



עלון מודעות אבטחת מידע למשתמשי מחשב

# התקפות בשיחות טלפון והונאות

## סקירה כללית

כאשר אתה חושב על פושעי סייבר אתה כנראה חושב על גאונים מרושעים שיושבים מאחורי מחשב ומשגרים התקפות מתוככמות דרך האינטרנט. בעוד שרבים ממושעי הסייבר של היום עושים שימוש בטכנולוגיות כמו דוא"ל או הודעות מיידיות, הרעים משתמשים גם בטלפון כדי להערים קורבנותיהם. שני יתרונות גדולים בהתקפות באמצעות הטלפון. ראשית, בניגוד לדוא"ל יש פחות טכנולוגיות אבטחה המנטרות את שיחות הטלפון שיכולות לזהות ולהפסיק התקפות. שנית, הרבה יותר קל עבור הרעים להעביר רגשות בטלפון, מה שמעלה את הסבירות להערים על קורבנותיהם. בואו ללמוד איך לזהות ולהפסיק את ההתקפות האלו.

## כיצד התקפות בשיחות טלפון עובדות?

ראשית, אתה צריך להבין מה מטרת התוקפים. הם בדרך כלל רוצים את כספך, מידע או גישה למחשב (או כל השלושה). הם עושים זאת על ידי הונאה, הם ישכנעו אותך לעשות את מה שהם רוצים. הרעים מתקשרים לאנשים ברחבי העולם, יוצרים מצבים שנראים דחופים מאוד. הם רוצים להוציא אותך מאיזון, להפחיד אותך, כדי שלא תחשוב בבהירות, ולאחר מכן ללחוץ אותך לעשות טעות. חלק מהדוגמאות הנפוצות ביותר כוללות:

המתקשר מעמיד פנים שהוא מגיע ממחלקת מס ממשלתית או משירות המסים ומספר לך שיש לך מסים שלא שולמו. הם מסבירים שאם לא תשלם את המסים שלך מיד תלך לכלא, ואז ילחצו עליך לשלם את המסים בטלפון באמצעות כרטיס האשראי שלך. זוהי הונאה, רוב מחלקות המס, כולל מס הכנסה, לא מתקשרים או שולחים דוא"ל. כל הודעות המס הרשמיות נשלחות בדואר רגיל.



המתקשר מעמיד פנים שהוא תומך של Microsoft ומסביר שהמחשב שלך נגוע. ברגע שהם משכנעים אותך שהמחשב נגוע, הם לוחצים עליך לקנות את התוכנה שלהם או לתת להם גישה מרחוק למחשב. מיקרוסופט לא תתקשר אליך.



אתה מקבל הודעת דואר קולי אוטומטית שחשבון הבנק שלך בוטל, ושאתה צריך להתקשר למספר חזרה כדי להפעיל אותו מחדש. כאשר אתה מתקשר, אתה מקבל מערכת אוטומטית המבקשת ממך לאשר את הזהות שלך ושואלת אותך על מיני שאלות פרטיות. זה לא באמת הבנק שלך, הם פשוט מקליטים את כל המידע שלך עבור הונאת זהות.



## הגן על עצמך

ההגנה הטובה ביותר שיש לך נגד התקפות טלפון היא אתה בעצמך. זכור את הדברים הבאים:

בכל פעם שמישהו מתקשר אליך ויוצר תחושה אדירה של דחיפות, לוחץ עליך לעשות משהו, הייה חשדן. גם אם שיחת הטלפון נראית בסדר בהתחלה, אבל אז מתחילה להרגיש מוזר, אתה יכול לעצור ולומר "לא" בכל עת.



אם אתה סבור ששיחת טלפון היא התקפה, פשוט נתק. אם ברצונך לאשר אם שיחת הטלפון הייתה חוקית, עבור אל אתר האינטרנט של הארגון (כגון הבנק שלך) וקבל את מספר הטלפון של תמיכת הלקוחות והתקשר אליהם בעצמך ישירות. ככה אתה באמת יודע שאתה מדבר עם הארגון האמיתי.



אף פעם אל תסמוך על שיחה מזהה, הרעים לעיתים קרובות מזייפים את מספר המתקשר, כך שזה נראה כאילו הוא מגיע מארגון לגיטימי או ממספר באותו אזור חיוג כמו מספר הטלפון שלך.



לעולם אל תאפשר למתקשר לבצע השתלטות על המחשב שלך או לגרום לך להוריד תוכנות. כך הרעים יכולים להדביק את המחשב שלך.



אם שיחת טלפון מגיעה ממישהו שאינך מכיר באופן אישי, אפשר לשיחה לעבור ישירות לתא הקולי. בדרך זו תוכל לסקור שיחות לא ידועות בזמן שלך. אפשרות נוספת, בטלפונים רבים אתה יכול לאפשר זאת כברירת מחדל עם התכונה "לא להפריע".



הונאות והתקפות בטלפון נמצאות במגמת עלייה. אמצעי ההגנה היעיל ביותר בגילוי ועצירת ההתקפה, הוא אתה.



## עורכת אורחת

ג'ן פוקס מספקת מודעות אבטחה, הנדסה חברתית, שירותי הערכת סיכונים כיועצת אבטחה בכירה ב-All Covered. מצא את ג'ן בטוויטר כ-@j\_fox.

## מקורות

<https://www.consumer.ftc.gov/topics/privacy-identity-online-security>

<https://www.ftccomplaintassistant.gov/#crnt>

<https://www.sans.org/u/Fi5>

מידע צרכני על זהות, פרטיות ואבטחה מקוונת:

דווח על הונאת טלפון (בארה"ב):

הנדסה חברתית:

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Security Awareness, 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 [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter). עורכי המערכת: וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי | תורגם על ידי: גדי מרגלית ודרור ענבר