הנדסה חברתית

הנדסה חברתית היא שיטה שבה תוקפים מנצלים תכונות פסיכולוגיות של אנשים כדי לגרום להם לחשוף מידע רגיש או לבצע פעולות מסוימות. התוקפים משתמשים בשיטות כמו התחזות, שכנוע והונאה כדי להשיג את מטרותיהם.

הנה מספר שיטות נפוצות ומוכרות:

פישינג

"פישינג" (דיוג) הוא ניסיון לגניבת מידע רגיש על ידי התחזות לגורם לגיטימי ברשת. תוקפים שולחים הודעות אימייל עם קישורים מזויפים/זדוניים, שמובילים את הקורבן להזין פרטים אישיים או להוריד נוזקות. לעתים, לחיצה על הקישור בלבד מספיקה לתקיפת המכשיר ועלולה להוביל לדלף מידע אישי וארגוני.

כיצד להימנע ולהישמר?

- המנעו מלחיצה על קישורים ממקורות לא מוכרים/רשמיים.
- גלו ערנות לבקשת מידע אישי, פיננסי, או עסקי - ביטחוני בהקשרי אלביט.
- בדקו שגיאות כתיב ושגיאות הקשר, חשדו בהודעות הכתובות בטון דחוף, תקיף או מאיים.
- פנו ישירות לשולח ההודעה אם השיחה חסרת הקשר הגיוני.
- אל תגיבו להודעות חשודות, חסמו את המספר ממנו התקבלה ההודעה ודווחו לאגף הביטחון.

סמישינג

"סמישינג" הוא "פישינג" דרך SMS שבו התוקף מנסה לגרום לקורבן להוריד נזקה או לחשוף מידע אישי. בשנה האחרונה התקיימו מספר תרגילי סמישינג לעובדי החברה, על מנת להעלות את המודעות לסיכונים ודרכי המניעה ממתקפה מסוג סמישינג, אשר עלולה להוביל לדלף מידע אישי, עסקי וביטחוני ופגיעה ברשת הארגונית.

כיצד להימנע ולהישמר?

אז...כמו ב"פישינג" ובנוסף:

- הימנעו מלחיצה על קישורים בהודעות טקסט, במיוחד אם נשלחו ממי שאינכם מכירים.
- אין להתקשר למספר הטלפון ממנו נשלחה הודעת הטקסט או למספר הטלפון שמצוין בהודעה.
- אם יש ספק, בררו מול מספר טלפון / אתר רשמי של בית העסק שיצר איתכם קשר על מנת לאמת את לגיטימיות ההודעה.

וישינג

"וישינג" (Voice Phishing) הוא "פישינג" קולי דרך שיחות טלפון, שבהן התוקפים מתחזים לגורמים עסקיים לגיטימיים כמו נציג מהבנק, נציג חברת כרטיסי אשראי או עירייה כדי לדלות מידע.

כיצד להימנע ולהישמר?

- הימנעו ממסירת מידע אישי למתקשרים לא מזוהים.
- חשדו אם המתקשר מבקש מידע שכבר אמור להיות ידוע לו.
- היו ערניים, התוקף עלול להשתמש בטקטיקות הפחדה או שכנוע כדי לשכנע אתכם למסור מידע או לפעול ללא מחשבה.
- אם יש ספק בשיחה, נתקו אותה, חסמו את מספר הטלפון ודווחו למוקד הסייבר.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC