אאוץ! | אפריל 2017

מרכז סליקה בנקאי בע"מ שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- מהם משפטי סיסמאות
- שימוש במשפטי סיסמאות באופן מאובטח
- משאבים

משפטי סיסמאות

רקע כללי

על בסיס יומיומי משתמשים בסיסמאות, החל מגישה לדוא"ל או לאתר הבנקאות באינטרנט, רכישת מוצרים ואף גישה לטלפון החכם שלך. עם זאת, סיסמאות הן גם אחת הנקודות החלשות ביותר שלך; אם מישהו לומד או מנחש את הסיסמה שלך הוא יכול לגשת לחשבונות שלך בדיוק כמוך, דבר המאפשר לו להעביר את הכסף שלך, לקרוא את המיילים שלך או לגנוב את זהותך. לכן סיס־מאות חזקות חיוניות על מנת להגן עליך. עם זאת, סיסמאות בדרך כלל מבלבלות, קשה לזכור אותן וקשה להקליד אותן. בעלון זה תוכל ללמוד כיצד ליצור סיסמות חזקות שיהיה לך קל לזכור ולהקליד – הם נקראים משפטי סיסמאות.

עורך אורח

מי-נוף וין היא מדריכת SANS מוסמכת, מנכ"לית ויועצת עבור פתרונות IT מאובטחים. היא בעלת מומחיות בהסמכות מובילות, מעל 14 שנים בפיתוח, תהליכים, וניהול תוכנית אבטחת סייבר לתעשיות ומגזרים שונים. טוויטר: **@MenopN** :Twitter
לינקדאין: My-Ngoc "Menop" Nguyen

משפטי סיסמאות

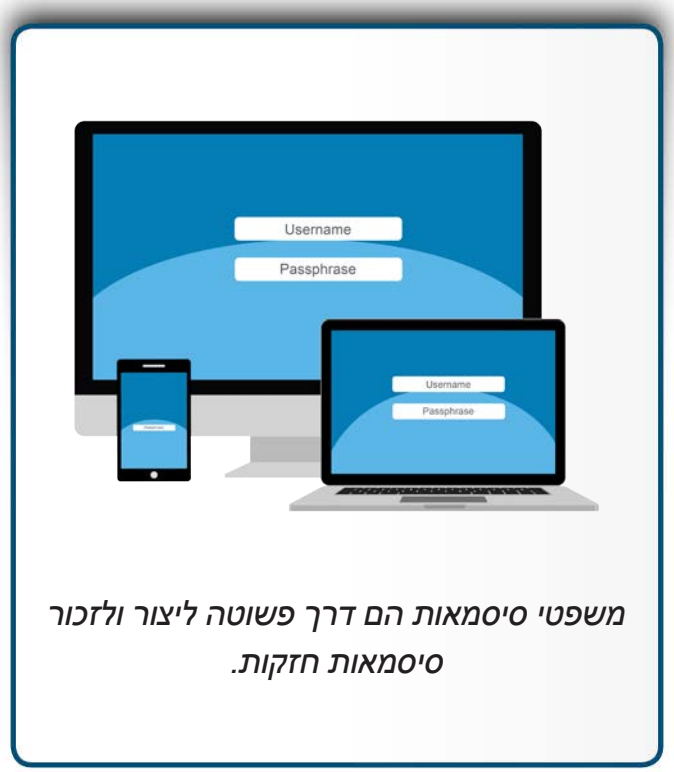
האתגר העומד בפני כולנו הוא, שתוקפי הסייבר פיתחו שיטות מתוחכמות ויעילות לניחוש של סיסמאות. משמעות הדבר כי התוקפים יכולים לפרוץ את הסיסמאות במידה והם חלשות או קלות לניחוש. צעד חשוב שיעזור לך להגן על עצמך הוא להשתמש בסיסמאות חזקות. בדרך כלל זה נעשה על ידי יצירת סיסמאות מורכבות, אולם סיסמאות כאלו יכול להיות קשה לזכור, מבלבל וקשה להקליד. במקום זאת, אנו ממליצים לך להשתמש במשפטי סיסמאות, סדרה של מילים אקראיות או משפט. ככל שיש יותר תווים, משפט הסיסמה שלך יותר חזק. היתרון הוא שמשפטי הסיסמאות הרבה יותר קל לזכור ומצד שני קשה מאוד לתוקפי סייבר לפרוץ את הסיסמה. הנה שתי דוגמאות שונות.

לקחת-בקלות-את-החיים
זמן לתה 01:23

מה הופך את משפטי הסיסמאות האלו לחזקים כל כך, זה לא רק האורך של הסיסמה, בנוסף הם משתמשים באותיות גדולות וסמלים (זוכרים, רווחים וסימני פיסוק הם סימנים). במקביל קל לזכור את משפטי הסיסמאות. אתה יכול לעשות את משפט הסיסמה אפילו חזק יותר אם אתה רוצה על ידי החלפת אותיות עם מספרים או סמלים, כגון החלפת האות

משפטי סיסמאות

‹a› עם סמל "@" או האות "o" עם המספר אפס. במי־ דה ואתר אינטרנט או תוכנה מגבילים את כמות התווים שתוכל להשתמש בסיסמה, השתמשו במספר התווים המרבי המותר.



