่ไม่ได้รับอนุญาต จำกัดหรือบล็อกการแชร์นอกสภาพแวดล้อมของคุณ (โดยเฉพาะสำหรับนักเรียน) และบังคับใช้นโยบายที่ตรวจสอบการแชร์เนื้อหาที่ละเอียดอ่อน

การสูญหายหรือการขโมยอุปกรณ์

การที่อุปกรณ์สูญหายไม่ได้หมายความว่าคุณจะสูญเสียข้อมูลไปด้วย ผู้ดูแลระบบควรกำหนดแผนการซึ่งเป็นมาตรฐานเพื่อให้แน่ใจว่าจะเข้าถึงข้อมูลและเอกสารได้ในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย เช่น การเก็บเอกสารไว้ในสภาพแวดล้อมระบบคลาวด์ หรือดาวน์โหลดและพิมพ์รหัสสำรองสำหรับกระบวนการยืนยันแบบ 2 ขั้นตอนเพื่อไม่ให้การเข้าถึงบัญชีต้องหยุดชะงัก

เมื่อมีการรายงานว่าอุปกรณ์สูญหายหรือถูกขโมย หากเป็นไปได้ควรตรวจสอบว่าได้ทำมีการล็อกอุปกรณ์จากระยะไกลแล้ว และล็อกหรือแจ้งให้บัญชีที่เกี่ยวข้องทราบแล้วแล้วเพื่อป้องกันไม่ให้สามารถใช้อุปกรณ์นั้นเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต คุณสามารถล้างข้อมูล Chromebook จากระยะไกลในกรณีที่อุปกรณ์สูญหายและตรวจสอบบัญชี Google Workspace for Education เพื่อหากิจกรรมที่น่าสงสัยหรือถูกระงับ (ล็อก) ได้ หากจำเป็น

การปกป้องขั้นสูงสำหรับผู้ใช้ที่มีความเสี่ยงสูง

Google มีโปรแกรมการปกป้องขั้นสูง (APP) สำหรับผู้ใช้ที่มีระดับการเข้าถึงสูงและข้อมูลที่ละเอียดอ่อน (รวมถึงผู้ดูแลระบบ Google Workspace for Education) โดย APP จะปกป้องผู้ใช้ได้มากกว่าเมื่อมีการโจมตีแบบกำหนดเป้าหมาย เช่น การพยายามทำฟิชชิง การดาวน์โหลดที่เป็นอันตราย และการละเมิดรหัสผ่าน APP ได้รับการออกแบบมาโดยเฉพาะเพื่อป้องกันการโจมตีออนไลน์แบบกำหนดเป้าหมายในบัญชี Google รวมถึงใช้การตรวจสอบสิทธิที่รัดกุม คีย์ความปลอดภัย และจำกัดการเข้าถึงข้อมูลของบัญชีโดยบุคคลที่สามได้อัตโนมัติ นอกจากนี้ ผู้ให้บริการบัญชีออนไลน์รายอื่นยังมอบวิธีป้องกันบัญชีที่แข็งแกร่งให้กับผู้ใช้ที่มีความเสี่ยงสูงด้วยเช่นกัน ผู้ดูแลระบบและเจ้าหน้าที่ควรใช้การป้องกันเหล่านี้เสมอ หากมีสิทธิเข้าถึงข้อมูลส่วนบุคคลหรือระบบเทคโนโลยี

อัปเดตและอัปเกรดระบบของคุณ

สิ่งที่สำคัญที่สุดอย่างหนึ่งที่ทุกคนทำได้เพื่อปกป้องตนเองก็คือการอัปเดตระบบปฏิบัติการของอุปกรณ์และแอปพลิเคชันอยู่เสมอ ซึ่งถือเป็นเรื่องที่สำคัญมากสำหรับสถาบันการศึกษาระดับ K-12 เนื่องจากเป็นส่วนสำคัญในการศึกษาและชีวิตประจำวันของเด็กๆ การโจมตีด้วยมัลแวร์ส่วนใหญ่ทั้งในสภาพแวดล้อมการศึกษาและสภาพแวดล้อมที่มีความเสี่ยงสูงอื่นๆ เป็นการโจมตีบนระบบ Windows ไม่ว่าจะเป็น SolarWinds, การโจมตีโดยแรนซัมแวร์ในเขตการศึกษาลอสแอนเจลิสยูนิฟายด์, การแฮ็กเขตการศึกษาลิตเติลร็อก, การละเมิดข้อมูลบนเซิร์ฟเวอร์ Microsoft Exchange, การโจมตีโดยแรนซัมแวร์ในเขตการศึกษาแอลบูเคอร์คี และการละเมิดหน่วยงานรัฐบาลในระบบของ Microsoft ที่เกิดขึ้นเมื่อไม่นานมานี้ สถานการณ์เหล่านี้แสดงให้เห็นว่าการใช้ผลิตภัณฑ์และบริการระบบคลาวด์จะทำให้งานของผู้ดูแลระบบง่ายขึ้น โดยลดพื้นที่การโจมตีและช่วยให้มั่นใจได้ว่าระบบและแอปพลิเคชันจะทันสมัยอยู่เสมอโดยอัตโนมัติ

อัปเกรดเป็นระบบปฏิบัติการที่ทันสมัยและเป็นเวอร์ชันล่าสุดเสมอ

ระบบปฏิบัติการ (OS) เวอร์ชันล่าสุดมักจะมีฟีเจอร์ความปลอดภัยใหม่ๆ ที่ช่วยป้องกันเวกเตอร์การโจมตีที่รู้จัก คุณควรเปิดใช้ฟังก์ชันการอัปเดตอัตโนมัติในระบบปฏิบัติการของอุปกรณ์ หรือหากทำการอัปเดตอัตโนมัติไม่ได้ ให้ดาวน์โหลดและติดตั้งแพตช์ จากนั้นทำการอัปเดตจากผู้ให้บริการที่เชื่อถือได้อย่างน้อยเดือนละครั้ง

Chromebook ทำงานบน ChromeOS จึงมีการอัปเดตอัตโนมัติบ่อยครั้งด้วยแพตช์ด้านความปลอดภัยล่าสุด เพื่อให้สามารถนำนวัตกรรมความปลอดภัยล่าสุดมาใช้ได้อย่างรวดเร็ว และจะตรวจสอบความสมบูรณ์ของระบบปฏิบัติการแบบอ่านอย่างเดียวก่อนเปิดเครื่อง อีกทั้งยังเข้ารหัสข้อมูลทั้งหมดที่จัดเก็บไว้ในอุปกรณ์ ปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเรียกใช้ทุกหน้าเว็บและแอปพลิเคชันในแซนด์บ็อกซ์ที่แยกจากกัน ดังนั้นหากเว็บไซต์หรือแอปหนึ่งติดมัลแวร์ ก็จะไม่สามารถแพร่กระจายไปยังส่วนอื่นๆ ของอุปกรณ์ได้

หากโรงเรียนของคุณยังไม่พร้อมที่จะเปลี่ยนไปใช้ Chromebook เรามี ChromeOS Flex ซึ่งเป็น ChromeOS เวอร์ชันที่สร้างมาเพื่อปรับปรุงให้อุปกรณ์ของโรงเรียนทันสมัย ChromeOS Flex จะมอบประสบการณ์การเรียนการสอนที่ทันสมัยและครบวงจรให้กับทุกคนและยังมาพร้อมความสามารถในการรักษาความปลอดภัยเชิงรุกและการจัดการในระบบคลาวด์ Flex สามารถมอบการป้องกันแบบอัตโนมัติ รวมถึงบล็อกโปรแกรมและแอปที่เป็นอันตรายโดยที่คุณไม่ต้องเปลี่ยนฮาร์ดแวร์ที่ใช้อยู่

