

รหัสผ่าน

ผู้เข้าร่วมจะได้เรียนรู้วิธีการรักษาข้อมูลออนไลน์อย่างปลอดภัยมากขึ้นโดยใช้รหัสผ่านที่คาดเดายากอยู่เสมอ ผู้เข้าร่วมจะได้เรียนรู้เกี่ยวกับหลักการออกแบบรหัสผ่านที่คาดเดายากและปัญหาในการแชร์รหัสผ่านที่อาจเกิดขึ้นได้ นอกจากนี้ ผู้เข้าร่วมจะได้เรียนรู้วิธีการเข้ารหัสผ่านให้ปลอดภัยและวิธีป้องกันการเข้าถึงบัญชีผู้ใช้ของตนโดยไม่ได้รับอนุญาต

เนื้อหา

ใบงานสำหรับการเรียนรู้เกี่ยวกับรหัสผ่าน

หลักพื้นฐานของรหัสผ่าน

ส่วนที่ 1

บอกนักเรียนของคุณ

เรามักจะไม่คำนึงถึงรหัสผ่านที่เราใช้สำหรับเว็บไซต์ แอป หรือบริการต่างๆ มากนัก แต่รหัสผ่านที่ดีช่วยให้ข้อมูลของคุณปลอดภัยมากขึ้น

ปฏิสัมพันธ์ในชั้นเรียน

ให้ผู้เข้าร่วมการอภิปรายกันโดยใช้คำถามด้านล่างต่อไปนี้
โปรดอย่ากับผู้เข้าร่วมว่าไม่ควรแชร์รหัสผ่านจริงๆ
ของตนระหว่างการทำกิจกรรมนี้หรือกิจกรรมอื่นๆ

ถามนักเรียนของคุณ

คุณมีรหัสผ่านทั้งหมดกี่รหัส

คุณมีรหัสผ่านที่แตกต่างกันสำหรับอีเมลและบัญชีผู้ใช้โซเชียลมีเดียต่างๆ ของคุณหรือไม่

รหัสผ่านแต่ละอันต่างกันมากหรือไม่ หรือแค่เปลี่ยนแปลงเล็กๆ น้อยๆ จากรหัสผ่านหลัก

หากคุณมีมากกว่าหนึ่งรหัสผ่าน คุณจำได้อย่างไรว่ารหัสผ่านใดใช้กับบัญชีผู้ใช้ไหน

ถามนักเรียนของคุณ

คุณลืมรหัสผ่านสำคัญบ่อยแค่ไหน

คุณทำอะไรหากคุณลืมรหัสผ่าน

คุณตั้งรหัสผ่านให้จำได้ง่ายอย่างไร

มีรหัสผ่านที่คุณใช้ทุกวันหรือไม่

จะเกิดอะไรขึ้นหากใครบางคนรู้รหัสผ่านของคุณโดยที่คุณไม่ทราบ

ขึ้นอยู่กับว่าเป็นใครหรือไม่

ข้อมูลประเภทใดที่คนอื่นอาจเรียนรู้เกี่ยวกับตัวคุณได้หากบุคคลนั้นใช้รหัสผ่านของคุณในการเข้าถึงบัญชีผู้ใช้ของคุณ

ส่วนที่ 2

ปฏิสัมพันธ์ในชั้นเรียน

ให้ผู้เข้าร่วมจับคู่กัน

บอกนักเรียนของคุณ

ปรึกษากับคู่ของคุณว่าจะเกิดอะไรขึ้นถ้ามีคนที่ไม่ประสงค์ดีรู้รหัสผ่านโซเชียลมีเดียโปรดของคุณ

ปฏิสัมพันธ์ในชั้นเรียน

ใช้เวลาผู้เข้าร่วม 5 นาทีในการปรึกษาหารือกัน และให้แต่ละกลุ่มเสนอและอธิบายให้กลุ่มอื่นๆ ฟัง

บอกนักเรียนของคุณ

ตอนนี้ให้คุยกับคู่ของคุณว่าจะเกิดอะไรขึ้นถ้าแฮกเกอร์รู้รหัสผ่านบัญชีธนาคารออนไลน์ของพ่อแม่หรือผู้ปกครองของคุณ

ปฏิสัมพันธ์ในชั้นเรียน

ใช้เวลาผู้เข้าร่วม 5 นาทีในการปรึกษาหารือกัน จากนั้น ให้แต่ละกลุ่มแสดงความเห็นของตน

