



עלון המודעות החודשי לביטחון עבורך

לעורר רגשות - איך תוקפי סייבר מרמים אותך

סקירה כללית

תוקפי סייבר מחדשים כל הזמן את הדרכים לגרום לנו לעשות דברים שאסור לנו לעשות, כמו לחיצה על קישורים זדוניים, פתיחת קבצים נגועים המצורפים לדוא"ל, רכישת כרטיסי מתנה או ויתור על הסיסמאות שלנו. בנוסף, לעתים קרובות הם משתמשים בטכנולוגיות או פלטפורמות שונות כדי לנסות להערים עלינו, כגון דואר אלקטרוני, שיחות טלפון, הודעות טקסט או מדיה חברתית. למרות שכל זה עשוי להיראות מרשים, רוב ההתקפות הללו חולקות את אותו הדבר: רגש. על ידי הכרת טריגרים רגשיים שבהם משתמשים תוקפי סייבר, לעתים קרובות אתה יכול לזהות את ההתקפות שלהם, לא משנה באיזו שיטה הם משתמשים.

הכל עניין של רגשות

הכל מתחיל ברגשות. אנחנו, בני אדם אנושיים, לעתים קרובות מדי מקבלים החלטות על סמך רגשות במקום עובדות. יש למעשה, תחום מחקר שלם על המושג הזה שנקרא "כלכלה התנהגותית", בהובלת חוקרים כמו דניאל כהנמן, ריצ'רד תאלר וקאס סונשטיין. למזלנו, אם אנחנו יודעים את הטריגרים הרגשיים שיש לחפש, נוכל להצליח לזהות ולעצור את רוב ההתקפות. להלן הטריגרים הרגשיים הנפוצים ביותר שרצוי להיזהר מהם. לפעמים תוקפי סייבר ישתמשו בשילוב של רגשות השונים באותו דוא"ל, הודעת טקסט, פוסט במדיה חברתית או שיחת טלפון - מה שהופך אותו להרבה יותר יעיל.

דחיפות: דחיפות היא אחד הטריגרים הרגשיים הנפוצים ביותר, מכיוון שהיא כל כך יעילה. תוקפי סייבר ישתמשו לעתים קרובות בפחד, חרדה, מחסור או הפחדה כדי לגרום לך לעשות טעות. לדוגמה, מייל דחוף מהמנהל שלך שדורש לשלוח לו מסמכים רגישים באופן דחוף, במציאות מדובר בתוקף סייבר שמתחזה למנהל שלך. או שאולי אתה מקבל הודעת טקסט מתוקף סייבר שמתחזה למשטרת ישראל המודיעה לך שתשלום הקנס שלך מאחר ואתה צריך לשלם עכשיו.

נעם: אתה מקבל הודעה על נושא פוליטי, סביבתי או חברתי שאתה מאוד נלהב לגביו - משהו כמו "לא תאמין מה הקבוצה הפוליטית או החברה התאגידית הזו עושים!"

סקרנות/הפתעה: לפעמים ההתקפות הכי מוצלחות נאמרות בלשון המעטה. הסקרנות משולבת בהפתעה; אנחנו רוצים ללמוד יותר. זו תגובה למשהו לא צפוי. לדוגמה, תוקף סייבר שולח לך הודעה שחבילה לא נמסרה ולחץ על קישור למידע נוסף, למרות שלא הזמנת שום דבר באינטרנט. אנחנו מתפתים ללמוד עוד! למרבה הצער, אין חבילה, רק כוונת דון בצד השני של הקישור הזה.

אמון: תוקפים משתמשים בשם או במותג שאתה סומך עליהם כדי לשכנע אותך לנקוט בפעולה. לדוגמה, הודעה המתחזה לבנק שלך, ארגון צדקה ידוע, ארגון ממשלתי מהימן, או אפילו מאדם שאתה מכיר. גם אם דוא"ל או הודעת טקסט משתמשים בלוגו ובשם של ארגון שאתה מכיר, לא אומר שההודעה באמת הגיעה מהם.

התרגשות: אתה מקבל הודעת טקסט מהבנק או מספק שירות שמודה לך על ביצוע התשלום בזמן. הודעת הטקסט מספקת קישור שבו אתה יכול לתבוע פרס - אייפד חדש, כמה מרגש! הקישור מוביל אותך לאתר שנראה רשמי, האתר מבקש את כל המידע האישי שלך ואומר שאתה צריך לספק פרטי כרטיס אשראי כדי לכסות עלויות משלוח או עלויות טיפול. זהו תוקף סייבר שפשוט גונב את הכסף שלך או את זהותך.

אמפתיה / חמלה: תוקפי סייבר מנצלים את הרצון הטוב שלך. לדוגמה, לאחר שיופיע אסון בחדשות, הם ישלחו מיליוני מיילים מזויפים המתחזות לארגון צדקה המשרת את הקורבנות ויבקשו ממך כסף.

על ידי הבנה טובה יותר של הפעלת רגשות, תהיו מוכנים הרבה יותר לזהות ולעצור את תוקפי הסייבר, ללא קשר לפיתוי, לטכנולוגיה או לפלטפורמה שבה הם משתמשים.

עורכת אורחת



My-Ngoc Nguyen היא המנכ"לית והמנהלת של פתרונות IT מאובטחים. עם 20 שנות ניסיון, יש לה ניסיון עמוק בניהול והבשלה של תוכניות אבטחת סייבר וניהול סיכונים הן לממשל הפדרלי והן למגזר הפרטי. היא מביאה את הניסיון הזה כמדריכה מוסמכת המלמדת באופן קבוע את הקורס MGT512.

<https://www.linkedin.com/in/menop>, [My-Ngoc Nguyen | SANS Institute](#), [@MenopN](#).

משאבים

התקפות הנדסה חברתית:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt813804c438f88f2c/6048fee92d310e5a62e19801/OUCH! No v 2020 - Social Engineering v.3-Hebrew.pdf>

הונאה טלפונית-התקפות טלפונית והונאות:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt32936c28fc3bf62b/60902a943aa0431020f5ee58/OUCH-Hebrew May 2021 - Vishing Phone Call Attacks and Scams v3-English.pdf>

שלושת ההונאות המובילות במדיה החברתית:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt84e4f3e3a4fb0800/62471216180ea87eed675d04/ouch! april 2022 hebrew top three social media scams.pdf>

איתור והפסקת התקפות הודעות:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt24bdb234479f71f9/61d249780d81d913d2ac6dff/ouch! january 2022 Hebrew spot and stop messaging attacks.pdf>

התקפות יוגנטשות מורכבות יותר:

<https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blte49d1db1102b1ee0/62b344448e531c5737f7ec81/ouch! july 2022 hebrew phishing attacks are getting trickier.pdf>

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר

OUCH! פורסם על ידי SANS Security Awareness ומופץ תחת רישיון Creative Commons BY-NC-ND 4.0. אתם חופשיים לשתף או להפיץ ביולטר זה כל עוד אתה לא מוכר או משנה אותו. ועדת מערכת: וולטר סקריינס, פיל הופמן, אלן וואגנר, לסלי רידאוט, פרינסס יאנג.