



עלון המודעות החודשי לביטחון עבורך



הונאה טלפונית - התקפות טלפוניות והונאות

סקירה כללית

כשאתה חושב על פושע סייבר אתה בטח חושב על מוח רשע שיושב מאחורי מחשב ופותח התקפות מתוחכמות דרך האינטרנט. בעוד שחלק מפושעי הסייבר של ימינו אכן משתמשים בטכנולוגיות מתקדמות, רבים פשוט משתמשים בטלפון כדי להערים על קורבנותיהם. ישנם שני יתרונות גדולים לשימוש בטלפון: בניגוד להתקפות אחרות, יש פחות טכנולוגיות אבטחה שיכולות לזהות ולעצור התקפת שיחות טלפון; כמו כן, הרבה יותר קל לפושעים להעביר רגש ולבנות אמון בטלפון, מה שמקל על הטעיית קורבנותיהם. בואו ללמוד כיצד לזהות ולהפסיק את ההתקפות הללו.

כיצד פועלות התקפות טלפון?

ראשית, צריך להבין כי עבריינים אלה בדרך כלל עוקבים אחר הכסף, המידע או הגישה שלך למחשב שלך (או לשלושת אלה). הם עושים זאת בכך שהם מטעים אותך לעשות משהו שאתה לא צריך לעשות, טכניקה שנקראת "הנדסה חברתית". פושעי סייבר לעיתים קרובות יוצרים מצבים שמרגישים דחופים מאוד ומציאותיים בשיחה. כמה מהדוגמאות הנפוצות ביותר כוללות:

- המתקשר מעמיד פנים שהם מהממשלה ומודיע לך שיש לך מיסים שלא שולמו. הם מסבירים שאם אתה לא משלם את המסים שלך מייד תיכנס לכלא, ואז לוחץ עליך לשלם את המסים שלך באמצעות כרטיס האשראי שלך בטלפון. זו תרמית. הממשלה תשלח הודעות מס רשמיות רק בדואר רגיל.
- המתקשר מתיימר להיות מחברה כמו אמזון, אפל או תמיכה טכנית של מיקרוסופט ומסביר שהמחשב שלך נגוע. ברגע שהם משכנעים אותך שהמחשב שלך נגוע, הם לוחצים עליך לקנות את התוכנה שלהם או לתת להם גישה מרחוק למחשב שלך.
- הודעה קולית אוטומטית מודיעה לך שחשבון הבנק או כרטיס האשראי שלך בוטל, ועליך להתקשר למספר כדי להפעיל אותו מחדש. כשאתה מתקשר אתה מקבל מערכת אוטומטית שמבקשת ממך לאשר את זהותך כמו גם כל מיני שאלות פרטיות. זה ממש לא הבנק שלך. הם פשוט מקליטים את כל המידע שלך לצורך הונאה וגניבת זהות.

הגן על עצמך

- ההגנה הגדולה ביותר שיש לך נגד התקפת שיחות טלפון היא אתה עצמך. זכור את הדברים האלה: בכל פעם שמישהו מתקשר אליך ויוצר תחושת דחיפות או לחץ אדירים, היה חשוך ביותר. התוקפים מנסים להאיץ בך לעשות טעות. גם אם שיחת הטלפון נראית בסדר בהתחלה, אם היא מתחילה להרגיש מוזרה, אתה יכול לעצור ולהגיד "לא" "בכל עת".

- היזהר במיוחד ממתקשרים שמתקשים לרכוש כרטיסי מתנה או כרטיסי חיוב ששולמו מראש.
- לעולם אל תסמוך על זיהוי המתקשר. אנשים רעים מזייפים קרובות את המספר, כך שנראה שהוא מגיע מארגון חוקי או שיש לו קידומת זהה למספר הטלפון שלך.
- לעולם אל תאפשר למתקשר לקחת שליטה זמנית במחשב שלך או להערים עליך להוריד תוכנה. כך הם יכולים להדביק את המחשב שלך.
- אלא אם כן ביצעת את השיחה, לעולם אל תתן לצד השני מידע שכבר היה צריך לדעת. לדוגמה, אם הבנק התקשר אליך, הם לא צריכים לבקש את מספר החשבון שלך.
- אם אתה מאמין ששיחת טלפון היא זדונית, פשוט לנתק את השיחה. אם ברצונך לדווח ששיחת הטלפון הייתה לגיטימית, היכנס לאתר הארגון (כגון הבנק שלך) והתקשר ישירות למספר הטלפון של תמיכת הלקוחות בעצמך. בדרך זו, אתה באמת יודע שאתה מדבר עם הארגון האמיתי.
- אם שיחת טלפון מגיעה ממישהו שאינך מכיר באופן אישי, תן לשיחה לעבור ישירות לתא הקולי. בדרך זו תוכל לסקור שיחות לא ידועות בזמנך הפנוי. אפילו יותר טוב, בטלפונים רבים תוכלו להפעיל זאת כברירת מחדל באמצעות התכונה "אל תפריעו".

כמות הונאות והתקפות בטלפון גוברת. אתה ההגנה הטובה ביותר בזיהוי ובעצירתם.



עורך אורח

ג'ן פוקס מחזיקה בסמל היכל התהילה של DEF CON 23 להנדסה חברתית ומספק חינוך למודעות אבטחה כמומחית לתוכנית אבטחה בדומינו'ס. ניתן למצוא את ג'ן בטוויטר בכינוי [@j fox](https://twitter.com/jfox).

משאבים

הנדסה חברתית: <https://www.sans.org/sites/default/files/2020-10/OUCH%21%20Nov%202020%20-%20Social%20Engineering%20v.3-Hebrew.pdf>

התקפות מסרים / סמסטים:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt46b447ff815ff84/6047f261f9638443346d63ff/201912-OUCH-December-Hebrew.pdf>

הונאה מותאמת אישית: <https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Hebrew.pdf>

בארץ ניתן לדווח למרכז המבצעי לניהול אירועי סייבר [בטלפון 119](#)

תורגם לקהילה על ידי: גדי מרגלית ודרור ענב:

אנו! יוצא לאור ומפורסם על ידי חברת SANS Security Awareness, הפצתו ברישיון [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). 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.