סיסמאות

המשתתפים ילמדו איך לשפר את האבטחה של המידע המקוון שלהם על ידי שימוש בסיסמאות חזקות ותחזוקה שלהן. המשתתפים ילמדו על העקרונות של תכנון סיסמאות חזקות ועל הבעיות הפוטנציאליות של שיתוף סיסמאות. הם ילמדו גם איך לשמור על בטיחות הסיסמאות שלהם ואיך לנקוט צעדים כדי למנוע גישה לא מורשית לחשבונות שלהם.

חומרים

לומדים על סיסמאות - דף לחלוקה

סיסמה - היסודות

חלק 1

ספר לתלמידים שלך

לעתים קרובות אנחנו לא מקדישים הרבה מחשבה לסיסמאות שבהן אנחנו משתמשים לאתרים, לאפליקציות ולשירותים. עם זאת, איכות הסיסמאות שלכם קובעת את רמת האבטחה של המידע שלכם.

אינטראקציה בכיתה

פתח דיון עם המשתתפים בעזרת השאלות הבאות. הזכר למשתתפים שחשוב לא לשתף את הסיסמאות האמיתיות שלהם בתרגיל זה או בכל תרגיל אחר.

שאל את התלמידים שלך

כמה סיסמאות יש לכם?

האם יש לכם סיסמאות שונות לכל אחד מחשבונות הדוא"ל והמדיה החברתית שלכם?

האם הן שונות מאוד או שאלה גרסאות של אותה סיסמה?

אם יש לכם יותר מסיסמה אחת, איך אתם זוכרים איזו סיסמה שייכת לאיזה חשבון?

שאל את התלמידים שלך

באיזו תדירות קורה שאתם שוכחים סיסמה חשובה?

מה אתם עושים כשאתם שוכחים סיסמה?

איך אתם דואגים לזכור בקלות את הסיסמאות שלכם?

האם יש סיסמה שאתם משתמשים בה כל יום?

מה היה קורה אם מישהו היה מגלה את הסיסמה שלכם ללא ידיעתכם?

האם התשובה תלויה בזהותו של אדם זה?

איזה סוג מידע מישהו היה יכול לגלות עליכם אם היה משתמש בסיסמה שלכם כדי להיכנס לחשבון שלכם?

חלק 2

אינטראקציה בכיתה

חלק את המשתתפים לזוגות.

ספר לתלמידים שלך

יחד עם בן הזוג שלכם, דברו על מה שהיה יכול לקרות אם מישהו שרוצה לעשות צרות היה מגלה את הסיסמה לפלטפורמת המדיה החברתית המועדפת שלכם.

אינטראקציה בכיתה

תן למשתתפים 5 דקות לדיון. בקש מהקבוצות לשתף את תוכן הדיונים שלהן.

ספר לתלמידים שלך

עכשיו דברו עם בן הזוג שלכם על מה שהיה קורה אם פורץ היה מגלה את הסיסמה לחשבון הבנק המקוון של ההורה/האדם שדואג לכם.

אינטראקציה בכיתה

תן למשתתפים 5 דקות לדיון. לאחר מכן בקש מהקבוצות לשתף את תוכן הדיונים שלהן.

חלק 3

ספר לתלמידים שלך

ייתכן שאתם תוהים איך פורץ יכול לגלות סיסמה פרטית. יש כמה דרכים; אחת מהן היא באמצעות הנדסה חברתית - או פיתוי מישהו לשתף את הסיסמה שלו. פורץ יכול לעשות זאת על ידי שליחת דוא"ל שנראה כאילו זוהי הודעה לגיטימית מפלטפורמה או מאתר שבו לאדם יש חשבון. הדוא"ל יכול לבקש מהאדם ללחוץ על קישור ולהתחבר באמצעות שם המשתמש והסיסמה שלו; כשהאדם יתחבר, מידע זה יהיה זמין לפורץ.

פורצים מנסים לפעמים לנחש סיסמאות על ידי שימוש בצירופים נפוצים כמו "סיסמה123", "בדיקה", שמכם הפרטי או שם המשפחה שלכם.