ส่วนที่ 3

บอกนักเรียนของคุณ

คุณอาจสงสัยว่าแฮกเกอร์รู้รหัสผ่านส่วนตัวของคนอื่นๆ ได้อย่างไร มีวิธีการอยู่ 2-3 วิธี วิธีหนึ่งคือการใช้เทคนิคแบบวิศวกรรมสังคม หรือการหลอกสอให้บางคนบอกรหัสผ่านนั่นเอง แฮกเกอร์สามารถทำได้โดยส่งอีเมลที่ดูเหมือนว่าส่งมาจากแพลตฟอร์มหรือเว็บไซต์อย่างถูกต้องตามกฎหมายซึ่งบุคคลนั้นมีบัญชีผู้ใช้อยู่ อีเมลอาจขอให้บุคคลนั้นคลิกที่ลิงก์และเข้าสู่ระบบโดยใช้ชื่อผู้ใช้และรหัสผ่านของตน หากบุคคลนั้นเข้าสู่ระบบ ข้อมูลจะส่งไปหาแฮกเกอร์

บางครั้ง แฮกเกอร์อาจพยายามเดารหัสผ่านโดยใช้คำง่ายๆ เช่น “password123”, “test” หรือชื่อนามสกุลของคุณ

อีกวิธีหนึ่งที่แฮกเกอร์ใช้เพื่อรู้รหัสผ่านคือ ผ่านสิ่งที่เรียกว่า “Brute Force Attack” (การสุ่มรหัสผ่าน) Brute Force Attack จะเกิดขึ้นเมื่อแฮกเกอร์พยายามเข้าสู่ระบบบัญชีผู้ใช้ของคุณโดยพยายามใช้รหัสผ่านแบบต่างๆ ซ้ำไปมา แม้ว่าแฮกเกอร์สามารถทำ “Brute Force Attack” ได้เอง แต่แฮกเกอร์มักใช้โปรแกรมคอมพิวเตอร์ที่ดำเนินการซ้ำๆ อัตโนมัติเพื่อหารหัสผ่านที่อาจเป็นไปได้ ตัวอย่างเช่น รายการรหัสผ่านที่อาจเป็นไปได้หรือชุดรหัสผ่านที่มีตัวเลขและตัวอักษรต่างๆ จนกว่าโปรแกรมจะพบรหัสผ่านที่ถูกต้อง

แน่นอนว่า “Brute Force Attack” บางวิธีค่อนข้างซับซ้อนมากกว่า

หากรหัสผ่านของคุณอยู่บนรายการรหัสผ่านที่อาจเป็นไปได้ เช่น “fido123” หรือ “password” บางโปรแกรมอาจเดาได้เร็วขึ้นได้โดยลองรหัสผ่านดังกล่าวก่อนลองใช้รหัสผ่านที่เป็นไปได้น้อยกว่าหรือก่อนลบรหัสผ่าน นอกจากนั้น แอ็กเกอร์ยังสามารถปรับแต่งการจำใจนี้ได้ หากแอ็กเกอร์ทราบข้อมูลเกี่ยวกับคุณ ตัวอย่างเช่น หากแอ็กเกอร์รู้ชื่อสัตว์เลี้ยงของคุณที่ชื่อ “Toby” แอ็กเกอร์อาจลองใช้ “Toby” พร้อมกับตัวเลขต่างๆ ต่อท้าย (เช่น ‘Toby629’ หรือ ‘Toby3020’)

หลักการในการออกแบบ

ส่วนที่ 1

ถามนักเรียนของคุณ

ใครที่ทราบบ้างว่าการมีรหัสผ่านที่ “เดาได้ยาก” หรือ “เดายากขึ้น” หมายความว่าอย่างไร เหตุใดจึงเป็นความคิดที่ดี

บอกนักเรียนของคุณ

รหัสผ่านที่เดาได้ยากช่วยปกป้องข้อมูลของคุณได้ ถึงแม้การมีรหัสผ่านที่เดายากจะไม่ได้รับประกันว่าบัญชีผู้ใช้ของคุณจะไม่ถูกแฮ็ก แต่การมีรหัสผ่านที่เดาง่ายจะทำให้ใครบางคนเข้าถึงข้อมูลของคุณได้ง่ายยิ่งขึ้น

แบบฝึกหัดเรื่องรหัสผ่าน

ถามนักเรียนของคุณ

ตัวอย่างของรหัสผ่านที่เดาง่ายมีอะไรบ้าง

1. ตัวอย่างเช่น Password, 12345, Hello!, วันเกิด, ชื่อเล่น

เหตุใดคุณจึงคิดว่ารหัสผ่านเหล่านี้เดาได้ง่าย

1. ผู้อื่นและ/หรือคอมพิวเตอร์สามารถเดารหัสผ่านเหล่านี้ได้อย่างง่ายดายโดยใช้ “Brute Force Attack”

