מרכז סליקה בנקאי בע"מ
שירותי בנק אוטומטיים בע"מ
SANS SECURING THE HUMAN
עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

## בגיליון זה...

- סקירה כללית
- כיצד מנהלי הסיסמאות עובדים
- בחירת מנהל סיסמאות

# מנהל סיסמאות

## סקירה כללית

אחד הצעדים החשובים ביותר שתוכל לנקוט כדי להגן על עצמך באינטרנט הוא להשתמש בסיסמה ייחודית וחזקה לכל אחד מהחשבונות והאפליקציות שלך. לצערנו, סביר להניח שלא תוכל לזכור את כל הסיסמאות השונות שלך עבור כל החשבונות השונים. זו הסיבה שאנשים רבים עושים שימוש חוזר באותה סיסמה. לרוע המזל, שימוש חוזר באותה סי־סמה הוא מסוכן, שכן ברגע שמישהו מגלה או משיג את הסיסמה שלך, הוא מסוגל לגשת לכל החשבונות שלך בהם השתמשת באותה הסיסמה. פתרון פשוט הוא להשתמש במנהל סיסמאות, המכונה לפעמים כספת לסיסמאות. זוהי תוכנה מאובטחת אשר מאחסנת את כל הסיסמאות שלך, ולכן קל להשתמש בסיסמה שונה עבור כל חשבון או אתר. מנהל הסיסמאות מקל עלייך את הצורך לזכור סיסמאות מורכבות למספר חשבונות או אתרים, אתה רק צריך לזכור את הסיסמה הראשית על מנת להיכנס לתוכנת מנהל הסיסמאות שלך.

**עורך אורח**
כריס כריסטיאנסון הוא יועץ אבטחת מידע מקליפורניה, עם למעלה מ-20 שנות ניסיון והסמכות טכניות רבות. הוא נאם במספר רב של כנסים ותורם למאמרים רבים בתעשיית האבטחה. כריס ניתן להשגה ב @cchristianson ובאתר https://ismellpackets.com.

## כיצד מנהלי הסיסמאות עובדים

מנהלי סיסמאות עובדים על-ידי אחסון כל הסיסמאות במסד נתונים מוצפן, הנקרא לעתים כספת. מנהל הסיסמאות מצפין את התוכן של הכספת ומגן עליה באמצעות סיסמה ראשית שרק אתה (המשתמש) יודע. כאשר אתה צריך לשחזר את הסיסמאות שלך, למשל לצורך חיבור לחשבון הבנק המקוון שלך או הדואר האלקטרוני, אתה פשוט מקליד את הסיסמה הראשית שלך לתוך מנהל הסיסמאות כדי לפתוח את הכספת. במקרים רבים מנהל הסיסמאות ישחזר באופן אוטומטי את הסיסמה שלך ויכניס אותך בצורה מאובטחת לאתר שברצונך להתחבר. כל התהליך של שמירת הסיסמאות נהייה פשוט ומאובטח משום שיש לך סיסמאות ייחודיות, חזקות, ואתה לא צריך לזכור אותן.

מנהלי סיסמאות מסוימים מאחסנים את הכספת במחשב או במכשיר הנייד, בעוד שאחרים מאחסנים אותה בענן. בנוסף, רוב מנהלי הסיסמאות כוללים את היכולת לסנכרן באופן אוטומטי את תוכן הכספת של הסיסמאות שלך במספר מכשירים שאתה מאשר. בדרך זו, כאשר אתה מעדכן סיסמה במחשב הנייד, שינויים אלה מסונכרנים לכל המכשירים האחרים שלך.

© SANS Institute 2017

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

# מנהל סיסמאות

*מנהלי סיסמאות הם דרך פשוטה, נוחה ויעילה לאחסן ולהשתמש בסיסמאות הרגישות שלך בצורה מאובטחת.*

לא משנה היכן מאוחסן מסד הנתונים, עליך רק להתקין את תוכנת מנהל הסיסמאות ולהשתמש בה.

כאשר אתה מגדיר בפעם הראשונה את תוכנת ניהול הסיסמאות, עליך להזין או לייבא באופן ידני את פרטי משתמשי הכניסה והסיסמאות שלך. לאחר מכן, מנהל הסיסמאות יכול לזהות כאשר אתה מנסה להירשם לחשבון מקוון חדש או לעדכן את הסיסמה של חשבון קיים, לעדכן באופן אוטומטי את הכספת בהתאם. זה אפשרי כי רוב מנהלי הסיסמה עובדים יד ביד עם דפדפן האינטרנט שלך. שילוב זה גם מאפשר להם להיכנס באופן אוטומטי לאתרים ולאחסן את הסיסמה במאובטח.