อัปเกรดเป็นเบราว์เซอร์ที่ทันสมัยและเป็นเวอร์ชันล่าสุดเสมอ

การอัปเดตเบราว์เซอร์ให้ทันสมัยและปลอดภัยเป็นเรื่องสำคัญ เบราว์เซอร์ที่ทันสมัยมีฟีเจอร์ความปลอดภัยที่ล้ำหน้ากว่าและสามารถแจ้งให้ผู้ใช้เปิดใช้งานได้อย่างง่ายดาย หรือจะให้ผู้ดูแลระบบกำหนดค่าให้มีการเปิดใช้ฟีเจอร์เหล่านี้ตามค่าเริ่มต้นบนคอมพิวเตอร์ของสถาบันก็ได้ ซึ่งจะช่วยปกป้องความลับของข้อมูลที่ละเอียดอ่อนก็ส่งผ่านอินเทอร์เน็ต อย่างไรก็ดี เบราว์เซอร์ต้องได้รับการอัปเดตอยู่เสมอ ไม่ว่าจะใช้ในการทำงาน เรียนรู้ หรือทำกิจกรรมออนไลน์อื่นๆ เบราว์เซอร์ที่ทันสมัยจะมีลักษณะดังนี้

- **ใช้การรักษาความปลอดภัยที่มีประสิทธิภาพ** รวมถึงการแยกเว็บไซต์และการปกป้องด้วย Google Safe Browsing เพื่อป้องกันไม่ให้ผู้ใช้เข้าเว็บไซต์ที่อันตรายโดยไม่ตั้งใจ
- **เปิดใช้การอัปเดตอัตโนมัติ**เพื่อให้แน่ใจว่าเบราว์เซอร์ได้รับการอัปเดตความปลอดภัยอย่างรวดเร็ว
- **ตรวจสอบว่าการเชื่อมต่อปลอดภัย** เบราว์เซอร์ที่ทันสมัยควรใช้ Transport Layer Security (TLS) โดยผู้ใช้จะคลิกที่ข้าง URL และตรวจสอบได้ว่าการเชื่อมต่อมีเครื่องหมายว่าปลอดภัยหรือไม่

Chrome สร้างขึ้นโดยคำนึงถึงความปลอดภัยและมาพร้อมฟีเจอร์ความปลอดภัยต่างๆ เช่น Google Safe Browsing ที่เปิดอยู่โดยค่าเริ่มต้น และยังมีเครื่องมือจัดการรหัสผ่านในตัวที่จะกรอกรหัสผ่านโดยอัตโนมัติขณะที่คุณท่องเว็บ ซึ่งทำให้คุณใช้รหัสผ่านที่รัดกุมได้อย่างสะดวกสบาย

ใช้ระบบแจ้งเตือนและตรวจสอบแบบเรียลไทม์

ระบบแจ้งเตือนและตรวจสอบแบบเรียลไทม์ช่วยให้โรงเรียนตรวจสอบและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วก่อนจะเกิด ความเสียหาย การมีเครื่องมือรักษาความปลอดภัยที่ทำงานอยู่เบื้องหลังเพื่อรวบรวมและบันทึกการดำเนินการด้านความปลอดภัยจากทั่วทั้งระบบเป็นสิ่งที่สำคัญ เครื่องมือ AI มีประสิทธิภาพดีในการกรองข้อมูลจำนวนมากที่รวบรวมไว้เพื่อค้นหาความผิดปกติและรูปแบบ ซึ่งสามารถนำมาใช้ตรวจจับภัยคุกคามได้อย่างรวดเร็วและสะดวกยิ่งขึ้น รวมถึงเพื่อประมวลผลและแก้ไขช่องโหว่ อีกทั้งยังช่วยให้สามารถจัดลำดับความสำคัญของกิจกรรมที่ต้องได้รับการตรวจสอบโดยผู้ดูแลระบบไอทีหรือเจ้าหน้าที่

โรงเรียนต่างๆ สามารถใช้ฟีเจอร์การแจ้งเตือนและการตรวจสอบซึ่งมาพร้อมซอฟต์แวร์หลักที่ใช้สำหรับการทำงานร่วมกันและการสื่อสาร เช่น Google Workspace for Education หรือจะใช้โซลูชันการจัดการข้อมูลและการดำเนินการด้านความปลอดภัย (SIEM) แยกต่างหากก็ได้

ระบบแจ้งเตือนและตรวจสอบแบบเรียลไทม์จะติดตามกิจกรรมต่างๆ ทั่วทั้งเครือข่าย อุปกรณ์ แอปพลิเคชัน ผู้ใช้ และข้อมูลของโรงเรียน เช่น การเข้าสู่ระบบของผู้ใช้ การเข้าถึงไฟล์ การบุกรุกที่อาจเกิดขึ้น การขโมยหรือการพยายามขโมยข้อมูล และกิจกรรมอื่นๆ ของผู้ดูแลระบบ

หากระบบตรวจพบกิจกรรมที่น่าสงสัย ก็จะส่งการแจ้งเตือนไปยังเจ้าหน้าที่ไอทีของโรงเรียน ซึ่งช่วยให้ผู้ดูแลระบบตรวจสอบปัญหาและดำเนินการเพื่อจัดการกับภัยคุกคามได้อย่างทันท่วงที

นอกจากนี้ คุณยังใช้เครื่องมือแจ้งเตือนและตรวจสอบเพื่อทำความเข้าใจภัยคุกคามที่โรงเรียนต้องเผชิญให้ลึกซึ้งยิ่งขึ้นได้ การวิเคราะห์ข้อมูลจากระบบเรียลไทม์เหล่านี้ทำให้โรงเรียนสามารถระบุแนวโน้มและรูปแบบที่ช่วยให้ปกป้องตนเองได้ดียิ่งขึ้น

แนวทางปฏิบัติแนะนำในการใช้ระบบแจ้งเตือนและติดตาม (รวมถึง SIEM) มีดังนี้

1. **ระบุเป้าหมายด้านการรักษาความปลอดภัย**
ระบุว่าข้อมูลและระบบใดมีความสำคัญที่สุดสำหรับโรงเรียน และภัยคุกคามประเภทใดที่มีความเสี่ยงมากที่สุดต่อข้อมูลและระบบดังกล่าว จากนั้นจึงระบุข้อมูลที่ต้องการรวบรวมเพื่อตรวจสอบภัยคุกคามเหล่านั้น

2. **เก็บข้อมูลที่ถูกต้องและกำหนดค่าอย่างเหมาะสม**
คุณควรรวบรวมข้อมูลที่ถูกต้องและกำหนดค่าแอปพลิเคชันเพื่อให้บรรลุเป้าหมายด้านความปลอดภัยที่เกี่ยวข้องที่สุด โดยอาจรวมถึงข้อมูลจากไฟร์วอลล์ ตัวกรองเนื้อหา ระบบตรวจจับการบุกรุก เว็บเซิร์ฟเวอร์ และอุปกรณ์รักษาความปลอดภัยอื่นๆ ตลอดจนซอฟต์แวร์การสื่อสารและการทำงานร่วมกัน ระบบข้อมูลโรงเรียน และระบบบริหารจัดการการเรียนรู้

3. **ตรวจสอบและตอบสนองเมื่อมีการแจ้งเตือนการแจ้งเตือน**
เมื่อระบบทำการแจ้งเตือน คุณก็ควรตรวจสอบปัญหาและดำเนินการอย่างเหมาะสมด้วยเช่นกัน บางครั้งอาจต้องทำงานร่วมกันหลายทีมเพื่อตรวจสอบแหล่งที่มาของการแจ้งเตือน อย่างไรก็ดี ขอแนะนำให้พิจารณาว่าเป็นภัยคุกคามจริงหรือไม่ หรือดำเนินการบางอย่างเพื่อจัดการกับภัยคุกคาม เช่น การระงับบัญชี การรีเซ็ตรหัสผ่านของผู้ใช้ การกักเก็บหรือการลบอีเมล การเปลี่ยนแปลงสิทธิในไฟล์ หรือการล้างข้อมูลในอุปกรณ์

ฝึกครู เจ้าหน้าที่ และนักเรียน

สถาบันการศึกษาระดับ K-12 ควรยกระดับการรับรู้และสร้างเสริมนิสัยที่เกี่ยวข้องกับการรักษาความปลอดภัยของชุมชนโรงเรียน โดยใช้แคมเปญและการร่วมมือเพื่อส่งเสริมผู้ใช้ การให้ความรู้แก่ครู เจ้าหน้าที่ และนักเรียนเกี่ยวกับความสำคัญของความปลอดภัยเป็นสิ่งที่จะช่วยให้ทุกคนปกป้องตัวเองในโลกออนไลน์ และช่วยป้องกันภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ร้ายแรง สอนให้พวกเขารู้วิธีใช้ผลิตภัณฑ์และบริการที่มีในสถาบัน วิธีตรวจจับและรายงานภัยคุกคาม เช่น อีเมลฟิชชิง และที่สำคัญที่สุด คือวิธีดำเนินการเพื่อป้องกันการโจมตีเหล่านี้ โรงเรียนและเขตการศึกษาควรยกระดับการรับรู้และสร้างเสริมนิสัยที่เกี่ยวข้องกับการรักษาความปลอดภัยของชุมชนโรงเรียน โดยใช้แคมเปญและการร่วมมือเพื่อส่งเสริมผู้ใช้