คุณสามารถเปลี่ยนให้รหัสผ่านเดาได้ยากขึ้นด้วยวิธีใดบ้าง

1. การเพิ่มตัวเลข ตัวพิมพ์เล็กและพิมพ์ใหญ่ สัญลักษณ์, การสร้างรหัสผ่านให้ยาว และการหลีกเลี่ยงวลีหรือคำทั่วไป

ปฏิสัมพันธ์ในชั้นเรียน

หลังจากผู้เข้าร่วมได้แสดงความคิดเห็นแล้ว ให้เขียนคำแนะนำเหล่านี้ลงบนกระดาน:

ให้มีตัวเลขอย่างน้อยหนึ่งตัว

ให้มีสัญลักษณ์อย่างน้อยหนึ่งตัว

ให้มีตัวพิมพ์เล็กและตัวพิมพ์ใหญ่อย่างน้อยอย่างละหนึ่งตัว

รหัสผ่านควรวาวอย่างน้อย 7 ตัวอักษร

รหัสผ่านควรจดจำได้ง่าย (เว้นแต่จะใช้ตัวจัดการรหัสผ่าน)

ตัวจัดการรหัสผ่านคือ

เว็บไซต์/แอปที่ช่วยให้ผู้ใช้สามารถบันทึกและจัดการรหัสผ่านของตนได้

รหัสผ่านไม่ควรเป็นคำทั่วไปหรือข้อมูลส่วนตัว (เช่น วันเกิด ชื่อผู้ปกครอง เป็นต้น)

ไม่ควรใช้รหัสผ่านเดียวกันบนเว็บไซต์อื่นๆ

บอกนักเรียนของคุณ

มีวิธีการสร้างรหัสผ่านที่เดาได้ยากอยู่สองวิธีด้วยกัน วิธีแรกคือ การปฏิบัติตาม “วิธีการสร้างรหัสผ่าน” ที่เขียนไว้บนกระดาน การใช้วิธีการดังกล่าวช่วยให้คุณใส่องค์ประกอบที่เดาได้ยากลงในรหัสผ่านแบบข้อความ/ตัวเลข ซึ่งทำให้รหัสผ่านเดาได้ยากยิ่งขึ้น แต่ข้อเสียของวิธีนี้คือทำให้รหัสผ่านจดจำได้ยาก

รหัสผ่านที่คาดเดายาก

บอกนักเรียนของคุณ

อีกหนึ่งวิธีการสร้างรหัสผ่านที่คาดเดายาก คือการใช้รหัสผ่านยาวๆ

ยิ่งรหัสผ่านยาวก็ยิ่งเดาได้ยาก

การสร้างรหัสผ่านโดยใช้คำที่ไม่มีความเกี่ยวข้องกันสี่คำขึ้นไปจะทำให้ผู้อื่น รวมถึง Brute Force Attack เดารหัสผ่านได้ยากขึ้น

วิธีนี้มีข้อดีคือช่วยให้คุณสร้างรหัสผ่านที่จดจำง่ายกว่าวิธีการสร้างรหัสผ่านตามสูตร

วิธีสุดท้าย คือ การนำทั้งสองวิธีที่พูดไปข้างต้นมาใช้ด้วยกัน

โดยใช้คำที่ไม่มีความเกี่ยวข้องกันสี่คำขึ้นไปและใช้สัญลักษณ์และตัวเลขรวมเข้าไปด้วย

จุดมุ่งหมายของวิธีการที่ต่างกันนี้นั้นเหมือนกันคือ

การพัฒนาให้รหัสผ่านไม่ซ้ำกันและทำให้ผู้อื่นเดารหัสผ่านได้ยาก

บอกนักเรียนของคุณ

ให้ผู้เข้าร่วมจับคู่กัน

ให้แต่ละคู่สร้างรหัสผ่านที่คาดเดายากโดยใช้คำแนะนำที่เขียนไว้บนกระดานก่อนหน้านี้

อย่าลืมว่า รหัสผ่านที่คอมพิวเตอร์สามารถเดาสุ่มได้ยาก

อาจเป็นรหัสผ่านที่คนหรือคอมพิวเตอร์ซึ่งมีลิสต์รหัสผ่านยาวที่พบบ่อยสามารถเดาได้

จะไม่มีภารกิจกระดาศที่มีรหัสผ่านของคุณเมื่อจบกิจกรรมนี้ คุณไม่ควรนำรหัสผ่านนี้ไปใช้จริง เนื่องจากคนอื่นๆ ในกลุ่มรู้รหัสผ่านดังกล่าว

ใช้เวลาผู้เข้าร่วม 5 นาทีในการทำกิจกรรมนี้ จากนั้นให้เดินไปรอบๆ

ห้องและถามผู้เข้าร่วมว่ารหัสผ่านที่เดาได้ยากที่สุดที่พวกเขาคิดขึ้นคืออะไร

ถามผู้เข้าร่วมว่าพวกเขาจำรหัสผ่านที่สร้างขึ้นโดยไม่ต้องดูรหัสผ่านโดยตรงได้หรือไม่