דרך נוספת שבה פורצים יכולים לגלות סיסמה פרטית היא באמצעות מה שנקרא התקפת "כוח גס". התקפה כזו מתרחשת כשפורץ מנסה להתחבר לחשבון שלכם על ידי ניסוי חוזר ונשנה של סיסמאות שונות. פורץ יכול לבצע התקפת "כוח גס" באופן ידני, אך היא מבוצעת לעתים קרובות על ידי הפעלת תוכנית מחשב שמנסה באופן מהיר ואוטומטי כל שילוב סיסמאות אפשרי שניתן להעלות על הדעת. לדוגמה, רשימה של סיסמאות סבירות, או קבוצת סיסמאות המהוות שילובי אותיות ומספרים, עד שהתוכנית מוצאת את קוד הסיסמה הנכון.

יש כמובן התקפות "כוח גס" מתוחכמות יותר. אם הסיסמה שלכם כלולה ברשימה של סיסמאות סבירות, כמו "123456" או "סיסמה", חלק מהתוכניות יכולות לנחש אותה מהר יותר על ידי ניסוי אפשרויות אלה לפני אפשרויות פחות סבירות או אפשרויות אקראיות. ההתקפה יכולה גם להיות ממוקדת יותר אם הפורץ יודע מידע עליכם. לדוגמה, אם הפורץ יודע שלכלב שלכם קוראים רקסי, הוא יכול לנסות את 'רקסי' עם שילובי מספרים שונים אחריו (למשל 'רקסי629' או

רקסי3020').

עקרונות תכנון

חלק 1

שאל את התלמידים שלך

מי יודע מהי סיסמה "חזקה" או "חזקה יותר"? למה זה רעיון טוב?

ספר לתלמידים שלך

סיסמה חזקה עוזרת להגן על המידע שלכם. סיסמה חזקה אמנם לא מבטיחה שהחשבון שלכם לא ייפרץ, אך סיסמה חלשה מאפשרת לאנשים לגשת למידע שלכם בצורה קלה הרבה יותר.

תרגיל סיסמאות

שאל את התלמידים שלך

איך נראות סיסמאות חלשות?

1. רשימה חלקית של דוגמאות: 'סיסמה', '12345', 'שלום!', תאריך לידה, כינוי.

מדוע לדעתכם סיסמאות אלה חלשות?

1. אדם אחר ו/או מחשב שמפעיל התקפת "כוח גס" יכולים לנחש אותן בקלות.

באילו דרכים ניתן להפוך סיסמה לחזקה יותר?

1. הוספת מספרים, אותיות גדולות וקטנות, סמלים, הארכת הסיסמה והימנעות משימוש במילים ובביטויים נפוצים לבדם.

אינטראקציה בכיתה

לאחר שהמשתתפים מביעים את דעתם, כתוב על הלוח את ההוראות הבאות:

יש לכלול לפחות מספר אחד.

יש לכלול לפחות סמל אחד.

יש לכלול לפחות אות גדולה אחת ואות קטנה אחת.

סיסמאות צריכות להכיל לפחות 7 תווים.

יש לבחור סיסמאות שניתן לזכור בקלות (אלא אם משתמשים במנהל סיסמאות).

מנהל סיסמאות הוא אתר או אפליקציה שעוזרים למשתמשים לשמור ולארגן את הסיסמאות שלהם.

אין ליצור סיסמאות הכוללות מילה נפוצה בודדת או מידע אישי (תאריך לידה, שם הורה וכן הלאה).

אין להשתמש באותה סיסמה באתרים שונים.

ספר לתלמידים שלך

יש שתי גישות ליצירת סיסמאות חזקות. הראשונה היא להשתמש ב"מתכון לסיסמאות" כמו זה שמופיע על הלוח. שימוש במתכון כזה מעודד אתכם לכלול מרכיבים שקשה לנחש בסיסמה של טקסט/מספרים, וכך קשה יותר לנחש את הסיסמה עצמה. החיסרון של גישה זו הוא שקשה יותר לזכור את הסיסמאות.

סיסמאות חזקות

ספר לתלמידים שלך

גישה אחרת ליצירת סיסמאות חזקות קשורה לאורך הסיסמה. מכיוון שחוזק הסיסמה קשור לאורך הסיסמה, שימוש ברצף של ארבע מילים או יותר שאינן קשורות זו לזו מקשה מאוד על ניחוש הסיסמאות על ידי בני אדם והתקפות "כוח גס". היתרון הנוסף של שיטה זו הוא שהתוצאה היא סיסמאות שקל יותר לזכור בהשוואה לשיטת המתכון.