วิธีใช้อุปกรณ์และซอฟต์แวร์อย่างปลอดภัย

ผู้ดูแลระบบอาจร่วมมือกับครูและผู้เชี่ยวชาญในการพัฒนาหลักสูตรการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับที่เหมาะสมกับวัยเพื่อช่วยให้นักเรียนเข้าใจวิธีใช้อุปกรณ์ ซอฟต์แวร์ และระบบอย่างปลอดภัย การสร้างสื่อการฝึกอบรมของโรงเรียนหรือเขตการศึกษาโดยเฉพาะจะช่วยให้คำแนะนำที่เหมาะกับบริบทแก่ครูและนักเรียน นอกจากนี้ คุณยังใช้ประโยชน์จากสื่อสำเร็จรูปที่มีอยู่ เช่น โปรแกรม Be Internet Awesome บน Safety.Google และ Khan Academy แล้วนำมาปรับแต่งให้เข้ากับความต้องการของตนเองได้อีกด้วย โปรแกรมเหล่านี้จะช่วยให้ผู้ใช้ของคุณปลอดภัยไม่ว่าจะอยู่ในโรงเรียนหรือชุมชน

การสังเกตภัยคุกคาม

การฝึกครู เจ้าหน้าที่ และนักเรียนให้สังเกตเห็นภัยคุกคามเป็นส่วนสำคัญในการปกป้องตนเองให้ปลอดภัย การสอนเด็กๆ ให้รู้วิธีแยกแยะภัยคุกคามเป็นเรื่องสำคัญ เนื่องจากเด็กเหล่านี้อาจไม่รู้ว่าต้องทำอย่างไร จึงจะแยกแยะได้ว่าสิ่งใดถูกต้อง เด็กๆ ควรรู้จักภัยคุกคามบางประเภทและเข้าใจวิธีรายงาน ผู้ดูแลระบบจึงควรเน้นหัวข้อที่คิดว่าจะให้ผลลัพธ์ที่ดีที่สุดจากการฝึกอบรม ที่สำคัญ การฝึกต้องไม่เพียงแค่สอนให้ผู้ใช้รับรู้ถึงภัยคุกคามเท่านั้น แต่ต้องบอกวิธีดำเนินการด้วย ภัยคุกคามทั่วไปที่ผู้ใช้ควรรู้จัก ได้แก่ แรนซัมแวร์ ฟิชชิง วิศวกรรมสังคม มัลแวร์ และกลโกง ในกรณีที่สถาบันเผชิญกับภัยคุกคามบางชนิดเป็นประจำ ขอแนะนำให้เน้นย้ำการให้ความรู้เกี่ยวกับภัยคุกคามนั้นๆ แก่ชุมชนโรงเรียนเป็นพิเศษ

รักษาความปลอดภัยของข้อมูลและการแชร์ไฟล์

ครูและเจ้าหน้าที่ควรได้รับการฝึกอบรมเกี่ยวกับการแชร์ไฟล์และข้อมูลอย่างเหมาะสม รวมถึงวิธีสังเกตคำขอที่ไม่เหมาะสมผ่านทางอีเมล โดยทั่วไป แล้วครูและเจ้าหน้าที่ควรทราบว่าควรแชร์และประมวลผลข้อมูลส่วนบุคคลที่ละเอียดอ่อนเมื่อจำเป็นเท่านั้น และควรต้องป้องกันข้อมูลเพิ่มเติมอีกชั้นเสมอ เช่น ต้องไม่แชร์ผ่านอีเมลหรือกับบุคคลภายนอก ขอแนะนำให้ครูและเจ้าหน้าที่ใช้ความสามารถในการป้องกันข้อมูลรั่วไหล (รวมอยู่ใน ChromeOS และ Workspace for Education) เพื่อเตือนและป้องกันไม่ให้ผู้ใช้ปลายทางแชร์ไฟล์ซึ่งมีข้อมูลที่ละเอียดอ่อน (เช่น หมายเลขประกันสังคม) หรือคัดลอกและวางเนื้อหาที่ละเอียดอ่อนนอกโดเมน

การนำแนวทางของ Google มาใช้ในสถานการณ์จริง: อุปกรณ์และบริการสำหรับการศึกษา

กระบวนการการจัดหาซอฟต์แวร์เป็นหนึ่งในวิธีที่ทรงพลังที่สุดที่เขตการศึกษาใช้ปกป้องตนเองได้ ซอฟต์แวร์ควรได้รับการออกแบบและมีสถาปัตยกรรมที่แข็งแกร่งเพื่อลดความเสี่ยงในการเกิดช่องโหว่ และมาพร้อมการรักษาความปลอดภัยในตัวทุกชั้น การกำหนดให้โรงเรียนซื้อซอฟต์แวร์ที่ปลอดภัยหรือจากบริษัทที่มีประวัติด้านความปลอดภัยที่ได้รับการพิสูจน์แล้วสามารถช่วยลดความเสี่ยงทางไซเบอร์ในวงกว้างได้เป็นอย่างมาก ตัวอย่างเช่น Google ได้ปรับปรุง ChromeOS ของเราให้แข็งแกร่งขึ้นขณะเดียวกันก็ใช้โซลูชันอัจฉริยะเชิงรุกที่ใช้ประโยชน์จากจุดแข็งของความเชี่ยวชาญที่เรามีด้านแมชชีนเลิร์นนิง

Google มุ่งมั่นสร้างสรรค์ผลิตภัณฑ์ซึ่งจะช่วยปกป้องความเป็นส่วนตัวของนักเรียนและครู รวมทั้งมอบความปลอดภัยในระดับที่ดีที่สุดสำหรับสถาบันของคุณ คุณสามารถวางใจได้ว่าผลิตภัณฑ์และบริการของ Google for Education จะปกป้องผู้ใช้ อุปกรณ์ และข้อมูลอย่างต่อเนื่องเพื่อให้ปลอดภัยจากภัยคุกคามอันซับซ้อนที่มีจำนวนเพิ่มขึ้นเรื่อยๆ ในส่วนนี้เราจะขออธิบายรายละเอียดของคำแนะนำต่างๆ ด้านความปลอดภัยเมื่อใช้ผลิตภัณฑ์ Google for Education สำหรับผู้ดูแลระบบไอทีของโรงเรียน

Google Workspace for Education

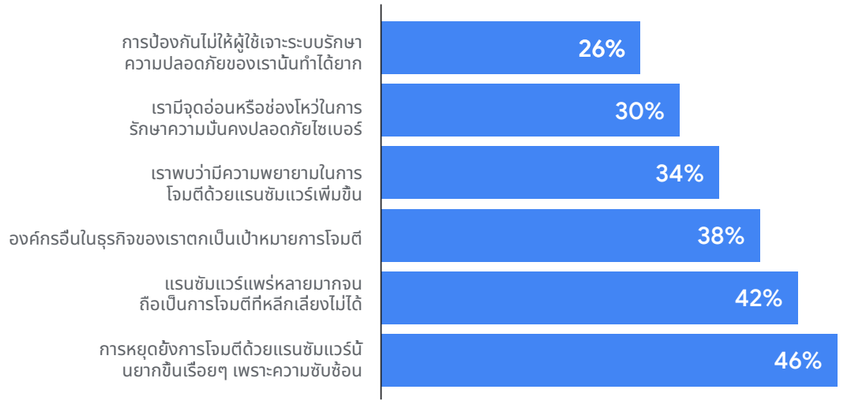
Google Workspace for Education คือชุดเครื่องมือและบริการของ Google ที่ออกแบบมาสำหรับโรงเรียนโดยเฉพาะ เพื่อทำงานร่วมกัน อำนวยความสะดวกให้การสอนดำเนินไปอย่างราบรื่น และทำให้การเรียนรู้ปลอดภัย ผลิตภัณฑ์และบริการของ Google for Education สามารถปกป้องผู้ใช้ อุปกรณ์ และข้อมูลอย่างต่อเนื่องเพื่อให้ปลอดภัยจากภัยคุกคามอันซับซ้อนที่มีจำนวนเพิ่มขึ้นเรื่อยๆ มาพร้อมเครื่องมือต่างๆ เช่น ศูนย์แจ้งเตือนและศูนย์ความปลอดภัย, ห้องนิรภัยสำหรับ eDiscovery, Identity and Access Management และการป้องกันข้อมูลรั่วไหล

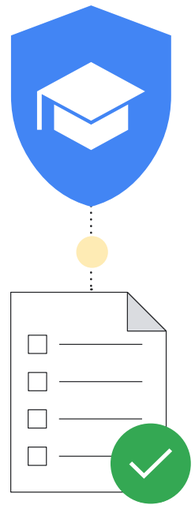
หากคุณเพิ่งเริ่มใช้งาน Google Workspace for Education เราได้รวบรวมสื่อที่มีประโยชน์ไว้ในเอกสารนี้แล้วซึ่งจะช่วยคุณตั้งค่าสิ่งต่างๆ ให้สอดคล้องกับคำแนะนำในคู่มือนี้ หากต้องการความช่วยเหลือในการเริ่มต้นใช้งาน Google Workspace for Education โปรดดูคู่มือการตั้งค่าไอทีฉบับย่อนี้

เช็กลิสต์สำหรับการรักษาความปลอดภัย

ดูข้อมูลเพิ่มเติมเกี่ยวกับวิธีเพิ่มความปลอดภัยและความเป็นส่วนตัวให้กับสถาบันได้ในเช็กลิสต์สำหรับการรักษาความปลอดภัย นอกจากนี้ โรงเรียนที่ใช้ Google Workspace for Education รุ่น Standard และ Plus ยังสามารถใช้หน้าความปลอดภัยของระบบเพื่อตรวจสอบการกำหนดค่าของคอนโซลผู้ดูแลระบบได้อีกด้วย อาทิเช่น คุณสามารถตรวจสอบสถานะของการตั้งค่าได้ เช่น การส่งต่ออีเมลอัตโนมัติ การเข้ารหัสอุปกรณ์ การตั้งค่าการแชร์ไดรฟ์ และอื่นๆ อีกมากมาย หรือหากจำเป็น คุณสามาร ปรับการตั้งค่าโดเมนตามหลักเกณฑ์ด้าน ความปลอดภัยทั่วไปและแนวทางปฏิบัติแนะนำไปพร้อมๆ กับปรับแนวทางเหล่านี้ให้เหมาะกับความต้องการทางธุรกิจและนโยบายการบริหารความเสี่ยงขององค์กรได้อีกด้วย

ทำไมวงการศึกษามักตกเป็นเป้าโจมตี





แหล่งที่มา: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

เคล็ดลับที่มีประโยชน์อื่นๆ ที่จะช่วยให้คุณสามารถใช้การป้องกันที่มาพร้อม Google Workspace for Education ได้อย่างเต็มประสิทธิภาพที่สุด มีดังนี้

ตั้งค่าหน่วยขององค์กร (OU)

ทุกคนคงเห็นด้วยว่าผู้ใช้ทั้งหมดในบัญชี Google Workspace for Education ของคุณจำเป็นต้องมีการตั้งค่าแบบเดียวกัน หน่วยองค์กรคือกลุ่มผู้ใช้ที่ให้คุณกำหนดบริการ การตั้งค่า และสิทธิต่างๆ แก่ผู้ใช้ที่แตกต่างกันได้ เช่น ใช้การยืนยันแบบ 2 ขั้นตอนสำหรับครูและเจ้าหน้าที่ และการตรวจสอบสิทธิที่เหมาะสมกับวัยสำหรับนักเรียนอายุน้อย ขอแนะนำให้ตั้งค่าหน่วยขององค์กรสำหรับเจ้าหน้าที่ ครู และนักเรียนแยกกันเพื่อให้บังคับใช้นโยบายที่แตกต่างกันกับผู้ใช้แต่ละกลุ่มต่างๆ ได้ การออกแบบโครงสร้างที่ดี¦เป็นปัจจัยสำคัญที่จะช่วยให้คุณจัดการบัญชี Google Workspace for Education ได้อย่างมีประสิทธิภาพและยืดหยุ่น

กำหนดนโยบายรหัสผ่านและการปกป้องบัญชีผู้ดูแลระบบ

ตามที่กล่าวไปแล้ว การตรวจสอบสิทธิผู้ใช้เป็นปัจจัยที่สำคัญอย่างยิ่งในการรักษาความปลอดภัยของสถาบัน เราจึงสร้างวิธีที่ยืดหยุ่นในการจัดการการตรวจสอบสิทธิสำหรับผู้ดูแลระบบ ซึ่งจะช่วยให้มั่นใจได้ว่าผู้ใช้มีการป้องกันบัญชีที่เหมาะสมและปลอดภัย กำหนดนโยบายรหัสผ่านเพื่อให้มั่นใจว่าผู้ใช้จะสร้างรหัสผ่านที่รัดกุม และพิจารณาการกำหนดให้ใช้การยืนยันแบบ 2 ขั้นตอนในกรณีที่เหมาะสมตามการจัดกลุ่มที่แนะนำในส่วนการลงชื่อเข้าใช้อย่างปลอดภัย คุณสามารถบังคับใช้การยืนยันแบบ 2 ขั้นตอนกับผู้ใช้บางส่วน (ให้ผู้ใช้มีเวลาตั้งค่า) แล้วใช้การยืนยันแบบ 2 ขั้นตอนผ่านวิธีต่างๆ ได้แก่ คีย์ความปลอดภัย (ปลอดภัยที่สุด), Google Prompt (ใช้แอปของ Google บน Android และ iOS), แอปสร้างรหัสยืนยัน (เช่น Google Authenticator) และข้อความหรือการโทร (แม้จะเป็นวิธีที่ปลอดภัยน้อยที่สุดก็ตาม)

หากองค์กรใช้ผู้ให้บริการข้อมูลประจำตัว (IdP) รายอื่นที่ไม่ใช่ Google คุณสามารถตั้งค่าการลงชื่อเพียงครั้งเดียว (SSO) ผ่านผู้ให้บริการข้อมูลประจำตัวบุคคลที่สามได้ และยังใช้การยืนยันแบบ 2 ขั้นตอนกับ SSO สำหรับบัญชีที่ไม่ใช่ผู้ดูแลระบบขั้นสูงได้อีกด้วย หากต้องการ

เปิดหรือปิดบริการ

จากคอนโซลผู้ดูแลระบบของ Google ผู้ดูแลระบบจะควบคุมได้ว่าผู้ใช้สามารถเข้าถึงบริการใดของ Google ด้วยบัญชี Google Workspace for Education คุณควบคุมการเข้าถึงบริการของ Google เช่น ปฏิทิน ไดรฟ์ และ Meet ได้โดยการเปิดหรือปิดบริการตามหน่วยขององค์กร (OU) (และเปิดบริการเมื่อใช้ Groups ได้ด้วย) รวมถึงสามารถตรวจสอบความแตกต่างระหว่างบริการหลักและบริการเพิ่มเติมของ Workspace ก่อนเปิดใช้บริการเพิ่มเติม เช่น YouTube, Google Maps และ Blogger เราขอแนะนำให้ผู้ดูแลระบบกำหนดการเข้าถึงบริการของ Google ตามอายุ และโปรดทราบว่าข้อจำกัดในการใช้บริการบางอย่างของ Google จะมีผลกับผู้ใช้ที่มีอายุต่ำกว่า 18 ปีโดยอัตโนมัติเมื่อลงชื่อเข้าใช้บัญชี Google Workspace for Education

นอกจากนี้ คุณยังใช้การเข้าถึงแบบ Context-Aware (ใช้ได้ใน Workspace for Education Standard และ Plus) เพื่ออนุญาตหรือบล็อกการเข้าถึงแอป Google เช่น Gmail, ไดรฟ์ และปฏิทินตามที่อยู่ IP, ต้นทางทางภูมิศาสตร์, นโยบายความปลอดภัย หรือระบบปฏิบัติการของอุปกรณ์ เช่น อนุญาตให้ใช้ไดรฟ์สำหรับเดสก์ท็อปได้เฉพาะในอุปกรณ์ของบริษัทในประเทศ/ภูมิภาคที่ระบุเท่านั้น