บางเว็บไซต์อาจมีเงื่อนไขในการสร้างรหัสผ่าน แต่บางเว็บไซต์ก็ไม่มีข้อกำหนดดังกล่าว
นอกจากนั้น คุณสามารถสร้างรหัสผ่านได้โดยใช้คำสุ่มทั่วไป

ปฏิสัมพันธ์ในชั้นเรียน

ในคู่เดิม ให้ผู้เข้าร่วมสร้างรหัสผ่านใหม่ซึ่งประกอบด้วยคำหลายๆ คำ
บอกพวกเขาว่ารหัสผ่านควรจะประกอบด้วยอย่างน้อย 4 คำเพื่อให้ทั้งคาดเดายากและจำง่าย
ใช้เวลาผู้เข้าร่วม 5 นาทีในการทำกิจกรรมนี้
จากนั้นให้เดินไปรอบห้องและถามผู้เข้าร่วมว่าคิดตัวอย่างรหัสผ่านอะไรได้บ้าง
แล้วย้ำกับผู้เข้าร่วมอีกรอบว่าจะไม่มีการเก็บกระดาษแผ่นนี้หลังจบกิจกรรม
และไม่ควรนำรหัสผ่านนี้ไปใช้จริงกับบัญชีผู้ใช้ใดๆ ของตนเอง

บอกนักเรียนของคุณ

บางเว็บไซต์จะใช้ระบบที่เรียกว่าการยืนยันตัวตนแบบหลายชั้น (หรือแบบสองชั้น)
ในการยืนยันตัวตนของคุณ เว็บไซต์เหล่านี้มักส่งรหัสแบบใช้ครั้งเดียวผ่านทาง SMS, แอป
หรืออีเมล และต้องนำไปกรอกพร้อมกับรหัสผ่าน

วิธีนี้ทำให้บัญชีผู้ใช้ของคุณปลอดภัยมากยิ่งขึ้น
โดยเพิ่มระดับการรักษาความปลอดภัยพิเศษที่เจาะได้ยากขึ้น ตัวอย่างเช่น
บุคคลหนึ่งต้องมีรหัสผ่านและสิทธิ์เข้าถึงแอป อุปกรณ์ หรืออีเมลที่เชื่อมโยงกับบัญชีผู้ใช้
เพื่อเข้าสู่ระบบบัญชีผู้ใช้ของคุณ

การรักษาห้สผ่านให้ปลอดภัย

ส่วนที่หนึ่ง

บอกนักเรียนของคุณ

ถึงคุณจะทำห้สผ่านที่ทั้งคนและคอมพิวเตอร์เดาได้ยาก แต่ยังมีวิธีอื่นๆที่สามารถเจาะห้สผ่านได้

ถามนักเรียนของคุณ

วิธีอื่นๆ ที่สามารถเจาะห้สผ่านได้มีอะไรบ้าง

1. ตัวอย่างเช่น การนำห้สผ่านไปใช้กับบัญชีผู้ใช้หลายบัญชี การใช้ห้สผ่านที่มีข้อมูลส่วนตัว การใช้ห้สผ่านเดิมเป็นเวลหลายปี การลืมห้สผ่าน

คุณคิดว่าควรเปลี่ยนห้สผ่านบ่อยแค่ไหน

บอกนักเรียนของคุณ

แม้ห้สผ่านที่เดาได้ยากก็อาจตกอยู่ในอันตรายหรือถูกขโมยได้ แต่มีหลายสิ่งที่คุณสามารถทำได้เพื่อป้องกันตัวเอง หากเว็บไซต์ที่คุณมีบัญชีผู้ใช้มีการละเมิดข้อมูลหรือข้อมูลรั่วไหล ให้เปลี่ยนห้สผ่านของคุณบนเว็บไซต์ดังกล่าว รวมถึงเว็บไซต์อื่นๆ ที่คุณใช้ห้สผ่านคล้ายๆกัน

การจดจำห้สผ่านที่ยาวและซับซ้อนอาจเป็นเรื่องยาก

ถามนักเรียนของคุณ

คุณคิดว่าเป็นความคิดที่ดีหรือไม่ในการจดห้สผ่านของคุณลงบนกระดาษหรือไฟล์เอกสารบนคอมพิวเตอร์ เพราะเหตุใดจึงเป็นหรือไม่เป็นเช่นนั้น

ปฏิสัมพันธ์ในชั้นเรียน

กล่าวถึงความเป็นไปได้ที่ใครบางคนอาจพบกระดาษแผ่นนั้นหรือเจอไฟล์นั้นบนคอมพิวเตอร์ อธิบายถึงตัวจัดการห้สผ่าน ซึ่งเป็นแอปพลิเคชันที่ช่วยให้ผู้ใช้สามารถบันทึกและจัดการห้สผ่านของตนเองได้

