אאוץ! | אפריל 2019

עלון מודעות אבטחת מידע למשתמשי מחשב

הפיכת סיסמאות לדבר פשוט

סקירה כללית

לעתים קרובות אומרים לך שסיסמאות הן המפתח להגנה על החשבונות שלך (וזה נכון!), אבל לעתים רחוקות אתה מקבל דרך פשוטה לנהל וליצור באופן מאובטח את כל הסיסמאות שלך. הפעם אנו נכסה שלושה שלבים קלים כדי לפשט את השימוש בסיסמאות שלך, לנעול את החשבונות שלך ולהגן על העתיד שלך.

ביטויים

הימים של סיסמאות מטורפות ומורכבות הסתיימו. סיסמאות אלו קשה לזכור, קשה להקליד. בשימוש במחשבים המהירים של היום, קל יחסית לתוקף סייבר לפצח את הסיסמה. המפתח לסיסמאות טובות הוא להפוך אותן לארוכות יותר, כמה שיותר תווים, יותר טוב. אלו נקראים משפטי סיסמה, סוג של סיסמה חזקה המשתמשת במשפט קצר או מילים אקראיות. הנה שתי דוגמאות:

- **הגיע הזמן לקפה חזק וטעים!**
- **שבלול-אבוד-זוחל-בים-לאט**

שני משפטי סיסמאות אלו חזקים בגלל שהם באורך של יותר מ-20 תווים, קל לזכור אותם ופשוט להקליד, אבל קשה לפצח. אתה תיתקל באתרי אינטרנט או מצבים המחייבים אותך להוסיף סמלים, מספרים או אותיות גדולות לסיסמה שלך, וזה בסדר. זכור כי האורך הוא החשוב ביותר.

מנהלי סיסמאות

אתה צריך סיסמה ייחודית עבור כל חשבון. אם אתה משתמש באותה סיסמה עבור חשבונות מרובים, אתה מציב את עצמך בסכנה גדולה. כל מה שתוקף סייבר צריך לעשות הוא לפרוץ לאתר אינטרנט שבו אתה משתמש, לגנוב את הסיסמא שלך, ולאחר מכן להשתמש בסיסמה שלך להיכנס לכל החשבונות האחרים שלך בדיוק כמו שאתה עושה. זה קורה הרבה יותר פעמים ממנה שאתה חושב. לא מאמין בזה? בדוק את אתר האינטרנט https://haveibeenpwned.com כדי לראות באילו אתרים אתה משתמש שנפרצו בעבר ואת הסיסמאות שלך כפוטנציאל לסכנה. אז מה אתה צריך לעשות? השתמש במנהל סיסמאות.

אלו הן תוכניות מחשב מיוחדות המאחסנות את כל הסיסמאות שלך בכספת מוצפנת. אתה רק צריך לזכור סיסמה אחת, עבור מנהל הסיסמאות שלך. מנהל הסיסמאות באופן אוטומטי מאחזר את הסיסמאות שלך בכל זמן שאתה צריך אותן ואף ממלא את הסיסמה באתרי אינטרנט עבורך. למנהל סיסמאות יש גם תכונות אחרות כגון אחסון התשובות שלך לשאלות סודיות, מזהיר אותך כאשר אתה משתמש בסיסמא חוזרת, מחולל סיסמאות המבטיח לך להשתמש בסיסמאות חזקות, ותכונות רבות אחרות. רוב מנהלי הסיסמאות גם מסונכרנים באופן מאובטח על פני כמעט כל מחשב או התקן שלך, כך שלא משנה באיזה מערכת אתה משתמש יש לך גישה קלה ומאובטחת לכל הסיסמאות שלך.

לבסוף, הקפד לרשום את הסיסמה למנהל הסיסמאות שלך ולאחסן אותה במיקום בטוח בבית. מנהלי סיסמאות מסוימים אפילו מאפשרים לך להדפיס ערכת שחזור סיסמת הניהול. בדרך זו, אם תשכח את הסיסמה למנהל הסיסמאות שלך, יש לך גיבוי. לחלופין, אם אתה חולה או מוצא את עצמך במצב חירום, בן הזוג שלך או בן משפחה מהימן יכול לאחזר את המידע בשמך.

אימות דו-שלבי

אימות דו-שלבי (הנקרא לעתים קרובות אימות דו-גורמי, אימות דו-שלבי או אימות מרובה גורמים) מוסיף שכבה נוספת של אבטחה. זה מחייב אותך לשני שלבים כאשר אתה מתחבר לחשבונות שלך, את הסיסמה שלך וקוד מספרי שנוצר על ידי הטלפון החכם או שנשלחו לטלפון. תהליך זה מבטיח שגם אם תוקף סייבר ישיג את הסיסמה שלך הוא עדיין לא יכול להיכנס לחשבונות שלך. אימות דו-שלבי הוא פשוט להתקנה ואתה בדרך כלל רק צריך להשתמש בו פעם אחת כאשר אתה מתחבר ממחשב או התקן חדש. אפשר אימות דו-גורמי בכל עת, במיוחד עבור החשבונות החשובים ביותר שלך, כגון חשבון הבנק, חשבון השקעות או גישה לדוא"ל שלך. אם אתה משתמש במנהל סיסמאות, מומלץ מאוד להגן עליו באמצעות ביטוי סיסמה חזק ואימות דו-שלבי.

זה אולי נשמע טיפשי, אבל שלושה שלבים פשוטים אלה יעזרו לך להגן על העבודה שלך, המוניטין ועל העתיד הפיננסי שלך.

עורך אורח

ג'סטין הנדרסון (@SecurityMapper) הוא המייסד של חברת H&A לפתרונות אבטחה, מדריך מוסמך של SANS, ומחבר קורס בהגנת סייבר וקורס בהתמחות SIEM. הוא אוהב את כל הדברים הקשורים לסייבר וביטחון ויועץ מזה כ-15 שנה.

מקורות

האם נפרצתי?:	https://haveibeenpwned.com
אימות דו-שלבי:	https://TwoFactorAuth.org/
הנחיות בנושא הזהות דיגיטלית של NIST SP800-63B:	https://pages.nist.gov/800-63-3/sp800-63b.html
פוסטר: אתה יעד:	https://www.sans.org/u/OGi