วิธีการให้สิทธิเข้าถึงบริการแก่ผู้ใช้

ในคอนโซลผู้ดูแลระบบของ Google คุณสามารถปิดไม่ให้หน่วยขององค์กรเข้าถึงบริการของ Google เช่น Google ไดรฟ์ แต่หากมีผู้ใช้บางรายในหน่วยขององค์กรจำเป็นต้องใช้ไดรฟ์ คุณสามารถเลือกดำเนินการได้ 2 วิธี ดังนี้

1. ย้ายผู้ใช้ไปยังหน่วยขององค์กรที่เปิดให้ใช้ไดรฟ์
2. เพิ่มผู้ใช้ในกลุ่มที่มีสิทธิเข้าถึง แล้วเปิดไดรฟ์ให้กับกลุ่ม เมื่อใช้วิธีนี้สมาชิกแต่ละรายจะสามารถเข้าถึงบริการได้ แม้ว่าหน่วยองค์กรของตนจะปิดบริการเอาไว้ก็ตาม

แหล่งที่มา: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

กำหนดนโยบายการแชร์ข้อมูลและกฎการเก็บรักษา

ในฐานะผู้ดูแลระบบ คุณสามารถควบคุมว่าผู้ใช้จะแชร์ไฟล์และโฟลเดอร์ Google ไดรฟ์กับบุคคลภายนอกองค์กรได้หรือไม่ วิธีนี้จะช่วยป้องกันการแชร์ข้อมูลและไฟล์โดยไม่ได้ตั้งใจหรือในวงกว้างเกินไป และป้องกันไม่ให้ข้อมูลรั่วไหล การแยกไฟล์และไดรฟ์ การสร้างหน่วยองค์กร และการดำเนินการภายใต้หลักการให้สิทธิขั้นต่ำที่สุดเป็นสิ่งสำคัญในการป้องกันไม่ให้ผู้โจมตีเคลื่อนไหวข้ามเครือข่าย หากผู้โจมตีแฝงตัวเข้ามาในบัญชีเดียว ยิ่งผู้โจมตีเข้าถึงข้อมูลและเครือข่ายได้น้อย ความเสียหายก็จะยิ่งน้อยลง

ปิดการแชร์ไฟล์ภายนอกสำหรับนักเรียน (หรือจำกัดการแชร์ภายนอกไปยังโดเมนที่อนุญาตเท่านั้น) และตั้งค่า "เครื่องมือตรวจสอบสิทธิการเข้าถึง" เป็น "ผู้รับเท่านั้น" หากอนุญาตให้ผู้ใช้บางรายหรือทั้งหมดแชร์ไฟล์นอกโดเมน ให้เปิดใช้คำเตือนเมื่อผู้ใช้ดำเนินการ รวมทั้งปิดใช้การเผยแพร่ไฟล์บนเว็บ และกำหนดให้บุคคลภายนอกที่ทำงานร่วมกันลงชื่อเข้าใช้ด้วยบัญชี Google เท่านั้น

นอกจากนี้ ลูกค้า Workspace for Education Standard และ Plus ยังใช้กลุ่มเป้าหมายและกฎการเชื่อถือเพื่อกำหนดคำแนะนำและข้อจำกัดการแชร์ในระดับที่ละเอียดกว่าได้อีกด้วย ตัวอย่างเช่น เมื่อใช้กลุ่มเป้าหมาย คุณจะตั้งค่ากลุ่มเป้าหมายการแชร์ลิงก์เริ่มต้นสำหรับครูเป็น "ครูและเจ้าหน้าที่" ได้ แทนที่จะเป็นทุกคนในสถาบัน ส่วนกฎการเชื่อถือจะช่วยให้คุณสามารถบล็อกนักเรียนระดับประถมศึกษาไม่ให้แชร์ไฟล์กับนักเรียนในระดับชั้นที่สูงกว่าได้

ตรวจสอบนโยบายไดรฟ์ที่แชร์เพื่อให้แน่ใจว่ามีเพียงผู้ใช้ที่เหมาะสมเท่านั้นที่สามารถสร้างไดรฟ์ที่แชร์และป้องกันไม่ให้ผู้ใช้ภายนอกเข้าถึงไดรฟ์ที่แชร์ เราขอแนะนำให้คุณอนุญาตให้มีเพียงผู้ดูแลระบบ (หรือเจ้าหน้าที่และครู) เท่านั้นที่สร้างไดรฟ์ที่แชร์ได้ และจัดการการเข้าถึงไดรฟ์ที่แชร์อย่างใกล้ชิด

หากเป็นไปได้ ให้พิจารณาการจำกัดระดับการเข้าถึงไดเรกทอรีและการแชร์รายชื่อติดต่อ โดยอาจปิดใช้การแชร์รายชื่อติดต่อสำหรับผู้ใช้บางรายหรือทั้งหมดหรือสร้างไดเรกทอรีที่กำหนดเองเพื่อจำกัดว่าใครจะเห็นผู้ใช้รายใดบ้าง กำหนดนโยบายการป้องกันข้อมูลรั่วไหล (DLP) ในไดรฟ์และ Gmail เพื่อตรวจหาและบล็อกข้อมูลที่ละเอียดอ่อน เรามีนโยบายที่สร้างไว้ล่วงหน้าซึ่งสามารถนำมาใช้ประโยชน์เพื่อปกป้องข้อมูลที่ละเอียดอ่อนทั่วไป (เช่น ข้อมูลธนาคารหรือหมายเลขบัตรเครดิต) นอกจากนี้ คุณยังสามารถสร้างนโยบายที่กำหนดเองตามคีย์เวิร์ด รายการคำ และนิพจน์ทั่วไป (Regex) ได้อีกด้วย

จัดการการตั้งค่า Gmail

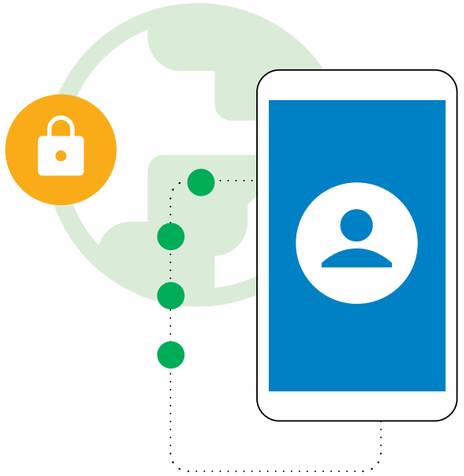
Gmail เป็นหนึ่งในบริการหลักของ Google Workspace for Education และมีการตั้งค่าหลายอย่างที่ผู้ดูแลระบบ สามารถนำไปใช้เพื่อปกป้องสถาบันและผู้ใช้ได้ ป้องกันจดหมายขยะ การปลอมแปลง และฟิชชิงด้วยการตรวจสอบสิทธิ์ของ Gmail ปรับแต่งการตั้งค่าตัวกรองจดหมายขยะ รวมถึงกำหนดการตรวจสอบสิทธิ์ผู้ส่งสำหรับผู้ส่งที่ได้รับอนุมัติทั้งหมดและปิดใช้การข้ามตัวกรองจดหมายขยะสำหรับผู้ส่งภายใน

ปิดใช้การเข้าถึงแบบ POP/IMAP หากเป็นไปได้ รวมถึงเปิดใช้การสแกนข้อความก่อนส่งแบบพิเศษและการป้องกันฟิชชิงและมัลแวร์ขั้นสูง คุณก็สามารถเปิดใช้คำเตือนสำหรับผู้รับภายนอกหากอนุญาตให้ผู้ใช้บางรายหรือทั้งหมดส่งอีเมลไปยังภายนอกได้

ลูกค้า Google Workspace for Education Standard และ Plus ยังช่วยป้องกันมัลแวร์และแรนซัมแวร์ได้ด้วยการตั้งค่ากฎเพื่อตรวจหาไฟล์แนบที่เป็นอันตรายโดยใช้แซนด์บ็อกซ์ความปลอดภัย

