אאוץ! | ספטמבר 2019

הונאות דרך מדיה חברתית

סקירה כללית

רבים מאיתנו קיבלו התקפות בצורת דוא"ל מתחזה, בעבודה או בבית. אלו מיילים שנראים לגיטימיים, למשל מהבנק, הבוס שלך או החנות המקוונת המועדפת עליך. עם זאת, מדובר בהתקפה, בניסיון להאיץ בך או לגרום לך לבצע פעולה שאסור לך לנקוט, כמו פתיחת קובץ מצורף נגוע, שיתוף סיסמתך או העברת כסף. האתגר הוא ככל שאנו משתפרים באיתור ועצירת התקפות הדוא"ל הללו, כך גם פושעי הסייבר מנסים דרכים אחרות ליצור קשר והונות אנשים.

ניסיונות להונאה או ניסיונות לרמות אותך יכולות לקרות כמעט בכל צורה של תקשורת שבה אתה משתמש, החל מוואטסאפ, סקייפ, טוויטר, אינסטגרם, פייסבוק או אפילו אפליקציות משחק. תקשורת בפלטפורמות או בערוצים אלו יכולה להרגיש אמינה או לא פורמאלית, וזו בדיוק הסיבה שהתוקפים משתמשים בפלטפורמות אלו כדי להטעות אחרים. בנוסף, עם הטכנולוגיות של ימינו זה הפך להרבה יותר קל לכל תוקף בכל מקום בעולם להעמיד פנים שהוא כל דבר או כל מי שהם רוצים. חשוב לזכור כי כל תקשורת שעוברת דרכם עשויה שלא להיות כפי שהיא נראית ושאנשים הם לא תמיד כפי שהם נראים.

נקודות מפתח

להלן הרמזים הנפוצים ביותר שההודעה שקיבלת זה עתה או הפוסט שקראת זה עתה עשוי להיות התקפה.

דחיפות: הודעה שיש לה תחושת דחיפות הדורשת "פעולה מיידית" לפני שקורה משהו רע, כמו לאיים על סגירת חשבון או לשלוח אותך לכלא. התוקף רוצה להאיץ אותך לבצע טעות.

לחץ: לחץ עלייך לעקוף או להתעלם ממדיניות או נהלים בעבודה.

סקרנות: תחושה חזקה של סקרנות או משהו שטוב מכדי להיות אמיתי. לא, לא זכית בלוטו.

רגיש: בקשה למידע רגיש במיוחד, כגון מספר כרטיס האשראי או הסיסמה שלך, או כל מידע שבאמת לא נוח לך לשתף.

הודעות רשמיות: ההודעה אומרת שהיא מגיעה מארגון רשמי, אך יש לה דקדוק לא נכון או שגיאות כתיב. רוב הארגונים הממשלתיים לא ישתמשו במדיה חברתית לצורך תקשורת רשמית ישירות אתכם. אם אינכם בטוחים אם ההודעה לגיטימית, התקשרו לארגון אך השתמשו במספר טלפון מהימן, למשל מספר הטלפון מאתר האינטרנט שלהם.

התחזות: אתה מקבל הודעה מחבר או עמית לעבודה, אך הטון או הניסוח פשוט לא נשמעים לך. אם אתה חושד, התקשר לשולח בטלפון כדי לוודא שהוא שלח את ההודעה. קל לתוקף סייבר ליצור הודעות שנראות כמו מישהו שאתה מכיר. במקרים מסוימים הם יכולים להשתלט על אחד החשבונות של החבר שלך, ואז להעמיד פנים שהוא החבר שלך ולפנות אליך. שימו לב במיוחד להודעות טקסט, וואטסאפ או כל לפורמט של הודעות קצרות אחרות, שקשה יותר להבין את אישיותו של השולח.

אתה ההגנה הטובה ביותר מפני הונאות והתקפות כאלו. אם פוסט או הודעה נראים מוזרים או חשודים, פשוט התעלם או מחק אותם. אם זה ממישהו שאתה מכיר באופן אישי, התקשר לאדם בטלפון כדי לאשר אם הוא באמת שלח את הודעה.

עורך אורח

ד"ר ג'סיקה בארקר (@drjessicabarker) מובילה את הצד האנושי של אבטחת המידע. היא משמשת כמנכ"לית משותפת של חברת Cygenta, שם היא עוקבת אחר תשוקתה להשפיע באופן חיובי על מודעות, התנהגויות ותרבות ברשת. היא יו"ר של מועדון בשם ClubCISO ודוברת מפתח פופולרית.

מקורות

הנדסה חברתית: https://www.sans.org/u/Uz6
הונאות שיחות טלפון: https://www.sans.org/u/Uzb
עצור את הדיוג הזה: https://www.sans.org/u/Uzg
הונאה בהתאמה אישית: https://www.sans.org/u/Uzl