מהי התקפת הנדסה חברתית?

הנדסה חברתית (Social Engineering) הוא מונח מתחום אבטחת המידע ואחת מהטכניקות למימוש לוחמת סייבר. משמעותו הוא ניצולן של תכונות פסיכולוגיות אנושיות, לטובת הונאה, שכנוע והתחזות ,המביאות את האדם לציית מרצון לבקשת התוקף ולמסור לידיו מידע אישי פרטי או על ארגון, מוסד או מערכות מחשב הקשורות, באמצעותו יממש את זממו ויפגע בקורבן כלכלית ,תדמיתית, פרודוקטיבית, לתועלת אישית וכו׳

הנדסה חברתית אינה מוגבלת למפגש פנים אל פנים. היא יכולה להתבצע באמצעות טכנולוגיות מגוונות .לדוגמה, בשיחת טלפון, בדואר אלקטרוני, סמס, פייסבוק, טוויטר, צ׳אט או שיחה מקוונת. לעיתים התוקף אף יכול לשלב מהלך כפול ,כלומר, ראשית ישלח לקורבן דואר אלקטרוני, ולאחריו ישלח הודעת סמס שתעצים בקורבן את תחושת אמינות, או לדוגמה ,בעת ביקור בשרות בנקאי מקוון ישלח התוקף דואר אלקטרוני המתחזה לשירות הבנקאי המבקש את עדכון הפרטים האישיים.

תוקף העושה שימוש בהנדסה חברתית עשוי להראות או להישמע צנוע ומכובד. הוא לא יעורר חשד ,ויתכן אף ויקרין קסם אישי כך שיעורר באדם העומד מולו אמפטיה ורצון לעזור .
בדרך להשגת מטרתו עשוי התוקף להתחזות לכל דמות שתשרת את מטרתו. לדוגמה, עובד חדש, טכנאי המגיע לביקור, מנהל בכיר, שליח ועוד. הוא אפילו עשוי להציג אישורים או תעודות התומכים בזהותו הבדויה, כל זאת כדי לאפשר לו להציג שאלות שיאפשרו לו לאסוף מספיק מידע כדי לחדור לרשת הארגון או להשיג את רצונו מן הקורבן התמים.
תוקף הממוקד במטרתו לא ישקוט. במידה ולא הצליח לאסוף מספיק מידע מהמקור הראשון, ישתמש בפיסות המידע שאסף להגברת אמינותו, ויפנה למקור אחר בארגון וכך הלאה עד להשגת מבוקשו.

כיצד להיזהר ולהימנע ממתקפות הנדסה חברתית?

- העצה הטובה ביותר היא להפעיל הגיון בריא. להיות מודעים ואף מעט חשדניים, אם משהו נראה חשוד ,יש סיכוי סביר שהוא אכן חשוד!
- אל תמסרו לאדם מידע שמלכתחילה לא אמורה להיות לו גישה אליו, או שהוא היה אמור כבר לדעת אותו.
- היזהרו מגורם לא מוכר המנסה לטעת בכם תחושה של דחיפות גדולה .
- אל תיבהלו מניסיונות להלחיץ באמצעות סנקציה או מועד אחרון.

- אל תמסרו לעולם פרטים מזהים בטלפון לרבות סיסמאות גישה גם לאנשים המזדהים כאנשי התמיכה של הארגון עצרו וחישבו לפני מסירת מידע!
- חשדו בהפתעות שהן טובות מדי מכדי להיות אמיתיות .הרי אין הגיון כלל בהודעה כי זכיתם בהגרלת הלוטו אם מעולם לא השתתפתם בהגרלה.

- הישמרו מהודעות דואר אלקטרוני ממקור חדש או לא מזוהה – אם לא ציפיתם להודעה, אל תפתחו בשום אופן! אל תקליקו על קישורים – בהודעות שהגיעו ממקור לא ידוע והימנעו מהורדה או שמירה של קבצים המצורפים להודעות חשודות. להרחבה בנושא ראו התגוננות מתרמיות במייל .
- שימרו על פרטיכם האישיים ברשתות החברתיות. חישבו היטב טרם שאתם משתפים אחד את השני בכל דבר אפשרי. השימוש ברשתות החברתיות הפך שכיח ביותר, והן הפכו בסיס עיקרי למתקפות דיוג והנדסה חברתית. היו מודעים לסכנה הטמונה בחשיפת מידע ברשתות החברתיות. הגנו על המידע האישי שלכם ואל תחשפו אותו בחופשיות .דוגמה פשוטה להנדסה חברתית שנפוצה ברשת הפייסבוק, היא קישור לאפליקציה "מי צפה בפרופיל שלי" שמשכה משתמשים רבים להתקין אותה וכך להיפגע מתוכנה זדונית.

<u>מה לעשות במידה ונפלתם יעד למתקפת הנדסה חברתית?</u>

- במידה והנכם חוששים כי נפלתם יעד לתקיפה, מהרו לדווח על האירוע למהנדס המיחשוב היחידתי או לממונה אבטחת המידע בטכניון CISO@technion.ac.il.
- גם אם נפלתם קורבן או עלה בלבכם החשש שהותקפתם, כאנשים פרטיים או כעובדי ארגון, מהרו והחליפו את כל סיסמאותיכם. הקפידו להשתמש בסיסמה שונה לכל שירות וחשבון. צרו והשתמשו בסיסמאות ארוכות ומורכבות. סיסמה מורכבת חייבת להכיל אותיות גדולות וקטנות, ספרות ותווים מיוחדים.
- היו ערים לכל שינוי חריג בחשבונותיכם ובשירותים המקוונים בהם אתם נעזרים ,עקבו באופן מדוקדק אחר דפי הפרוט שהנכם מקבלים משירותים בנקאים כך תגלו בזמן הונאה במידה והתרחשה.

קישורים

<u>הנדסה חברתית – Securing the human</u>

<u>ויקיפדיה – הנדסה חברתית</u>

<u>לפרוץ למוח האנושי: הסיכון הגדול ביותר לאבטחת מידע הוא הנדסה חברתית - GeekTime</u>

<u>מי צפה בפרופיל שלי – משטרת ישראל - פייסבוק</u>