แอปพลิเคชันของบุคคลที่สาม

ใช้เวิร์กโฟลว์การอนุมัติในตัวเพื่ออนุมัติแอปพลิเคชันของบุคคลที่สามซึ่งเข้าถึงข้อมูลบัญชีผ่าน API วิธีนี้จะช่วยป้องกันไม่ให้มีการแชร์ข้อมูลที่ไม่ได้รับอนุญาตกับแอปพลิเคชันของบุคคลที่สามที่ไม่ผ่านการอนุมัติให้ใช้ในโรงเรียน



รายงานและการตรวจสอบ

ในฐานะผู้ดูแลระบบ คุณสามารถดูรายงานและบันทึกเหตุการณ์ในคอนโซลผู้ดูแลระบบของ Google เพื่อตรวจสอบกิจกรรมในองค์กร เช่น ความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้น ดูว่าใครลงชื่อเข้าใช้เมื่อใด ตลอดจนทำความเข้าใจวิธีที่ผู้ใช้สร้างและแชร์เนื้อหา นอกจากนี้ คุณยังสามารถดูข้อมูลระดับโดเมนไปพร้อมกับข้อมูลระดับผู้ใช้แบบละเอียดได้ในกราฟและตาราง ดูรายงานและบันทึกการตรวจสอบ (รวมถึงศูนย์แจ้งเตือน) เพื่อระบุความเสี่ยงด้านความปลอดภัย วิเคราะห์การใช้บริการ วินิจฉัยปัญหาการกำหนดค่า ติดตามกิจกรรมของผู้ใช้ และอื่นๆ อีกมากมาย

ผู้ดูแลระบบ Google Workspace for Education Standard และ Plus สามารถใช้ประโยชน์จากแดชบอร์ดความปลอดภัยเพื่อดูภาพรวมของรายงานความปลอดภัยต่างๆ ระบุแนวโน้ม รวมถึงเปรียบเทียบข้อมูลปัจจุบันและข้อมูลย้อนหลัง เช่น การแชร์ไฟล์ในไดรฟ์, กิจกรรมที่เป็นจดหมายขยะ ฟิชชิง และมัลแวร์ใน Gmail, การเข้าสู่ระบบบัญชีผู้ใช้ที่น่าสงสัย และกิจกรรมในอุปกรณ์ที่ น่าสงสัย บันทึกการใช้งาน กิจกรรม และการตรวจสอบส่วนใหญ่ รวมถึงเหตุการณ์ในบันทึกของผู้ดูแลระบบ, ไดรฟ์, Meet และ Chat พร้อมรายงานความปลอดภัยที่จะเก็บไว้ให้ 6 เดือน

ใช้ศูนย์ความปลอดภัยให้เป็นประโยชน์

ผู้ดูแลระบบ Google Workspace for Education Plus และ Standard สามารถใช้ศูนย์ความปลอดภัย ซึ่งจะให้ข้อมูลและการวิเคราะห์ด้านความปลอดภัยขั้นสูง รวมถึงยกระดับการเข้าถึงและการควบคุมปัญหาด้านความปลอดภัยที่ส่งผลต่อโดเมนของคุณ

ศูนย์ความปลอดภัยมีเครื่องมือตรวจสอบความปลอดภัย ซึ่งจะช่วยให้ผู้ดูแลระบบระบุ คัดแยก และดำเนินการกับปัญหาด้านความปลอดภัยและความเป็นส่วนตัว เช่น การโจมตีแบบฟิชชิง การแชร์ไฟล์อย่างไม่เหมาะสม ผู้ใช้และกิจกรรมในอุปกรณ์ที่น่าสงสัย และอื่นๆ อีกมากมาย

Google Workspace คือชุดโปรแกรมเพื่อการสื่อสารและการทำงานร่วมกันบนระบบคลาวด์ที่ปลอดภัยที่สุดในโลก

0

คือปริมาณช่องโหว่ในซอฟต์แวร์ของ Workspace ตั้งแต่พฤศจิกายน 2021*

50%

คือค่าใช้จ่ายที่ประหยัดได้เมื่อใช้ Workspace แทนการชำระเบี้ยประกันภัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ลดลง 2x

เหตุการณ์ด้านความปลอดภัยในองค์กรที่ใช้ Workspace ลดลง 2 เท่าเมื่อเทียบกับ Microsoft 365

ลดลง 2.5x

เหตุการณ์ด้านความปลอดภัยในองค์กรที่ใช้ Workspace ลดลง 2.5 เท่าเมื่อเทียบกับ Microsoft Exchange

เหตุการณ์ด้านความปลอดภัยในองค์กรที่ใช้ Workspace ลดลง 2.5 เท่าเมื่อเทียบกับ Microsoft Exchange

Google Chromebooks for Education

Chromebook เป็นคอมพิวเตอร์ที่มีความปลอดภัยและรองรับการปรับขนาดได้อย่างมาก นักเรียนและครูต่างก็ใช้งาน Chromebook ได้อย่างสะดวกสบายเพราะมาพร้อมฟีเจอร์ความปลอดภัยในตัวที่ทำงานได้ทันทีตั้งแต่แกะกล่อง ธุรกิจ โรงเรียน หรือผู้ใช้อุปกรณ์ ChromeOS ไม่เคยรายงานว่าพบการโจมตีด้วยแรนซัมแวร์เลย Chromebook ช่วยปกป้องโรงเรียนจากภัยคุกคามที่พัฒนาขึ้นเรื่อยๆ ด้วยฟีเจอร์ที่ทันสมัย และการอัปเดตฟีเจอร์ทำงานในเบื้องหลังโดยอัตโนมัติ ผู้ใช้จึงกลับมาทำงานได้ภายในไม่กี่วินาที

การอัปเดตระบบปฏิบัติการและแอปพลิเคชันแบบอัตโนมัติ พร้อมการป้องกันมัลแวร์ในตัว

ผู้โจมตีพยายามใช้ประโยชน์จากข้อบกพร่องและช่องโหว่ในระบบปฏิบัติการ เบราว์เซอร์ และแอปยอดนิยมอย่างไม่ลดละเพื่อติดตั้งมัลแวร์และขโมยข้อมูลผู้ใช้ Chromebook จึงปกป้องคุณและผู้ใช้ด้วยการอัปเดตระบบปฏิบัติการและแอปพลิเคชันให้ทันสมัยอยู่เสมอ เนื่องจากอุปกรณ์สร้างมาโดยคำนึงถึงความปลอดภัยตั้งแต่ต้นพร้อมการอัปเดตความปลอดภัย และแอปพลิเคชันระบบคลาวด์ก็ไม่จำเป็นต้องมีการอัปเดตซอฟต์แวร์เหมือนแอปในเครื่อง ชิปความปลอดภัยที่ออกแบบโดย Google ใน Chromebook จะช่วยให้อุปกรณ์ปลอดภัย ปกป้องตัวตนของผู้ใช้ และดูแลความสมบูรณ์ของระบบ

Chromebook ที่คุณมีจะเรียกใช้การอัปเดตการป้องกันมัลแวร์ล่าสุดโดยอัตโนมัติ ดังนั้น นักเรียนและนักการศึกษาจะได้รับการปกป้องจากภัยคุกคามทางไซเบอร์ด้วยฟีเจอร์ความปลอดภัยในตัว เช่น การเข้ารหัสข้อมูล การเปิดเครื่องที่ได้รับการยืนยัน แซนด์บ็อกซ์ และการอัปเดตอัตโนมัติ

Pรักษาความปลอดภัยของข้อมูลผู้ใช้

เมื่อลงชื่อเข้าใช้ Chromebook ด้วยบัญชี Google ข้อมูลทั้งหมดของคุณจะได้รับการจัดเก็บไว้ในไฟล์ที่เข้ารหัส เพื่อให้มั่นใจได้ว่าจะไม่มีใครสามารถใช้อุปกรณ์นี้ดูข้อมูลของคุณหรือลงชื่อเข้าใช้แอปพลิเคชันด้วยโดยใช้บัญชีของคุณ นักเรียนจึงสามารถใช้อุปกรณ์ร่วมกันได้ภายในห้องเรียน ด้านโรงเรียนก็สามารถลดต้นทุนรวมของการประมวลผลได้อย่างง่ายดายและปลอดภัย หรือหากต้องการฟีเจอร์ความปลอดภัยขั้นสูง เราก็มี Chrome Education Upgrade ซึ่งเป็นใบอนุญาตสำหรับโปรแกรมจัดการอุปกรณ์ที่พร้อมมอบการเข้าถึงที่เหนือกว่า