ส่วนที่สอง

บอกนักเรียนของคุณ

ในแต่ละวัน เราใช้งานบัญชีผู้ใช้หลายรายการบนเว็บไซต์ต่างๆ มากมาย ซึ่งอาจเป็นเรื่องที่ยากในการเข้าสู่ระบบและออกจากระบบทุกครั้งที่เราออกเว็บไซต์

ถามนักเรียนของคุณ

คุณเคยใช้คุณสมบัติ “บันทึกรหัสผ่าน” ในเบราว์เซอร์ในการบันทึกรหัสผ่านบนเว็บไซต์หรือไม่ เพราะเหตุใดจึงเป็นหรือไม่เป็นเช่นนั้น

คุณเข้าใจวิธีที่เว็บไซต์ใช้เพื่อจดจำคุณหรือไม่

1. ให้นักเรียนลองอธิบาย จากนั้นให้อธิบายว่า
เว็บไซต์สามารถจดจำได้ว่าคุณเข้าสู่ระบบโดยบันทึกคุกกี้ไว้
คุกกี้คือไฟล์ขนาดเล็กที่เก็บอยู่ในคอมพิวเตอร์ของคุณ เพื่อช่วยให้เว็บไซต์จำคุณและคอมพิวเตอร์ของคุณได้เมื่อคุณเข้าเยี่ยมชมเว็บไซต์ในครั้งต่อไป
คุณจึงไม่ต้องเข้าสู่ระบบใหม่อีกครั้ง อย่างไรก็ตาม
คุกกี้สามารถนำไปใช้ในการติดตามคุณได้ว่าคุณเข้าดูเว็บไซต์ใดบ้าง
นั่นคือวิธีที่โฆษณาใช้กำหนดเป้าหมายไปที่คุณ

จะเป็นไรหรือไม่ถ้าคุณบันทึกรหัสผ่านไว้บนคอมพิวเตอร์ของคุณเอง

ถามนักเรียนของคุณ

คอมพิวเตอร์ของคุณมีรหัสผ่านเพื่อเข้าใช้งานหรือไม่

จะเป็นอย่างไรถ้าคุณใช้คอมพิวเตอร์ร่วมกับผู้อื่น

1. ในกรณีนี้
ถึงแม้รหัสผ่านของคุณอาจจะปรากฏในช่องกรอกรหัสเป็นจุดสีดำหรือเครื่องหมายดอกจัน
แต่คนอื่นที่ใช้คอมพิวเตอร์ของคุณก็อาจหายได้ว่ารหัสผ่านของคุณคืออะไร การที่คุณไม่อาจมองเห็นรหัสผ่านบนหน้าจอไม่ได้หมายความว่าไม่มีการจัดเก็บรหัสผ่านไว้ที่ใด

ถามนักเรียนของคุณ

มีกรณีใดหรือไม่ที่การแชร์รหัสผ่านกับคนอื่นเป็นเรื่องที่ไม่เป็นไร เมื่อใด เหตุใดคุณจึงไม่แชร์

1. ตัวอย่างเช่น ผู้ปกครองของคุณอาจต้องการรหัสผ่าน
หรือพวกเขามีบัญชีผู้ใช้ร่วมสำหรับครอบครัวในบริการอย่างเช่น Netflix

คุณแชร์รหัสผ่านของคุณกับบุคคลอื่นหรือไม่ หากคุณแชร์ คุณแชร์ให้ผู้ใด/เพราะเหตุใด

ถ้าคุณมีเพื่อนสนิทอยู่คนหนึ่ง เพื่อนคนนั้นจะขอให้คุณแชร์รหัสผ่านของคุณโดยบอกว่า
“ถ้าแคร่ฉันก็ต้องแชร์รหัสผ่านให้ฉันรู้” โหม เพราะเหตุใดจึงเป็นหรือไม่เป็นเช่นนั้น

บอกนักเรียนของคุณ

คุณสามารถเลือกแชร์รหัสผ่านของคุณกับคนที่คุณแครงได้
แต่การแครงใครสักคนไม่จำเป็นต้องให้เขาได้รับสิทธิ์เข้าถึงบัญชีผู้ใช้ออนไลน์ของคุณ

พิจารณาความสัมพันธ์ของคุณกับบุคคลหนึ่งอย่างรอบคอบก่อนแชร์รหัสผ่าน และอย่าลืมคิดถึงความเป็นไปได้ที่ความสัมพันธ์ดังกล่าวอาจเปลี่ยนแปลงเมื่อเวลาผ่านไป ตัวอย่างเช่น การแชร์กับพ่อแม่ผู้ปกครองต่างจากการแชร์กับเพื่อนสนิทของคุณมาก