לסיום, ניתן להשתמש בשילוב של שתי השיטות על ידי יצירת רצף של ארבע מילים או יותר שאינן קשורות זו לזו, והוספת סמלים ומספרים.

לכל השיטות השונות האלה יש אותה מטרה: פיתוח סיסמאות ייחודיות שיהיה קשה לאנשים אחרים לנחש.

ספר לתלמידים שלך

חלק את המשתתפים לזוגות.

בזוגות, נסו ליצור סיסמה חזקה בעזרת ההוראות הכתובות על הלוח. זכרו שיכולה להיות סיסמה שקשה למחשב לנחש באופן אקראי, אך ניתן עדיין לנחש אותה בקלות על ידי אדם או מחשב המכיל רשימה של סיסמאות ארוכות נפוצות. בסוף הפעילות לא נאסוף את הפתקים עם הסיסמאות שלכם. מומלץ שלא תשתמשו בסיסמה הזו בפועל באחד החשבונות שלכם, מכיוון שחברי הקבוצה יידעו אותה.

תן למשתתפים 5 דקות לכך. לאחר מכן הסתובב בחדר ושאל את המשתתפים מה לדעתם הדוגמאות החזקות ביותר של סיסמאות שהם יצרו. שאל את המשתתפים אם הם יכולים לזכור את הסיסמאות שיצרו מבלי להסתכל בהן ישירות.

אתרים מסוימים ידרשו שהסיסמה שלכם תעמוד בחלק מהתנאים האלה (או בכולם), אך באתרים

אחרים אין הגבלות כאלה. ניתן גם ליצור סיסמאות באמצעות רצף של מילים נפוצות אקראיות.

אינטראקציה בכיתה

באותם זוגות, בקש מהמשתתפים ליצור סיסמאות חדשות שיהיו רצף מילים. אמור להם שצריכות להיות ארבע מילים לפחות בסיסמה כדי שהיא תהיה גם חזקה וגם יהיה קל לזכור אותה. תן למשתתפים 5 דקות לכך. לאחר מכן הסתובב בחדר ובקש מהמשתתפים דוגמאות לסיסמאות. שוב, הזכר למשתתפים שהדף לא ייאסף בסוף הפעילות, ושאין להשתמש בסיסמאות בחשבונות שלהם.

ספר לתלמידים שלך

יש אתרים שמשתמשים במערכת בשם אימות רב-שלבי (או דו-שלבי) כדי לוודא את זהותכם. אתרים אלה משתמשים לעתים קרובות בהודעות טקסט, באפליקציה או בדוא"ל כדי לשלוח קוד חד-פעמי שיש להזין יחד עם הסיסמה.

שיטה זו יכולה לשפר מאוד את בטיחות החשבונות שלכם על ידי הוספת שכבת אבטחה נוספת שהרבה יותר קשה לפרוץ. לדוגמה, כדי להתחבר לחשבון שלכם, אדם צריך לדעת את הסיסמה שלכם וצריכה להיות לו גישה לאפליקציה, למכשיר או לכתובת הדוא"ל הקשורים לחשבון.

שמירה על בטיחות הסיסמאות

חלק ראשון

ספר לתלמידים שלך

גם אם אתם יוצרים סיסמה שקשה מאוד למחשב או לאדם לפצח, סיסמה יכולה להיות חלשה מבחינות אחרות.

שאל את התלמידים שלך

באילו דרכים סיסמאות יכולות להיות חלשות?

1. הדוגמאות כוללות, בין היתר: שימוש חוזר באותה סיסמה לכמה חשבונות, שימוש בסיסמה המכילה פרטים אישיים, שימוש באותה סיסמה במשך שנים רבות, שכחת סיסמה.

באיזו תדירות אתם חושבים שכדאי להחליף סיסמאות?

ספר לתלמידים שלך

גם סיסמאות טובות יכולות להיפרץ או להיגנב, אך יש דברים שאתם יכולים לעשות כדי להגן על עצמכם. אם יש פריצה לנתונים באתר שיש לכם חשבון בו, הקפידו לשנות את הסיסמה שלכם באתר זה וכן באתרים אחרים שבהם אתם משתמשים בסיסמאות דומות.

קשה לזכור הרבה סיסמאות ארוכות ומסובכות.