นโยบายความปลอดภัยสำหรับอุปกรณ์ที่สามารถจัดการผู้ใช้จากระยะไกลได้

ผู้ดูแลระบบของโรงเรียนสามารถกำหนดค่านโยบาย ChromeOS และติดตั้ง/อัปเดตแอปพลิเคชันจากระยะไกลได้โดยใช้คอนโซลผู้ดูแลระบบของ Google เพียงคลิกปุ่มเดียว ผู้ดูแลระบบไอทีหนึ่งคนก็จะสามารถอัปเดตนโยบายและการกำหนดค่าของ Chromebook หลายล้านเครื่องได้ในทันทีจึงมีประโยชน์เป็นอย่างมาก เช่น

ซึ่งมีประโยชน์ในการทำสิ่งต่อไปนี้

- กำหนดให้นักเรียนเข้าถึงได้เฉพาะเนื้อหาและแอปพลิเคชันที่โรงเรียนอนุมัติ
- ตั้งค่าให้แอปพลิเคชันและส่วนขยายทั้งหมดได้รับการอัปเดตพร้อมการแก้ไขด้านความปลอดภัยล่าสุด
- ป้องกันไม่ให้ผู้ใช้คัดลอก โอน หรือแชร์ข้อมูลของโรงเรียนไปอุปกรณ์อื่น
- ตัดสินใจโดยใช้ข้อมูลพร้อมคำแนะนำด้านความปลอดภัยที่ปรับแต่งขึ้นโดยเฉพาะจาก Google เพื่อจัดการกับภัยคุกคามด้านความปลอดภัย
- จัดการนโยบายความปลอดภัยและ Identity and Access Management สำหรับผู้ใช้ทุกคนได้จากส่วนกลางในคอนโซลผู้ดูแลระบบ

นโยบายอื่นๆ ทีสำคัญหากผู้ดูแลระบบต้องการกำหนดค่ามีดังนี้

นโยบายด้านอุปกรณ์

- **โหมดผู้มาเยือน**
  เราขอแนะนำให้คุณปิดใช้โหมดผู้มาเยือนของอุปกรณ์ เพื่อให้นักเรียนและครูต้องเข้าสู่ระบบโดยใช้ข้อมูลเข้าสู่ระบบของตนเองแทนการใช้อุปกรณ์แบบไม่ระบุตัวตน
- **ข้อจำกัดในการลงชื่อเข้าใช้**
  คุณอาจไม่ต้องการให้นักเรียนและครูลงชื่อเข้าใช้ Chromebook ของโรงเรียนด้วยบัญชี Gmail ส่วนตัว ดังนั้นให้บังคับใช้ข้อจำกัดการลงชื่อเข้าใช้โดยจำกัดเฉพาะโดเมน Workspace ของคุณในอุปกรณ์ที่นักเรียนใช้เท่านั้น
- **การรายงานผู้ใช้และอุปกรณ์**
  ผู้ดูแลระบบควรพิจารณาการเปิดการรายงานผู้ใช้และอุปกรณ์เพื่อให้รวบรวมเมตริกเกี่ยวกับความถี่ในการใช้งาน Chromebook, ผู้ที่ใช้งาน และสภาพของฮาร์ดแวร์ได้
- **การบังคับการลงทะเบียนซ้ำ**
  Chromebook ของโรงเรียนจะต้องอยู่ในโรงเรียนเท่านั้น เว้นแต่ผู้ดูแลระบบจะยกเลิกการจัดสรรดังกล่าว ผู้ดูแลระบบควรพิจารณาการใช้การบังคับการลงทะเบียน Chromebook ซ้ำ เพื่อให้ Chromebook ทำการลงทะเบียนซ้ำเสมอหากอุปกรณ์มีการล้างข้อมูลหรือมีการพยายามขโมยอุปกรณ์

นโยบายผู้ใช้

- **โหมดไม่ระบุตัวตน**
  Chromebook ของโรงเรียนควรมีการกำหนดค่าให้นักเรียนสามารถใช้ได้อย่างมีประสิทธิภาพ จึงควรจำกัดเบราว์เซอร์ที่ผ่านการตรวจสอบสิทธิเพื่อให้ตัวกรองเนื้อหาเว็บปกป้องนักเรียนจากเว็บไซต์ที่ไม่เหมาะสมได้ ผู้ดูแลระบบควรปิดใช้โหมดไม่ระบุตัวตนเพื่อป้องกันไม่ให้นักเรียนหลบเลี่ยงตัวกรองเว็บ
- **โหมดพร็อกซี**
  แม้ว่าบางโรงเรียนจะใช้พร็อกซีสำหรับการกรองเว็บ แต่คุณก็ควรป้องกันไม่ให้ผู้ใช้เปลี่ยนการตั้งค่าพร็อกซีเองได้
- **สิทธิการลงชื่อเข้าสู่ระบบพร้อมกันหลายบัญชี**
  หากผู้ใช้ได้รับอนุญาตให้เข้าสู่ระบบบัญชีรองขณะที่ใช้บัญชี Chromebook และบัญชี Workspace ของโรงเรียน ผู้ใช้ก็อาจขโมยข้อมูลที่มีความละเอียดอ่อนของนักเรียนหรือโรงเรียนไปยังบัญชีรองนั้นได้อย่างง่ายดาย ผู้ดูแลระบบจึงควรพิจารณาบล็อกการลงชื่อเข้าสู่ระบบพร้อมกันหลายบัญชี
- **ประวัติเบราว์เซอร์**
  การปิดไม่ให้นักเรียนล้างประวัติเบราว์เซอร์ของตนเองก็มีข้อดี เช่น หากเกิดเหตุการณ์ด้านความปลอดภัยทางอินเทอร์เน็ต บันทึกประวัติการใช้อินเทอร์เน็ตจะเป็นประโยชน์ในการตรวจสอบต่อไป

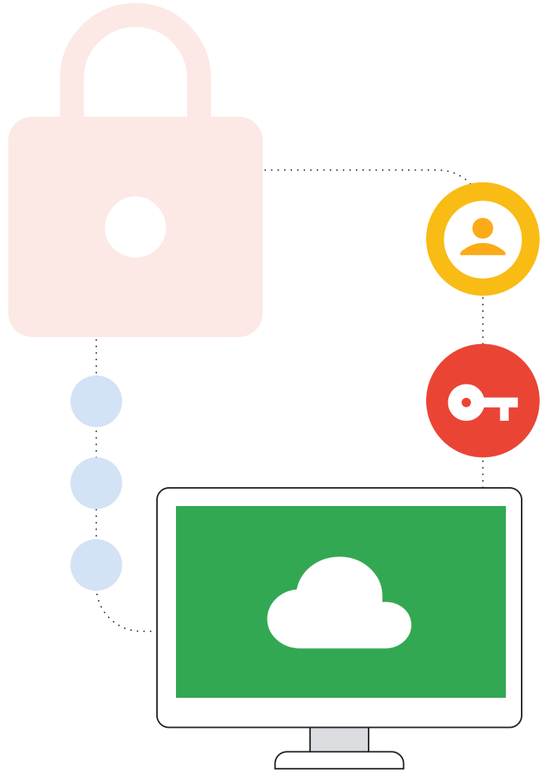
รายการนี้เป็นจุดเริ่มต้นที่ดีในการตรวจสอบว่าเครือข่ายของคุณปลอดภัยจากข้อผิดพลาดประเภทต่างๆ ที่พบบ่อยที่สุดซึ่งอาจนำไปสู่เหตุการณ์ทางไซเบอร์ที่สำคัญหรือไม่ ดูนโยบายความปลอดภัยที่แนะนำอื่นๆ ได้ใน[เช็กลิสต์สำหรับการรักษาความปลอดภัย]ของเรา