ถามนักเรียนของคุณ

หากคุณแชร์รหัสผ่าน จะเกิดอะไรขึ้นกับคุณบ้าง

1. ใครบางคนอาจแฮ็กเข้าบัญชีธนาคารของคุณ แฝงตัวเป็นคุณในโลกออนไลน์ หรือค้นหาความลับของคุณ

หากคุณแชร์รหัสผ่านสำหรับบัญชีผู้ใช้หนึ่ง คุณจะใช้บัญชีผู้ใช้อย่างกล่าวต่างออกไปหรือไม่

ถามนักเรียนของคุณ

มีรายการไหนที่คุณจะไม่ดูบน Netflix หรือมีอะไรที่คุณจะไม่เขียนลงในอีเมลหรือไม่ ถ้ามีคนอื่นที่สามารถเห็นได้ว่าคุณกำลังทำอะไรอยู่

ปฏิสัมพันธ์ในชั้นเรียน

ผู้เข้าร่วมควรไตร่ตรองถึงพฤติกรรมของตนเองเมื่อต้องใช้งานบัญชีผู้ใช้อยู่ร่วมกับคนอื่น ผู้เข้าร่วมควรระลึกไว้ว่าผู้อื่นๆ ที่ใช้บัญชีดังกล่าวร่วมกันสามารถเห็นกิจกรรมที่พวกเขาทำทางออนไลน์ได้

ถามนักเรียนของคุณ

หากบัญชีผู้ใช้ของคุณเป็นสิ่งที่แสดงความเป็นคุณ เช่น โพรไฟล์โซเชียลมีเดีย การให้ผู้อื่นใช้งานบัญชีผู้ใช้ของคุณเป็นเรื่องที่ยอมรับได้หรือไม่

ปฏิสัมพันธ์ในชั้นเรียน

หาหรือถึงความเป็นไปได้ที่ใครบางคนอาจแฝงตัวเป็นคุณและส่งข้อความไปยังเพื่อนๆ ของคุณ

ถามนักเรียนของคุณ

คุณให้อุปกรณ์ต่างๆ ที่คุณใช้บันทึกรหัสผ่านของคุณหรือไม่ เพราะเหตุใดจึงเป็นหรือไม่เป็นเช่นนั้น เป็นเรื่องที่ปลอดภัยหรือไม่ในการบันทึกรหัสผ่านของคุณไว้ในโทรศัพท์หรือคอมพิวเตอร์ส่วนตัว จะเกิดอะไรขึ้นหากคุณให้เพื่อนยืมโทรศัพท์หรือคอมพิวเตอร์ของคุณ

คุณแชร์อุปกรณ์ของคุณกับผู้อื่น เช่น ครอบครัวยุหรือเพื่อน หรือไม่ คุณแชร์บัญชีผู้ใช้บนอุปกรณ์ดังกล่าวหรือไม่ หรือแต่ละคนมีบัญชีผู้ใช้ของตนเอง

คุณเคยใช้อุปกรณ์ “สาธารณะ” เช่น อุปกรณ์ในห้องสมุด ที่โรงเรียน หรือที่อื่นใดหรือไม่ คุณใช้งานอุปกรณ์ดังกล่าวแบบเดียวกับที่คุณอาจใช้ที่อื่นหรือไม่

ส่วนที่สาม

ปฏิสัมพันธ์ในชั้นเรียน

ให้ผู้เข้าร่วมจับคู่กัน

บอกนักเรียนของคุณ

ในคู่ของคุณ ให้คุยกันว่าเคยเข้าสู่ระบบคอมพิวเตอร์ที่โรงเรียน ที่ห้องสมุด หรือที่ศูนย์คอมพิวเตอร์อื่นๆ และเห็นว่ายังมีคนเข้าสู่ระบบโซเชียลมีเดียหรืออีเมลค้างไว้หรือไม่ ให้ผู้เข้าร่วมลองคิดว่าพวกเขาจะสำรวจบัญชีผู้ใช้นั้นหรือทำอย่างอื่นไหม

ปฏิสัมพันธ์ในชั้นเรียน

ใช้เวลาผู้เข้าร่วม 5 นาทีในการปรึกษาหารือกัน จากนั้นให้ผู้เข้าร่วมแชร์ความเห็น กระตุ้นให้แต่ละกลุ่มอภิปรายเกี่ยวกับการใช้งานที่ไม่ได้รับอนุญาตดังกล่าว