שאל את התלמידים שלך

האם אתם חושבים שכדאי לכתוב את הסיסמאות שלכם על פתק, או בקובץ מסמך במחשב שלכם? למה או למה לא?

אינטראקציה בכיתה

ציין אפשרויות כמו מצב שבו מישהו ימצא את הפתק או יבחין בקובץ במחשב. הסבר שאחת הגישות היא להשתמש במנהל סיסמאות - אפליקציה שעוזרת למשתמשים לשמור ולארגן את הסיסמאות שלהם.

חלק שני

ספר לתלמידים שלך

בכל יום אנחנו משתמשים בהרבה חשבונות שונים באתרים שונים. ההתחברות וההתנתקות מכל אתר בכל פעם יכולות להיות מסובכות.

שאל את התלמידים שלך

האם השתמשתם אי פעם בתכונה 'שמור סיסמה' בדפדפן שלכם כדי לשמור סיסמה של אתר? למה או למה לא?

האם אתם מבינים איך האתר זוכר מי אתם?

1. בקש הסברים. לאחר מכן הסבר שאתרים יכולים לזכור שאנשים התחברו על ידי אחסון קובצי Cookie. לאתר לעזור כדי שלכם במחשב המאוחסנים קטנטנים קבצים הם Cookie לזהות אתכם ואת המחשב שלכם בביקורים עתידיים, מבלי שתתחברו שוב. עם זאת, ניתן להשתמש בקובצי Cookie גם כדי לעקוב אחריכם כשאתם עוברים מאתר לאתר. זו אחת הדרכים שבאמצעותה מודעות יכולות לפלח אתכם.

האם זה בסדר לשמור סיסמה אם זה קורה במחשב שלכם?

שאל את התלמידים שלך

האם למחשב שלכם יש סיסמת התחברות?

מה אם אתם משתפים את המחשב עם אחרים?

1. במקרה זה, גם אם הסיסמה בשדה הסיסמה מוסתרת באמצעות נקודות שחורות או כוכביות, אנשים אחרים שמשתמשים במחשב שלכם יכולים לגלות את הסיסמה. העובדה שאינכם רואים את הסיסמה על המסך לא אומרת שהסיסמה אינה מאוחסנת במקום כלשהו.

שאל את התלמידים שלך

האם יש מקרים שבהם זה בסדר לשתף סיסמה? מתי? למה?

1. דוגמאות אפשריות יכולות להיות הורים שרוצים לדעת את הסיסמאות של ילדיהם, או חשבון משותף/משפחתי בשירות כמו Netflix.

האם אתם משתפים את הסיסמאות שלכם עם אחרים? אם כן, עם מי/למה?

אם יש לכם חבר קרוב והוא ישתמש בנימוק של "אם באמת אכפת לך ממני", האם זה יגרום לכם לשתף איתו את הסיסמה שלכם? למה או למה לא?

ספר לתלמידים שלך

אתם יכולים לבחור לשתף את הסיסמה שלכם עם מישהו שחשוב לכם, אבל העובדה שאכפת לכם ממנו לא אומרת בהכרח שהוא צריך לקבל גישה מלאה לחשבונות המקוונים שלכם.

חשבו היטב על מערכת היחסים שלכם עם האדם הספציפי לפני שאתם משתפים, כולל איך מערכת היחסים הזו עשויה להשתנות עם הזמן. לדוגמה, שיתוף עם הורה/אדם שדואג לכם הוא בחירה שונה מאוד משיתוף עם החבר הטוב שלכם.

שאל את התלמידים שלך

מה יכול לקרות לכם אם תשתפו סיסמה?

1. מישהו יכול לפרוץ לחשבונות הבנק שלכם, להתחזות לכם באינטרנט או לגלות סודות שאתם מסתירים.

אם הייתם משתפים סיסמה לחשבון, האם הייתם משתמשים בחשבון זה בצורה שונה?

שאל את התלמידים שלך

האם יש דברים שלא הייתם צופים בהם ב-Netflix או לא הייתם כותבים בדוא"ל אם מישהו אחר היה יכול לראות מה אתם עושים?

אינטראקציה בכיתה

המשתתפים צריכים לחשוב על התנהגותם כשהם משתמשים בחשבון משותף. הם צריכים לזכור שהפעילות המקוונת שלהם גלויה למשתמשים אחרים בחשבון.