การจัดการปลายทางเพื่อการใช้งานที่ปลอดภัยทุกที่ทุกเวลา

ระบบตัวจัดการนโยบายระยะไกลของ ChromeOS ช่วยให้ผู้ดูแลระบบของโรงเรียนใช้การตั้งค่าความปลอดภัยและเรียกใช้เครื่องมือรักษาความปลอดภัยบนอุปกรณ์ เช่น ระบบกรองเนื้อหา แทนการใช้บนเซิร์ฟเวอร์เครือข่ายของโรงเรียน ซึ่งจะทำให้นักเรียนได้รับประโยชน์ด้านความปลอดภัยบน Chromebook ของโรงเรียนเมื่ออยู่ที่บ้าน เช่นเดียวกับเมื่ออยู่ในห้องเรียน ความปลอดภัยนั้นเป็นเรื่องที่สำคัญมากขึ้นเรื่อยๆ เพราะโรงเรียนต่างหันมาใช้หนังสือเรียนดิจิทัลและเครื่องมือการเรียนรู้ออนไลน์ รวมถึงจำเป็นต้องให้นักเรียนนำคอมพิวเตอร์กลับบ้านเพื่อทำการบ้านอีกด้วย

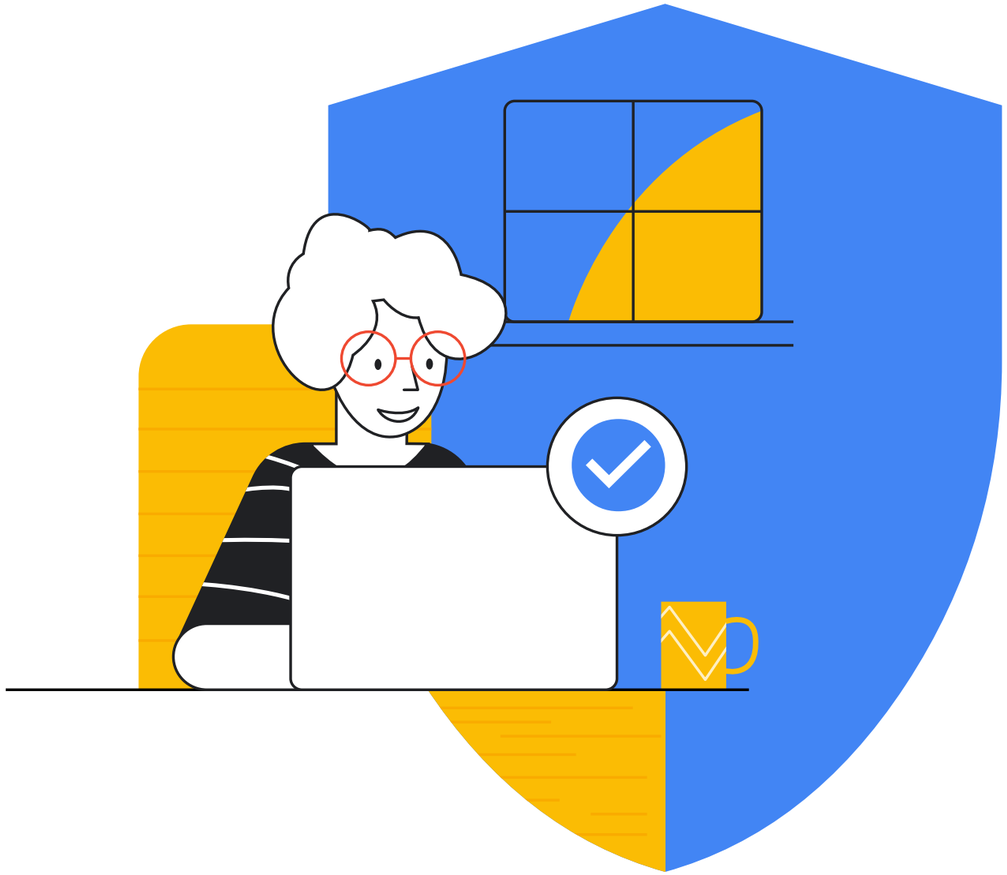
บทสรุป

ความท้าทายในการรักษาความปลอดภัยให้กับสถาบันการศึกษาระดับ K-12 จากการโจมตีทางไซเบอร์นับวันยิ่งซับซ้อน การลงทุนด้านการรักษาความมั่นคงปลอดภัยออนไลน์เพื่อปกป้องตัวคุณเอง นักเรียน ครู เจ้าหน้าที่ และระบบนิเวศออนไลน์ในวงกว้างจึงเป็นเรื่องคำแนะนำไปปรับใช้ให้ตรงกับตามความต้องการของตนเองโดยเฉพาะ รวมถึงก้าวให้ทันภัยคุกคามและเทคโนโลยีใหม่ๆ ที่เปลี่ยนแปลงอยู่เสมอ สถาบันการศึกษาระดับ K-12 จึงควรมีแหล่งข้อมูลที่เป็นประโยชน์เพื่อเป็นรากฐานที่มั่นคงของโปรแกรมรักษาความปลอดภัย เอกสารนี้ได้รวบรวมแหล่งข้อมูลสำหรับขั้นตอนต่อไปและการดำเนินการที่สามารถนำไปปฏิบัติได้จริง นอกจากนี้ Google ยังมีแหล่งข้อมูล การฝึกอบรม และผู้เชี่ยวชาญที่มีทักษะสูงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งพร้อมให้ความช่วยเหลือแก่โรงเรียนและองค์กรต่างๆ ตามคู่มือนี้ และยังมีหัวข้อที่เกี่ยวกับเทคโนโลยีใหม่ๆ เช่น AI เป็นต้น ผลิตภัณฑ์ของ Google ได้รับการปรับแต่งเพื่อการศึกษาและมอบโซลูชันสำเร็จรูปที่จะช่วยป้องกันอันตรายต่างๆ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งระบุไว้ในเอกสารแล้ว เรายินดีเป็นอย่างยิ่งที่จะได้ร่วมงานกับคุณเพื่อให้คุณสามารถออกแบบและใช้งานโปรแกรมการรักษาความปลอดภัยของสถาบันได้อย่างราบรื่น



รายการแหล่งข้อมูล

- Google "เคล็ดลับการออนไลน์อย่างปลอดภัย" (Tips to Stay Safe & Secure Online)" ศูนย์ความปลอดภัยของ Google, https://safety.google/security/security-tips/ เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- NIST "เฟรมเวิร์กสำหรับการปรับปรุงโครงสร้างพื้นฐานของการรักษาความมั่นคงปลอดภัยไซเบอร์ เวอร์ชัน 1.1" (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1)" NIST Technical Series Publications, 16 เมษายน 2018, https://doi.org/10.6028/NIST.CSWP.04162018 เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- Microsoft "โปรแกรม Microsoft AccountGuard" โปรแกรม Microsoft AccountGuard, https://www.microsoftaccountguard.com/en-us/ เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- Google "โปรแกรมการปกป้องขั้นสูง" โปรแกรมการปกป้องขั้นสูง ของ Google, https://landing.google.com/advancedprotection เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- Google "ศูนย์ความปลอดภัยของ Google" ศูนย์ความปลอดภัยของ Google - ท่องโลกออนไลน์ได้อย่างปลอดภัยยิ่งขึ้น, https://safety.google เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- Meta "ความรู้พื้นฐาน: ช่วยให้บัญชีปลอดภัย' (Basics: Help Secure Your Account)" ช่วยให้บัญชีปลอดภัย, https://www.facebook.com/gpa/resources/basics/security เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- Meta “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- NIST “SP 800-124 Rev. 1: แนวทางการจัดการการรักษาความปลอดภัยของอุปกรณ์เคลื่อนที่ในภาคธุรกิจ” (SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise) NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1 เข้าถึงเมื่อวันที่ 6 ตุลาคม 2022
- พาสคีย์: https://developers.google.com/identity/passkeys
- รายงานปกป้องอนาคตของเรา (Protecting Our Future) เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันการศึกษาระดับ K-12 โดย CISA https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- รายงานของ GAO https://www.gao.gov/products/gao-20-644
- สามารถ ดูข้อมูลเพิ่มเติมว่า Google for Education สามารถช่วยปกป้องสถาบันการศึกษาของคุณได้อย่างไรบ้างที่ ศูนย์ความเป็นส่วนตัวและความปลอดภัยของ Google for Education
- รายงานฟิชชิงของ Zcaler



Google for Education