

אבטחת מידע

מושגי חובה

1. **טביעת רגל דיגיטלית (Digital Footprint)** מכלול הנתונים והעקבות שאנו משאירים אחרינו בכל פעילות ברשת האינטרנט. טביעה זו כוללת אתרים שבהם גלשנו, פוסטים ותמונות שהעלינו, קניות אונליין ופרטים מזהים שהזנו. מידע זה נשמר אצל ספקי אינטרנט וחברות טכנולוגיה ולעיתים אף נמכר לגורמים שלישיים. תוקפים וגורמים עוינים עלולים לנצל מידע זה כדי לאסוף עלינו פרטים ולפגוע בפרטיותנו.
2. **דיוג / פשינג (Phishing)** שיטת הונאה נפוצה שנועדה להוציא במרמה מידע רגיש ואישי ממשתמשים ברשת. המטרות המרכזיות הן גניבת שמות משתמש, סיסמאות, פרטי כרטיסי אשראי ומספרי תעודת זהות. הפשינג מבוצע באמצעות הודעות מזויפות או קישורים זדוניים שנראים לגיטימיים לחלוטין. ברגע שהמשתמש לוחץ על הקישור ומזין פרטים, המידע עובר באופן מיידי לידי התוקפים.
3. **משינג (Smishing)** הונאת דיוג (פשינג) המבוצעת באופן ספציפי דרך הודעות טקסט קצרות (SMS) או אפליקציות מסרים. תוקפים שולחים הודעות המדמות פניות מגופים מוכרים כמו דואר, בנקים או חברות אשראי. ההודעות מכילות לרוב אלמנט של לחץ או דחיפות ומזמינות את המקבל ללחוץ על קישור מזויף. לחיצה על הקישור עלולה להוביל לגניבת מידע פיננסי או להורדת קבצים מזיקים.
4. **וישינג / דיוג קולי (Vishing)** סוג של פשינג המתרחש באמצעות שיחת טלפון קולית (Voice Phishing). במסגרת שיחה זו התוקף מתחזה לנציג רשמי של בנק, חברה מסחרית או גוף ממשלתי. המתחזה מנסה לרכוש את אמון הקורבן כדי לחלץ ממנו בעזרת קודים סודיים, סיסמאות או פרטי אשראי. הקורבן עלול למסור את המידע מתוך מחשבה שהוא מדבר עם נציג שירות לגיטימי.
5. **הנדסה חברתית (Social Engineering)** טכניקה המנצלת את התנהגות האדם, תמימותו או רגשותיו כדי לגרום לו לבצע פעולות מזיקות. השיטה אינה מסתמכת על פריצה טכנולוגית אלא על מניפולציה פסיכולוגית ישירה על הקורבן. התוקפים משתמשים ביצירת תחושת דחיפות, פחד, סקרנות או פיתוי כספי כדי להשיג גישה למידע. זהו הגורם האנושי שנחשב לנקודת התורפה המרכזית באבטחת מידע וסייבר.
6. **כופרה (Ransomware)** סוג של תוכנה זדונית (נוזקה) שמטרתה העיקרית היא לסחוט כסף מקורבנות ברשת. לאחר חדירתה למחשב או לטלפון, התוכנה מצפינה את הקבצים או נועלת את המכשיר לחלוטין. התוקפים דורשים מהקורבן תשלום דמי כופר כספיים בתמורה לשחרור הגישה לקבצים או פתיחת הנעילה. ברוב המקרים, גם לאחר תשלום הכופר אין ערובה לכך שהמידע אכן יוחזר.