שאל את התלמידים שלך

אם החשבון הוא ייצוג וירטואלי שלכם, כמו פרופיל במדיה חברתית, האם זה בסדר לאפשר לאנשים אחרים להשתמש בחשבון?

אינטראקציה בכיתה

דברו על האפשרות שמישהו יתחזה אליכם וישלח הודעות לחבריכם.

שאל את התלמידים שלך

האם אתם מאפשרים למכשירים שבהם אתם משתמשים לשמור את הסיסמאות שלכם? למה או למה לא? האם זה אומר ששמירת סיסמאות בטלפון או במחשב האישי שלכם היא פעולה בטוחה? מה קורה אם אתם משאילים לחבר את הטלפון או המחשב?

האם יש מכשירים שאתם משתפים עם אחרים, למשל בני משפחה או חברים? האם אתם משתפים חשבון במכשיר כזה, או שלכל אדם יש חשבון משלו?

האם אתם משתמשים לפעמים במכשיר "ציבורי", למשל בספרייה, בבית הספר או במקום אחר? האם אתם עושים במכשיר זה את אותם דברים שאתם עושים במקומות אחרים?

חלק שלישי

אינטראקציה בכיתה

חלק את המשתתפים לזוגות.

ספר לתלמידים שלך

בזוגות, ספרו זה לזה אם אי פעם התחברתם למחשב בבית ספר, בספרייה או בסביבה קהילתית אחרת וראיתם שמישהו אחר היה עדיין מחובר לחשבון המדיה החברתית או הדוא"ל שלו. בקש מהמשתתפים לחשוב אם הם היו מחטטים בחשבון או עושים משהו אחר.

אינטראקציה בכיתה

תן למשתתפים 5 דקות לדיון ולאחר מכן בקש מהם לשתף את תשובותיהם עם הקבוצה. הנחה דיון קבוצתי על שימוש לא מורשה שכזה.

גישה לא מורשית לחשבונות

חלק ראשון

אינטראקציה בכיתה

לתשומת לבך: חלק מהתוכן בפעילות זו נסקר ב"פעילות מס' 1: סיסמה - היסודות". תוכל להחליט אם ברצונך לעבור שוב על החומר או לדלג עליו.

ספר לתלמידים שלך

אחרים יכולים לגשת לחשבון שלכם, אפילו מבלי לדעת מראש או להצליח בניחוש אקראי של הסיסמה שלכם. אם מישהו יודע די פרטים אישיים עליכם, הוא יכול לנחש ניחושים מושכלים לגבי הסיסמה שלכם, או שהוא יכול לשכנע מישהו בחברה למסור את הפרטים שלכם. מכיוון שהוא לא משתמש בטכנולוגיה כדי לפרוץ לחשבונות שלכם, התקפה מסוג זה נקראת פריצה חברתית או הנדסה חברתית.

שאל את התלמידים שלך

הרימו יד אם אי פעם שכחתם את הסיסמה שלכם לאתר כלשהו.

מה קורה כשאתם לוחצים על "שכחתי את הסיסמה"?

1. האתר בדרך כלל מבקש תשובות לשאלות אבטחה, או מנסה לפנות אליכם באמצעות מספר טלפון או דוא"ל.

מהן חלק משאלות האבטחה שהאתר שואל?

1. הסבר איך חלק מהשאלות הן כאלה שחברים או מכרים יכולים לדעת או לנחש את התשובות להן. דברים כמו: שם של חיית מחמד, מקום לידה, שם הנעורים של האם, שם של מורה אהוב, שם של חבר טוב, קבוצת ספורט אהובה.

מי עוד יכול לדעת פרטים כאלה עליכם?

איך אתר פונה אליכם כששכחתם את הסיסמה?

למי עוד יכולה להיות גישה לנקודות יצירת הקשר שלכם?

שאל את התלמידים שלך

איך אדם זר יכול לגלות את הפרטים האישיים הקשורים לתשובותיכם לשאלות האבטחה?

1. פוסטים במדיה חברתית, חיפושים מקוונים של מידע ציבורי, ניחושים חוזרים ונשנים, פנייה אל חבריכם וכן הלאה.

האם תוכלו לציין דוגמאות של פוסטים במדיה חברתית עם פרטים אישיים?

1. לדוגמה, תמונת אינסטגרם של החתול שלכם כששמו מופיע בכיתוב, תמונה עם תיוג של מיקום, או פוסטים ציבוריים על ימי הולדת.

