לזהות את הסימנים ולגלוש בטוח:
10 סימני אזהרה להודעת דוא"ל או מסרון "פישינג" ואיך להתמודד

מתקפת פישינג, או בעברית דיוג, היא ניסיון לגניבת מידע ממשתמשים באמצעות התחזות תוך השפעה על המשתמש להכניס פרטים אישיים כגון סיסמה, תעודת זהות, מספר כרטיס אשראי, קוד וכו'. בתקופה האחרונה נסיונות אלו מתרבים ונעשים מתוחכמים יותר. בעוד חלק מהקישורים המופצים בדוא"ל או במסרון הם לגיטימיים, חשוב להיות מודעים לאפשרות שמדובר בניסיון דיוג. לרגל שבוע הסייבר, חיבר מערך הסייבר הלאומי מדריך לעשרה סימנים פשוטים שבאמצעותם ניתן לזהות את רוב ניסיונות הדיוג ולהימנע מהכנסת הפרטים או מהקלקה על הקישור. זיכרו - אל תלחצו, שלא תילחצו.

1. **כתובת השולח** - ארגונים רשמיים שולחים הודעות מכתובות לגיטימיות של הארגון ולרוב לא מכתובת גימייל למשל. כמו כן, צריכה להיות התאמה בין שם השולח לכתובת השולח.
2. **יצירת לחץ ותחושת דחיפות** - בקשה לביצוע פעולות מידיות מתוך "דחיפות", היא טכניקה נפוצה שנועדה לגרום לאנשים לפעול מלחץ ולהטעות אותם.
3. **היעדר פניה אישית** - לרוב, ארגונים רשמיים משתמשים בשם הפרטי של הלקוח ופונים אליו באופן אישי. פנייה כללית של "לקוח יקר", עשויה להוות סימן מחשיד.
4. **נוסח חובבני**- שגיאות כתיב וניסוח לקוי יכולים להעיד על התחזות. לרוב, ארגונים רשמיים לא שולחים הודעות עם שגיאות כתיב וניסוח לקוי.
5. **הבטחות מוגזמות** - הודעות המכילות הבטחות, הצעות לפרס או הצהרות בלתי סבירות הן בדרך כלל כאלה, לא סבירות ומזויפות.

6. **בקשה לפרטים אישיים** - אלא אם הלקוח נרשם באופן יזום לאתר או ביצע רכישה באינטרנט, לרוב אין סיבה שיבקשו ממנו פרטים אישיים כגון סיסמאות, קוד ופרטי כרטיס אשראי.
7. **שימוש בקישורים מקוצרים** - בחלק מן המתקפות, נוטים להשתמש בקישורים מקוצרים כדי להסתיר את הכתובת האמתית של הקישור. ואולם, לא כל כתובת מקוצרת היא פישינג.
8. **הפנייה לאתרים חיצוניים** -אתרים מתחזים שכתובתם דומה לכתובת האתר האמיתי אך שונה בסדר האותיות, המילים ולפעמים כוללת טעויות איות קטנות. מומלץ לבחון היטב את הכתובת של האתר.
9. **כתובת שגויה** - את אמינות כתובת האתר ניתן לוודא באמצעות אתרים ייעודים לכך או באמצעות הצגת הכתובת האמיתית של האתר על ידי מיקום העכבר על הקישור. בכל מקרה אם האתר מוכר, מומלץ לגשת אליו באופן יזום דרך הדפדפן ולא דרך הקישור שנשלח בהודעה.
10. **קבצים מצורפים** - מומלץ לבחון את פתיחת הצרופה שהתקבלה בדוא"ל או את הקובץ שמבקשים בקישור או באפליקציה להוריד למכשירך. מומלץ לשים לב אם הבקשה מגיעה ממקור או מכתובת דואר אלקטרוני של שולח שציפיתם לו, אך לעיתים צרופות מזיקות נשלחות גם מדוא"ל של שולח מוכר. חשוב לשים לב אם מדובר בקובץ הרצה - קובץ שנותן פקודות למחשב בסיומת EXE. לעיתים קובץ הרצה מסתתר גם בקובץ שנראה לגיטימי.

זיהיתי את הסימנים, התעורר חשדי, איך מתמודדים?

אל תלחצו ואל תילחצו - ברוב המקרים של הודעות דיוג, אם לא הקלקתם על הקישור או אם הקלקתם ולא מילאתם פרטים, אפשר להיות רגועים. במקום להקליק ישירות על הקישור, יש מה לעשות:

- **בדיקה באתר הרשמי** - במקום ללחוץ ישירות על הקישור שנשלח, כדאי לבדוק באתר הרשמי של הארגון או החברה באמצעות גלישה מהדפדפן או מחיפוש בגוגל. אם יש איזור אישי באותו אתר,

אפשר לבדוק בו האם יש בעיה או דרישה מסוימת כפי שאולי מנסים בהודעת הדיוג לטעון.

- **חיפוש אזהרה להודעת הדיוג** - באתר הרשמי של הארגון או ברשתות החברתיות הרשמיות שלו מופיעה לעיתים אזהרה מהודעת הדיוג המתחזה לארגון. כמו כן, ברשתות החברתיות של המערך מופיעות לעיתים אזהרות ממתקפות דיוג רחבות.
- **בדיקה עם מערך הסייבר הלאומי** - בחיוג ישיר 119 למרכז המבצעי של מערך הסייבר הלאומי, יכול כל אזרח וארגון לדווח, להתייעץ ולקבל סיוע ראשוני. זה חינם, זה פשוט וזה עובד 24/7.
- **הצלבת מידע קצרה** - אם למשל התקבלה הודעה על תשלום על חבילה שהוזמנה, מומלץ להצליב את מספר ההזמנה שמופיע בהודעה, עם אישור ההזמנה שהתקבל בעת הרכישה.
- **מחיקת ההודעה** - אם הסימנים נראים חשודים ובדיקה קצרה שלכם מעלה שמדובר בהודעה מתחזה, מומלץ לדווח עליה למערך, למחוק אותה ולחסום את המספר/ כתובת השולח.