זה קריטי כי הסיסמה הראשית שאתה משתמש בה כדי להגן על התוכן של תוכנת ניהול הסיסמאות היא סיסמה חזקה וקשה מאוד לניחוש. למעשה, אנו ממליצים שהסיסמה הראשית תהייה משפט-סיסמה, אחד מסוגי הסיסמאות החזקות ביותר האפשריות. אם מנהל הסיסמאות שלך תומך באימות דו-שלבי, מומלץ להשתמש בו עבור הסיסמה הראשית. לבסוף, הקפד לזכור את הסיסמה הראשית שלך. אם תשכח אותה, לא תוכל לגשת לסיסמאות האחרות שלך.

## בחירת מנהל סיסמאות

יש מנהלי סיסמאות רבים לבחירה. בסעיף מקורות אנו מספקים קישור לביקורות של מנהלי סיסמאות. בינתיים, כאשר אתה מנסה למצוא את התוכנה הכי טובה בשבילך, זכור את הדברים הבאים:

- מנהל הסיסמאות צריך להיות פשוט לשימוש. אם אתה מוצא שהפתרון מורכב מדי, שקול למצוא אחד אחר שמתאים לך יותר ולרמת המומחיות שלך.
- מנהל הסיסמאות אמור לפעול בכל המכשירים שאתה רוצה להתקין עליהם את התוכנה. בנוסף מנהל הסיסמאות ישמור על הסיסמאות שלך מסונכרנות בכל המכשירים שלך.
- השתמש רק במנהלי סיסמאות ידועים ואמינים. היזהר ממוצרים חדשים או בעלי משובים מועטים. פושעי הסייבר יכולים ליצור מנהלי סיסמאות מזויפים על מנת לגנוב את המידע שלך. חשוב מאוד לחשוד במידה והספק של התוכנה רושם שהוא פיתח פתרון ההצפנה ייחודי לו.

© SANS Institute 2017

שירותי בנק אוטומטיים בע"מ

מרכז סליקה בנקאי בע"מ

# מנהל סיסמאות

- הימנע מכל מנהל סיסמאות שטוען כי יוכל לשחזר את הסיסמה הראשית עבורך. זה אומר שהם יודעים את הסיסמה הראשית שלך, אשר חושפת אותך לסיכון גבוה.
- ודא שכל פתרון שתבחר ימשיך להיות מעודכן על ידי הספק באופן שוטף ולפני ההתקנה של תוכנת ניהול הסיסמאות תוודא שאתה מתקין את הגרסה הכי עדכנית.
- מנהל הסיסמאות צריך לכלול את היכולת ליצור סיסמאות חזקות באופן אוטומטי עבורך ולהראות לך את עוצמת הסיסמאות שבחרת.
- מנהל הסיסמאות אמור לתת לך את האפשרות לאחסן נתונים רגישים אחרים, כגון התשובות לשאלות האבטחה הסודיות שלך, כרטיסי אשראי או מספרי תעודות זהות.

מנהלי סיסמאות הם דרך מצוינת לאחסן בצורה מאובטחת את כל הסיסמאות ונתונים רגישים אחרים. עם זאת, מכיוון שהם שומרים על מידע חשוב, הקפד להשתמש בסיסמה ראשית ייחודית וחזקה, שתהייה קשה לניחוש או פיצוח, אך קלה לזכור מבחינתך.

## 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

| | |
|---|---|
| תוכנות מובילות לניהול סיסמאות של 2017: | https://www.pcmag.com/article2/0,2817,2407168,00.asp |
| משפטי סיסמה: | https://securingthehuman.sans.org/ouch/2017#april2017 |
| אימות דו-שלבי: | https://www.securingthehuman.org/ouch asked#september2015 |
| נעל את הכניסה שלך: | https://www.lockdownyourlogin.org/ |
| עצה אבטחה היומית של SANS: | https://www.sans.org/tip-of-the-day |

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Securing The Human, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה ouch@securingthehuman.org.

עורכי המערכת: 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