איך ניתן להשתמש ב-Google כדי לקבל מידע נוסף על מישהו ולפרוץ את הסיסמה שלו?

1. אם מנוע חיפוש מראה לכם תמונת מחזור של מישהו מכיתה ט' בעיתון בית הספר שמופיע באינטרנט, אתם יכולים לגלות איך קראו למורה שלו בכיתה ט'.

חלק שני

ספר לתלמידים שלך

פרסום מידע המכיל את התשובות לשאלות האבטחה שלכם יכול להיות מאוד לא בטוח. הקפידו לבחור שאלות אבטחה שרק אתם יודעים את התשובות להן. אתם יכולים גם להמציא תשובות לשאלות האבטחה, בתנאי שתשמרו אותן במנהל סיסמאות או שקל לזכור אותן.

אתרים יכולים לפנות למשתמשים באמצעות מספר טלפון או דוא"ל המשויכים לחשבון המשתמש. אם משתמש שוכח את הסיסמה שלו, אתרים מספקים לעתים קרובות סיסמה זמנית או קישור שהמשתמש יכול להשתמש בו כדי לאפס את הסיסמה.

שאל את התלמידים שלך

האם זוהי דרך בטוחה לוודא שהאדם שמבקש את הסיסמה החדשה הוא המשתמש עצמו?

מה קורה אם אתם משתפים את כתובת הדוא"ל המשויכת לחשבון?

1. השיטה של קישור לאיפוס הסיסמה היא שיטה בטוחה רוב הזמן, אך אם אתם משתפים חשבון או סיסמה עם מישהו אחר, היא חושפת אתכם לסיכון.

ספר לתלמידים שלך

פריצה חברתית יכולה להתבצע על ידי אנשים שפונים אליכם ישירות ומנסים לפתות אתכם למסור להם את הפרטים שלכם. לפעמים אנשים שולחים לכם דוא"ל שבו הם מתחזים למישהו אחר (למשל חבר, בן משפחה או מישהו מהבנק) ומבקשים מכם לשתף איתם מידע חשוב (למשל תאריך הלידה שלכם) כדי לאמת את זהותכם. לפעמים זה נעשה בצורה מתוחכמת יותר, למשל אם מישהו פורץ לחשבון המדיה החברתית של אחד מחבריכם ושולח לכם הודעה (ואולי גם לרבים אחרים) שבה הוא שואל מה תאריך הלידה שלכם או איפה גדלתם. אם אתם מקבלים הודעות מחבר שנראות מוזרות, כדאי לכם לפנות תחילה לחבר זה (מחוץ לפלטפורמת המדיה החברתית) כדי לבדוק אם הוא באמת שולח את התוכן הזה.

התקפות שמשתמשות בדוא"ל או באתר שנראים אמיתיים נקראות דיוג, והן יכולות להוביל לגניבת זהות. לדוגמה, גנב זהות יכול לפתוח כרטיסי אשראי בשמכם ולהשתמש בהם, וזה יכול

להקשות עליכם לקבל כרטיס אשראי כשתהיו גדולים.

דיוג יכול לאפשר לגנב להתחזות לכם ולגשת למידע נוסף, וכך הוא יוכל לחטט בדוא"ל שלכם, לשלוח הודעות לחבריכם כשהוא מתחזה לכם, או לגנוב את כספכם. תהליך זה יכול גם לאפשר לגנב לחסום את החשבון שלכם בפניכם על ידי יצירת סיסמה חדשה שאינכם יודעים.

משימה

דף לחלוקה

משימה

בקש מהמשתתפים להשיב לשאלות הבאות ולהוסיף את תשובותיהם כטקסט או כאובייקט חזותי לדף 'לומדים על סיסמאות'.

1. אילו שלוש תובנות ממפגש זה תיישמו בפעם הבאה שתצטרכו ליצור סיסמה?
2. ציינו מקרה אחד שבו לדעתכם זה בסדר לשתף את הסיסמה שלכם עם מישהו אחר.
3. באילו שלוש אסטרטגיות אתם יכולים להשתמש כדי לשתף את הסיסמה שלכם עם מישהו אחר ללא חשש?
4. ציינו שלוש דוגמאות של דברים שיכולים להשתבש אם סיסמה נופלת לידיים הלא נכונות.