SANS SECURITY AWARENESS

OUCH!

עלון מודעות אבטחת מידע למשתמשי מחשב

לעצור את הדייג

סקירה כללית

שירותי דואר אלקטרוני ושליחת הודעות (כגון סקייפ, טוויטר או סנאפצ'ט) הם אחת הדרכים העיקריות שאנו מתקשרים כיום. אנחנו משתמשים בטכנולוגיות אלו בתדירות יומיומית ולא רק לצרכי עבודה, אלא גם כדי לשמור על קשר עם חברים ובני משפחה. מכיוון שכל כך הרבה אנשים ברחבי העולם, תלויים בטכנולוגיות אלו, הן הפכו לאחת מיעדי ההתקפה העיקרים המ־שמשים את התוקפים הקיברנטים, שיטת התקפה בשם דיוג (phishing). נלמד מה זה דיוג, ואיך אתה יכול לזהות ולהפסיק את ההתקפות האלו, ללא קשר אם אתה בעבודה או בבית.

מה זה דיוג?

דיוג הוא סוג של התקפה המשתמשת בדוא"ל או בשירות העברת הודעות כדי לגרום לך לנקוט פעולה שאינך צריך לנקוט, כגון לחיצה על קישור זדוני, שיתוף הסיסמה או פתיחת קובץ נגוע אשר מצורף לדוא"ל. התוקפים מתאמצים להפוך את המסרים שהם שולחים למשכנעים ולגרות את המניעים הרגשיים שלך, כגון דחיפות או סקרנות. הם יכולים לגרום להודעה להיראות כאילו זה בא ממישהו שאתה מכיר, כגון חבר או חברה שאתם מתכתבים לעיתים קרובות. הם אפילו יכולים להוסיף לוגו של הבנק שלך או לזייף את כתובת הדוא"ל כך שההודעה נראית לגיטימית יותר. התוקפים שולחים הודעות כאלו למיליוני אנשים. התוקפים לא יודעים מי ייתפס בפיתיון, התוקפים יודעים שככל שהם שולחים יותר הודעות, יותר אנשים יפלו קורבן.

הגן על עצמך

כמעט בכל המקרים, פתיחה וקריאה של הודעת דוא"ל או הודעת טקסט היא בסדר. כדי שהתקפת דיוג תעבוד הרעים צריכים להערים עליך לעשות משהו. למרבה המזל יש רמזים כי הודעת דיוג היא אכן התקפה, הנה הנפוצים ביותר אלה:

- תחושה אדירה של דחיפות, הדורשת "פעולה מיידית" לפני שמשהו רע יקרה, כמו איום לסגור חשבון או לשלוח אותך לכלא. התוקף רוצה להאיץ בך לעשות טעות.
- לנסות להלחיץ אותך לעקוף או להתעלם מהמדיניות או מהנהלים בעבודה.
- תחושה גוברת של סקרנות או משהו שהוא טוב מכדי להיות אמיתי (לא, אתה לא זכית בהגרלה).

- הודעה שלא מופנית אלייך בשם, למשל "לקוח יקר". רוב המכרים יצרו איתך קשר בשמך.
- בקשת מידע רגיש במיוחד, כגון מספר כרטיס האשראי או הסיסמה שלך או כל מידע אחר שהשולח הלגיטימי כבר מכיר.
- ההודעה אומרת שהיא מגיעה מארגון רשמי, אך יש בה דקדוק או איות לקויי או שהשולח משתמש בכתובת דוא"ל אישית כגון @ gmail.com.
- ההודעה מגיעה מהודעת דוא"ל רשמית (כגון הבוס שלך), אך יש לה כתובת 'מענה' אל חשבון האימייל האישי של מישהו אחר.
- אתה מקבל הודעה ממישהו שאתה מכיר, אבל הטון או הניסוח פשוט לא מסתדר. אם אתה חושד, התקשר לשולח כדי לוודא שהוא אכן השולח. לתוקף סייבר קל ליצור הודעה שנראית כאילו נשלחה מחבר או עמית לעבודה.

בסופו של דבר השכל הישר הוא ההגנה הטובה ביותר. אם הודעת אימייל או הודעה טקסט נראית מוזרה, חשודה או טובה מכדי להיות אמיתית, ייתכן שהיא מהווה מתקפת דיוג.

עורכת אורחת

טוניה דודלי מפתחת ומפעילה תוכניות מודעות לאבטחה מאז 2011, כולל תוכנית לאימון מפני דיוג שזכתה בפרסים. ניתן למצוא אותה בכתובת www.linkedin.com/in/toniadudley.

מקורות

הנדסה חברתית:	https://www.sans.org/u/Cb1
סיוע לאחרים לאבטח את עצמם:	https://www.sans.org/u/Cb6
דואר אלקטרוני, עשה ואל תעשה:	https://www.sans.org/u/Cbg
הונאת המנכ"ל:	https://www.sans.org/u/Cbl
אאוץ! תרגומים וארכיונים:	https://www.sans.org/u/Cbq

רישיון