การเข้าถึงบัญชีผู้ใช้ที่ไม่ได้รับอนุญาต

ส่วนที่หนึ่ง

ปฏิสัมพันธ์ในชั้นเรียน

โปรดทราบว่า: ส่วนหนึ่งของเนื้อหาในกิจกรรมนี้ครอบคลุมอยู่แล้วใน “กิจกรรมที่ 1: หลักพื้นฐานของรหัสผ่าน”
คุณสามารถตัดสินใจได้ว่าจะเรียนรู้เนื้อหานี้อีกครั้งหรือข้ามเนื้อหาต่อไป

บอกนักเรียนของคุณ

ผู้อื่นสามารถเข้าถึงบัญชีผู้ใช้ของคุณได้
ถึงแม้จะไม่รู้รหัสผ่านหรือไม่สามารถเดารหัสผ่านของคุณได้ก็ตาม
หากใครบางคนรู้ข้อมูลส่วนตัวของคุณมากเกินไป บุคคลนั้นอาจสามารถคาดเดารหัสผ่านของคุณได้หรืออาจโน้มน้าวให้ใครบางคนที่เป็นที่เชื่อถือส่งข้อมูลของคุณให้
การโจมตีแบบนี้เรียกว่าการแฮ็กทางสังคมหรือวิศวกรรมทางสังคม
เนื่องจากพวกเขาไม่ได้ใช้เทคโนโลยีในการเจาะเข้าบัญชีผู้ใช้ของคุณ

ถามนักเรียนของคุณ

ให้ยกมือขึ้นหากเคยลืมรหัสผ่านของเว็บไซต์

จะเกิดอะไรขึ้นหากคุณคลิกที่ “ฉันลืมรหัสผ่านของฉัน”

1. โดยปกติ เว็บไซต์จะถามคำถามรักษาความปลอดภัยหรือพยายามที่จะติดต่อคุณโดยใช้หมายเลขโทรศัพท์มือถือหรืออีเมล

คำถามรักษาความปลอดภัยแบบใดที่เว็บไซต์ใช้ถามคุณ

1. อธิบายว่าคำถามเหล่านี้เป็นคำถามที่เพื่อนหรือคนรู้จักอาจตอบหรือเดาได้อย่างไร
ลองคำนึงถึง: ชื่อสัตว์เลี้ยง บ้านเกิด นามสกุลเดิมของแม่ ชื่อครูคนโปรด ชื่อเพื่อนสนิท ทีมโปรด

มีใครอีกบ้างที่อาจรู้ข้อมูลประเภทนี้ของคุณ

เว็บไซต์ติดต่อคุณอย่างไรเมื่อคุณลืมรหัสผ่าน

มีใครอีกบ้างที่มีสิทธิ์เข้าถึงช่องทางการติดต่อคุณได้

ถามนักเรียนของคุณ

คนแปลกหน้าสามารถรู้ข้อมูลส่วนตัวที่เชื่อมโยงกับคำตอบของคำถามรักษาความปลอดภัยของคุณได้อย่างไร

1. โพสต์โซเชียลมีเดีย การค้นหาข้อมูลสาธารณะทางออนไลน์ การเดาหลายครั้ง การติดต่อกับเพื่อนคุณ เป็นต้น

ตัวอย่างของโพสต์โซเชียลมีเดียที่มีข้อมูลส่วนตัวมีอะไรบ้าง

1. ตัวอย่างเช่น Instagram ของแมวคุณที่มีชื่ออยู่ในคำบรรยายภาพ รูปภาพที่มีแท็กตำแหน่งที่ตั้ง หรือโพสต์อวยพรวันเกิดที่เปิดเป็นสาธารณะ

คุณสามารถใช้ Google

เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับใครคนหนึ่งและแฮ็กห้สผ่านของเขาได้อย่างไร

1. หากเครื่องมือค้นหาแสดงรูปภาพของนักเรียนชั้นมัธยมศึกษาปีที่ 3 บนหนังสือพิมพ์ออนไลน์ของโรงเรียน คุณอาจหาชื่อคุณครูของชั้นมัธยมศึกษาปีที่ 3 นั้นได้

ส่วนที่สอง

บอกนักเรียนของคุณ

การโพสต์ข้อมูลที่มีคำตอบของคำถามรักษาความปลอดภัยของคุณเป็นสิ่งที่ไม่ปลอดภัยอย่างมาก ตรวจสอบให้แน่ใจว่าได้เลือกคำถามรักษาความปลอดภัยที่มีคุณคนเดียวที่ตอบได้ นอกจากนั้น คุณยังสามารถสมมติคำตอบของคำถามรักษาความปลอดภัยขึ้นเองได้