7. **אימות דו-שלבי (Two-Factor Authentication / 2FA)** מנגנון אבטחה מתקדם המוסיף שכבת הגנה נוספת לחשבונות הדיגיטליים מעבר לסיסמה הרגילה. בעת ההתחברות, המערכת דורשת זיהוי נוסף כמו קוד חד-פעמי שנשלח ב-SMS או באפליקציית ייעודית. כתוצאה מכך, גם אם גורם זר השיג את הסיסמה שלך, הוא לא יוכל להיכנס לחשבון. שימוש באימות זה מומלץ מאוד בכל האפליקציות, הרשתות החברתיות וחשבונות הבנק.
8. **עוגיות (Cookies)** קבצי טקסט קטנים שהאתרים שבהם אנחנו גולשים שומרים על גבי הדפדפן או המכשיר שלנו. הקבצים הללו משמשים לתיעוד העדפות הגלישה, שמירת מוצרים בסל הקניות וזיהוי המשתמש. עם זאת, עוגיות עלולות לשמש למעקב מקיף אחר ההתנהגות הדיגיטלית של המשתמש ברשת. אישור גורף של עוגיות באתרים לא מוכרים עלול לסכן את הפרטיות ולשתף מידע רגיש.
9. **פרוטוקול HTTPS** פרוטוקול תקשורת מאובטח להעברת נתונים בין הדפדפן של המשתמש לבין אתר האינטרנט. האות S מייצגת את המילה Secure (מאובטח) ומעידה כי המידע שעובר באתר מוצפן. גלישה באתר בעל כתובת HTTPS מונעת מצד שלישי לצפות בפרטים רגשים כגון סיסמאות ואשראי. בעת ביצוע קניות או הזנת מידע פיננסי, מומלץ לוודא שהפרוטוקול פעיל וסמל המנעול מופיע.
10. **מנהל סיסמאות (Password Manager)** תוכנה או אפליקציה מאובטחת המיועדת לאחסון, ניהול ויצירה של סיסמאות חזקות ושונות. מנהל הסיסמאות שומר את כל נתוני ההתחברות בצורה מוצפנת תחת סיסמת ראשי אחת ויחידה. כלי זה מונע את הצורך לזכור עשרות סיסמאות מורכבות או להשתמש בסיסמה קבועה וחלשה. השימוש בתוכנה זו נחשב לדרך המומלצת והמאובטחת ביותר לשמירה על החשבונות ברשת.
11. **הרשאות אפליקציה (App Permissions)** אישורים שהמשתמש מעניק לאפליקציה שהתקין כדי לגשת לרכיבים שונים במכשיר הנייד. הרשאות אלו יכולות לכלול גישה למיקרופון, למצלמה, לאנשי הקשר, לגלריית התמונות ולמיקום. חשוב לבחון כל בקשת הרשאה ולהעניק גישה רק לרכיבים שהאפליקציה באמת זקוקה להם. מתן הרשאות מיותרות לאפליקציות לא מוכרות עלול להוביל לזליגת מידע אישי ופגיעה בפרטיות.
12. **דיפ פייק (Deepfake)** טכנולוגיה המבוססת על בינה מלאכותית ליצירת סרטונים, תמונות או הקלטות קול מזויפות בלתי ניתנות להבחנה. התוקפים משתמשים בדיפ פייק כדי לחקות דמויות מוכרות, חברים או בני משפחה לצורך הונאה. באמצעות זיוף הקול והפנים, הפורצים מנסים לשכנע את הקורבן להעביר כספים או למסור מידע. טכנולוגיה זו מדגישה את הצורך באימות זהות ישיר ולא להסתמך רק על תוכן ויזואלי.
13. **כרטיס אשראי נטען (Prepaid Credit Card)** כרטיס תשלום המוטען מראש בסכום כסף מוגדר ואינו מקושר באופן ישיר לחשבון הבנק. כרטיס זה משמש ככלי בטוח לביצוע קניות באינטרנט, במיוחד באתרים חדשים או לא מוכרים. במידה ופרטי הכרטיס נחשפים או נגנבים, הנזק הכספי מוגבל אך ורק לסכום המוטען בו. מדובר בפתרון יעיל לצמצום סיכונים פיננסיים ומניעת תשלומים בלתי מורשים ברשת.
14. **מערך הסייבר הלאומי (מוקד 119)** גוף ממשלתי בישראל המופקד על הגנת המרחב האזרחי מפני איומי סייבר והונאות ברשת. המערך מפעיל את מוקד הדיווח 119 הזמין לציבור הרחב לאורך כל

שעות היממה. אזרחים שנתקלו באירוע סייבר, פריצה או הונאה פיננסית יכולים לפנות לקבלת סיוע והנחיות. דיווח מהיר למוקד מסייע לצמצם את הנזק האישי ולמנוע מפקטורים נוספים ליפול בקורבן.

15. **פלטפורמת תשלום מקוונת (Online Payment Platform)** שירות דיגיטלי (כדוגמת PayPal, Apple Pay, Google Pay) המאפשר ביצוע תשלומים מבלי לחשוף אשראי. הפלטפורמה מקשרת בין הקונה למוכר ומבצעת את העברת הכספים בצורה מאובטחת ומוצפנת. שירותים אלו מציעים לרוב הגנת קונה המאפשרת לקבל החזר כספי במקרה של הונאה. שימוש בפלטפורמות אלו מהווה חלופה בטוחה בהרבה ממסירת פרטי כרטיס אשראי ישירות לאתר.