משפטי סיסמאות הם דרך פשוטה ליצור ולזכור סיסמאות חזקות.

שימוש מאובטח במשפט הסיסמה

עליך להיות זהיר בצורה שאתה משתמש במשפטי הסיסמאות. משפטי הסיסמאות לא יעזור לך אם פושעי הסייבר יכולים בקלות לגנוב או להעתיק אותו.

1. השתמש בביטוי סיסמה שונה לכל חשבון או מכשיר שיש לך. לדוגמה, אף פעם לא להשתמש באותה הסיסמה עבור מקום העבודה או הכניסה לחשבון הבנק שלך יש להפריד בין החשבונות האישיים שלך, כגון פייסבוק או טוויטר. בדרך זו, אם אחד מהחשבונות שלך נפרץ, החשבונות האחרים שלך עדיין בטוחים. אם יש לך משפטי סיסמאות רבים מכדי לזכור (וזה נפוץ מאוד), כדאי להשתמש במנהל סיסמאות. זוהי תוכנה מיוחדת אשר מאחסנת באופן מאובטח את כל משפטי הסיסמאות שלך בשבילך. ככה שתי הסיסמאות היחידות שאתה צריך לזכור הם הכניסה למחשב או למכשיר שלך ותוכנת ניהול הסיסמאות.
2. לעולם אל תשתף את משפט הסיסמה שלך או האסטרטגיה שלך ליצירת אותם משפטי סיסמאות עם אף אחד אחר, כולל עמיתים לעבודה ואף הממונה עליך. זכור, ביטוי סיסמה הוא סוד; אם מישהו אחר יודע את משפט הסיסמה הוא כבר לא בטוח. אם בטעות שיתפת את משפט הסיסמה עם מישהו אחר, או שאתה מאמין כי משפט הסיסמה שלך נפרץ או נגנב, יש לשנות אותו מיד. היוצא מן הכלל היחידי הוא במידה ואתה רוצה לשתף את משפט הסיסמה אישי שלך עם בן משפחה מהימן ביותר במקרה של מצב חירום. גישה אחת היא לרשום את משפט הסיסמה אישי (לוודא שהם אינם קשורים לעבודה), ולאחסן אותם במקום בטוח, ולשתף את המיקום עם בן משפחה מהימן ביותר. ככה אם משהו יקרה לך ואתה צריך עזרה, יקיריכם יכולים לגשת לחשבונות הקריטיים שלך.
3. אין להשתמש במחשבים ציבוריים, כמו אלו בבתי מלון או בבתי קפה אינטרנט, על מנת להתחבר לחשבונות שלך. מאחר שכל אחד יכול להשתמש במחשבים אלה, הם עלולים להיות נגועים וללכוד את ההקלדות שלך. חשוב להיכנס לחשבונות שלך במחשבים מהימנים או מכשירים ניידים.
4. חשוב לשים לב, באתרים שבהם אתה נדרש לענות על שאלות אישיות. שאלות אלה משמשות כאשר שכחת את משפט הסיסמה שלך ויש צורך לאפס אותו. הבעיה היא שאת התשובות לשאלות האלו ניתן למצוא לעתים קרובות

משפטי סיסמאות

באינטרנט, או אפילו בעמוד הפייסבוק שלך. ודא כי כאשר אתה עונה על שאלות אישיות עלייך להשתמש במידע שאינו זמין לציבור או אפילו מידע פיקטיבי שהמצאת. לא זוכר את כל התשובות לשאלות האבטחה האלו? בחר נושא, למשל דמות מסרט ועליה לבסס את תשובותיך. אפשרות נוספת היא שוב להשתמש במנהל סיסמאות, רובם מאפשרים לך לאחסן מידע נוסף בצורה מאובטחת.

5. חשבונות מקוונים רבים מציעים משהו שנקרא אימות דו-גורמי, הידוע גם בשם אימות דו-שלבי. זה מקום שבו אתה צריך יותר מאשר משפט סיסמה על מנת להתחבר, כגון סיסמא הנשלחת למכשיר החכם שלך. אפשרות זו היא הרבה יותר בטוחה מאשר רק ביטוי סיסמה. במידת האפשר, תמיד לאפשר ולהשתמש בשיטות חזקות לבצע אימות.
6. על מנת להגן על הכניסה למכשירים ניידים בדרך כלל מחייבים קוד גישה אליהם. זכור כי קוד הגישה הוא לא יותר מאשר עוד סיסמה. ככל שקוד הגישה שלך ארוך יותר, כך גדלה האבטחה של המכשיר. התקנים ניידים רבים מאפשרים לך לשנות את קוד הגישה הסודי למשפט סיסמה או להשתמש באמצעים ביומטריים כמו טביעת האצבע שלך.
7. אם אתה כבר לא משתמש בחשבון, הקפד לסגור, למחוק או לבטל אותו.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

מנהל סיסמאות: https://securingthehuman.sans.org/ouch/2015#october2015

אימות דו-שלבי: https://securingthehuman.sans.org/ouch/2015#september2015

נעילת מסך הכניסה שלך: https://lockdownyourlogin.com

חמישה ימי לימודים על יסודות אבטחת סייבר: SANS SEC301: https://sans.org/sec301

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר


securingthehuman.sans.org/blog


/securethehuman


@securethehuman


securingthehuman.sans.org/gplus