

ouch!

עלון המודעות החודשי לביטחון עבורך

נפרצתי. עכשיו מה?

האם נפרצתי?

לא משנה כמה אתם מאובטחים, במוקדם או במאוחר אתם עלול לעבור תאונה ולהיפרץ. להלן רמזים שאולי נפרצתם ואם כן, מה לעשות.

החשבונות המקוונים שלכם

- בני משפחה או חברים אומרים שהם מקבלים ממכם הודעות יוצאות דופן או הזמנות שאתה יודע שלא שלחתם.
- הסיסמה שלכם לחשבון כבר לא עובדת, למרות שאתם יודעים שהסיסמה נכונה.
- אתם מקבלים התראות מאתרים שמישהו התחבר לחשבונכם כאשר אתם יודעים שלא התחברתם בעצמכם. אל תלחצו על אף קישור בהתראות כאלה כדי לבדוק את חשבונכם; במקום זאת, הקלידו את כתובת האתר בעצמכם בדפדפן שלכם, השתמשו בסימניה ששמרתם בעבר או גשו לחשבונכם מאפליקציה לנייד.

המחשב או המכשיר הנייד שלך

- תוכנית האנטי-וירוס שלכם מעלה התראה כי המערכת שלכם נגועה. ודאו שזו תוכנית האנטי-וירוס שלכם שמייצרת את ההתראה ולא חלון קופץ אקראי מאתר שמנסה להטעות אותכם להתקשר למספר או להתקין משהו אחר. לא בטוח? פיתחו ובידקו את תוכנית האנטי-וירוס שלכם כדי לאשר אם המחשב שלכם באמת נגוע.
- אתם מקבלים חלון קופץ שאומר שהמחשב שלכם הוצפן ועליכם לשלם כופר כדי להחזיר את הקבצים שלכם.
- נראה כי יישומים קורסים באופן אקראי או נטענים באטיות רבה.
- במהלך הגלישה באינטרנט, לעתים קרובות אתם מנותבים לדפים שלא רציתם לבקר בהם או שמופיעים דפים חדשים ולא רצויים.

נספח

- ישנם חיובים חשודים או לא ידועים בכרטיס האשראי שלכם או בחשבון הבנק שלכם שאתם יודעים שלא ביצעתם.

עכשיו מה? - כיצד להחזיר את השליטה

אם אתם חושדים שנפרצתם, הישארו רגועים; אתם תתגברו על זה. אם הפריצה קשורה לעבודה, אל תנסו לתקן את הבעיה בעצמכם; דווחו על כך מייד. אם מדובר במערכת או בחשבון אישי שנפרצו, הנה כמה צעדים שתוכלו לנקוט:

- **שחזור חשבונות מקוונים:** אם עדיין יש לכם גישה לחשבונכם, היכנסו ממחשב מהימן שאתם בטוחים שאינו נגוע ואפסו את הסיסמה שלכם. ברגע שאתם מתחברים, הקפדו להגדיר סיסמה חדשה, ייחודית וחזקה, כמה שיותר ארוכה יותר טוב. זיכרו, לכל אחד מהחשבונות שלכם צריכה להיות סיסמה אחרת. אם אינכם יכול לעקוב אחר כולן, אנו ממליצים להשתמש במנהל סיסמאות. כמו כן, אם זו אפשרות, הפעילו אימות רב שלבי (MFA) עבור חשבונותיכם, עזרו להבטיח שתוקפי הסייבר לא יוכלו לחזור. אם כבר אין לכם גישה לחשבונכם, פנו לאתר והודיעו להם שהשתלטו על חשבונכם.
- שחזור מחשב האישי או מכשיר: אם תוכנית האנטי-וירוס שלכם אינה מסוגלת לתקן את המחשב הנגוע או שאתם רוצים להיות בטוחים יותר שהמערכת שלכם בטוחה, שיקלו להתקין מחדש את מערכת ההפעלה ולבנות מחדש את המחשב. לעיתים קרובות הדבר דורש מחיקה או החלפה של הדיסק הקשיח ואז התקנה מחדש ועדכון של מערכת ההפעלה. אל תתקינו מחדש את מערכת ההפעלה מגיבויים. יש להשתמש בגיבויים רק לשחזור הקבצים האישיים שלכם. אם אתם מרגישים לא נוח לבנות מחדש, שיקלו להשתמש בשירות מקצועי שיעזור לכם. לחלופין, אם המחשב או המכשיר שלך ישנים, ייתכן שהגיע הזמן לרכוש מכשיר חדש.
- הצלת חשבונות פיננסיים: לבעיות בכרטיס האשראי שלכם או בחשבונות פיננסיים כלשהם, התקשרו מיד לבנק או לחברת כרטיסי האשראי שלכם. התקשרו אליהם באמצעות מספר טלפון מהימן, כגון מספר הטלפון המופיע בחלק האחורי של כרטיס הבנק שלכם, המספר המודפס בדוחות הכספיים שלכם, או בקרו באתר האינטרנט שלהם. עיקבו אחר דוחות האשראי והבנק שלכם לעתים קרובות. בנוסף, שיקלו להקפיא גישה לקבצי האשראי שלכם.

אם נגרם לכם נזק כספי או שאתם מרגישים מאוימים, דווחו על האירוע לאכיפת החוק המקומית.



עורך אורח

מקסים דיוורדט (טוויטר @alfasec) הוא מדריך מוסמך במכון SANS, בעיקר בהוראת קורסים להגנת הסייבר. הוא גם יועץ ראשי ב-NVISO, שם הוא מתמקד בציד איומים, תגובה לאירועים ובשלות לפרויקט SOC.

משאבים

כוחו של עדכו: <https://www.sans.org/security-awareness-training/resources/power-updating>
 יש גיבוי: <https://www.sans.org/security-awareness-training/resources/got-backups>
 סיסמאות: <https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf>
 כופרה: <https://www.sans.org/security-awareness-training/resources/ransomware>
 דיווח על גניבת זהות: <https://www.identitytheft.gov>
 הקפאת אשראי: <https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/>

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר

אאוי! יוצא לאור ומפורסם על ידי חברת Awareness Security SANS, הפצתו ברישיון license 0.4 ND-NC-BY Commons Creative. הנך רשאי להפיץ או להשתמש בעלון זה, כל עוד אתה לא מוכר או מבצע שינויים בעלון זה.
 עורכי המערכת: וולט סקריבנס, פיל הופמן, אלן וגנר, לס רידוט, פרינסס יאנג