ทราบใดที่คุณบันทึกคำตอบเอาไว้ในตัวจัดการรหัสผ่านหรือคำตอบนั้นจดจำได้ง่าย

เว็บไซต์อาจติดต่อผู้ใช้โดยใช้หมายเลขโทรศัพท์มือถือหรืออีเมลที่เชื่อมโยงกับบัญชีผู้ใช้ หากผู้ใช้ลืมรหัสผ่านของตน ทางเว็บไซต์มักจะมอบรหัสผ่านชั่วคราวหรือไฮเปอร์ลิงก์ที่ผู้ใช้สามารถคลิกเพื่อรีเซ็ตรหัสผ่านของตนเองได้

ถามนักเรียนของคุณ

การตรวจสอบว่าคนที่ขอรหัสผ่านใหม่คือผู้ใช้จริงๆ โดยวิธีการนี้ปลอดภัยหรือไม่

จะเกิดอะไรขึ้นหากคุณแชร์อีเมลที่เชื่อมโยงกับบัญชีผู้ใช้กับคนอื่น

1. โดยปกติแล้ว การใช้ลิงก์รีเซ็ตรหัสผ่านเป็นวิธีที่ปลอดภัย แต่ถ้าคุณแชร์บัญชีผู้ใช้หรือรหัสผ่านกับผู้อื่น ก็ถือเป็นเรื่องเสี่ยงได้

บอกนักเรียนของคุณ

การแฮ็กทางสังคมสามารถเกิดขึ้นได้โดยการที่มีคนติดต่อคุณโดยตรงหรือพยายามหลอกล่อให้คุณบอกข้อมูลของคุณ บางครั้ง ผู้คนจะส่งอีเมลหาคุณโดยแฝงตัวเป็นผู้อื่น (เช่น เพื่อน สมาชิกครอบครัว หรือเจ้าหน้าที่ธนาคาร) และขอให้คุณแชร์ข้อมูลสำคัญ (เช่น วันเกิด) เพื่อยืนยันตัวตนของคุณ หรืออาจมีเล่ห์เหลี่ยมแบบเนียนกว่านั้น เช่น หากมีคนแฮ็กบัญชีผู้ใช้โซเชียลมีเดียของคุณและส่งข้อความหาคุณ (และอาจอีกหลายๆ

คน) เพื่อถามวันเกิดของคุณหรือบ้านเกิดของคุณ หากคุณได้รับข้อความแปลกๆ จากเพื่อน
คุณอาจลองติดต่อเพื่อนของคุณก่อน (นอกแพลตฟอร์มโซเชียลมีเดีย)
เพื่อตรวจสอบว่าเพื่อนส่งข้อความนั้นให้คุณจริงๆ

การ жуใจมที่ใช้อีเมลหรือเว็บไซต์ที่ดูสมจริงเรียกว่าการฟิชชิ่ง
และอาจนำไปสู่การโจรกรรมข้อมูลระบุตัวตน ตัวอย่างเช่น
ผู้โจรกรรมข้อมูลระบุตัวตนอาจเปิดบัตรเครดิตโดยใช้ชื่อของคุณและนำบัตรเครดิตไปใช้งาน
ซึ่งทำให้คุณเปิดบัตรเครดิตได้ยากขึ้นในอนาคต

การฟิชชิ่งช่วยให้โจรสามารถแฝงตัวเป็นคุณและเข้าถึงข้อมูลอื่นๆ ได้
ซึ่งทำให้โจรสามารถสอดแนมผ่านอีเมลของคุณ ส่งข้อความหาเพื่อนคุณโดยแฝงตัวว่าเป็นคุณ
หรือขโมยเงินของคุณ นอกจากนั้น กระบวนการนี้ยังช่วยให้โจรสามารถบล็อกคุณออกจากบัญชี
ผู้ใช้ของคุณได้โดยสร้างรหัสผ่านใหม่ที่คุณไม่ทราบขึ้นมา

งาน

ใบงาน

งาน

ให้ผู้เข้าร่วมตอบคำถามต่อไปนี้และเพิ่มคำตอบของพวกเขาลงในใบงานสำหรับการเรียนรู้เกี่ยวกับรหัสผ่านในรูปแบบของข้อความหรือรูปภาพ

1. บอกแนวคิด 3

ข้อที่คุณได้เรียนรู้จากกิจกรรมนี้ที่คุณจะนำไปใช้ในการสร้างรหัสผ่านในอนาคต

2. ในสถานการณ์ใดที่คุณรู้สึกว่าคุณสามารถแชร์รหัสผ่านของคุณกับคนอื่นได้

3. บอกเทคนิคสามข้อที่คุณสามารถใช้เพื่อแชร์รหัสผ่านของคุณกับคนอื่นได้อย่างปลอดภัย

4. จะเกิดอะไรขึ้นได้บ้างถ้ารหัสผ่านตกอยู่ในมือของบุคคลที่ไม่หวังดี ลองบอกมาสักสามข้อ