התגוננות מפני מיילים זדוניים

דואר אלקטרוני (Email) הפך לא מכבר לכלי תקשורתי אשר קשה לדמיין את חיינו בלעדיו: היכולת לשלוח מייל לכל אחד, בכל מקום, בצירוף קבצים תמונות וסרטים, הפכה כבר ליכולת אשר איננו יכולים לתפקד בלעדיה.

עם זאת, התגברות השימוש ותלותנו בדואר האלקטרוני, מושכת גם תוקפים ועבריינים אשר מעוניינים לנצל את אמצעי התקשורת הזה לטובתם האישית.

להלן שלושה סוגים של מיילים זדוניים המשמשים את התוקפים ומספר כללי אצבע אשר ניתן לאמץ על מנת למזער את הסיכון להיפגע מהם.

סוגים של מיילים זדוניים

- **דואר הזבל (Spam)** דואר זבל הינו הודעה שיווקית אשר נשלחת לתיבת הדואר האישית שלכם מבלי שנתתם את אישורכם לכך. בין הודעות אלו ניתן לראות למשל:
  - "הרזייה בטוחה עכשיו!"
  - "המוצר שאתם צריכים בדיוק עכשיו נמצא בהנחה!"
  - "מתנה לכל רוכש!"
- דיוג (phishing) - דיוג הוא סוג של הנדסה חברתית. התקפות דיוג נעשות באמצעות הדואר האלקטרוני או אתרי אינטרנט זדוניים כדי להונות באמתלה כלשהי תוך התחזות לשולח לגיטימי ולבקש מידע אישי או לפתות את הקורבן למסור סכום כסף או מידע לידי שולח המייל. סוג זה של הונאות איננו חדש, אך קלות שליחת המיילים מאפשרת לעבריינים תפוצה רחבה בעלות נמוכה יחסית. מספיק כי אחוז קטן מאוד מהנמענים ייענה להצעות כדי לאפשר לפושעים לגרוף סכום כסף גדול. בין ההונאות המפורסמות יותר ניתן למנות את:
  - "הצילו, נתקעתי בחו"ל בלי כסף. אנא שלחו לי סכום קטן לחשבון הבנק הבא: ."...
  - "הזדמנות עסקית יוצאת דופן – רק היום!"
  - "נסיך אפריקאי מעוניין להוריש לך סכום כסף גדול. אנא שלח צ'ק קטן לכיסוי ההוצאות"...

- דיוג ממוקד(Spear Phishing) - מיילים אשר תכליתם לשמש כראש גשר למתקפה מורכבת יותר:

השימוש במייל אלקטרוני מאפשר לתוקף להשיג נגישות לפרטים אינטימיים או למחשב האישי .לדוגמא, תוקף יכול לשלוח דואר אלקטרוני, לכאורה מחברת כרטיסי אשראי מכובדת או מוסד פיננסי המבקש לכאורה לאור בעיה כלשהי את אימות פרטי החשבון. כאשר המשתמש יגיב על הפניה עם המידע המבוקש, התוקפים ישתמשו במידע כדי לקבל גישה לחשבונו. בין הטכניקות הללו ניתן למנות:

- ניסיונות להשגת פרטים אישיים תוך התחזות לשולח לגיטימי. לרוב יהיו אלו סיסמאות או פרטי כרטיס אשראי, לעתים אף באמצעות פנייה אישית והתאמת המייל לקורבן
- ניסיונות לגרום לקורבן לפתוח צרופה (Attachment) אשר עשויה להכיל תוכנה זדונית כגון סוס טרויאני .
- ניסיונות לגרום לקורבן ללחוץ על קישור המוביל את הקורבן לאתר זדוני אשר ידביק את מחשבו בתוכנה זדונית .

<u>כללי אצבע להתגוננות</u>

1. חפש סימנים חשודים:
   i. גורם המבקש ממך לשלוח פרטים אישיים אשר הוא אמור להכיר אותם.
   ii. ניסיונות להלחיץ באמצעות סנקציה או מועד אחרון.
   iii. המייל של השולח נראה חובבני או לא מתאים לתוכן המכתב למשל: מכתב מבנק אשר נשלח מתיבת Gmail.
   iv. ריבוי של סימני קריאה או אותיות גדולות.
   v. תחביר רעוע או שפה לקויה.
2. לא מכיר את השולח? אל תפתח את המייל, במידת האפשר.
3. לא מכיר את השולח? היזהר ואל תפתח צרופות(Attachments).
4. אל תלחץ על קישורים לאתרים מוכרים מתוך המייל. פתח את האתרים המוכרים בנפרד, בדפדפן.

5. אם אתה חושב שנפלת קורבן לדיוג, הקפד לשנות את הסיסמאות בכל החשבונות השונים בהם אתה משתמש. הקפד לא להשתמש באותה סיסמה בשירותים שונים והשתמש בסיסמה ארוכה ומורכבת.
6. במידה וקיבלת דואר זבל(Spam) – ניתן לפעול לפי ההנחיות הנוספות בסוף המסמך.
7. במידה ויש לך חשש כי הותקפת – אל תהסס, דווח למהנדס המיחשוב היחידתי או לממונה אבטחת המידע של הטכניון CISO@technion.ac.il
8. והכי חשוב: היגיון בריא! אם משהו נראה חשוד, יש סיכוי סביר שהוא אכן חשוד .

הנחיות נוספות:

גניבת זהות או הונאה

אם נפלתם קורבן לעבירות הונאה, ואתם חוששים כי נעשה שימוש בפרטיכם האישיים לצורך מטרות פליליות, ניתן לפנות ליחידה הארצית לחקירות הונאה של משטרת ישראל או לפנות לתחנת המשטרה הקרובה למקום מגוריכם ולהגיש תלונה.

ספאם (דואר זבל)

אם הודעות שיווקיות נשלחות לדואר האלקטרוני שלכם כחלק מהפצה מרוכזת של דואר מבלי שנתתם את אישורכם לכך, ניתן לראות בהודעות אלו כ"ספאם" (דואר זבל). לפי החוק, ניתן להגיש תביעה אזרחית בבית המשפט לתביעות קטנות נגד שולחי ספאם ולקבל פיצוי ללא הוכחת נזק של 1,000 ש"ח. הסבר על אופן הגשת התביעה ניתן למצוא באתר בתי המשפט וכן, לפניכם דוגמה לכתב תביעה בגין שליחת דואר זבל.

הטרדה מאיימת ברשת

אם נחשפתם למקרה של הטרדה אישית שהחלה ברשת אך יוצאת מגבולותיה ומהווה איום ממשי עבורכם בעולם הפיזי, תוכלו להגיש תלונה למשטרה או בקשה לבית המשפט לצו מניעה כנגד המטרידים, על פי חוק הטרדה מאיימת. כמו כן, עומדים לשירותכם ארגונים שונים שיכולים לסייע לכם להתמודד עם הטרדה ברשת .

הטרדה בפורומים או בצ'אטים

במקרים של התנהגות שאינה נאותה בפורומים או בצ'אט שמלווה בהתקפות אישיות עליכם, חשיפת זהותכם ברבים או חשיפת פרטים אישיים שלכם שאינכם מעוניינים שיחשפו, רצוי לתעד את מהלך השיחה באמצעות תצלומי מסך ושמירת קישורים להודעות רלוונטיות ולהפנותם לאתר המארח.

גניבת מספר כרטיס אשראי

אם הינכם חוששים כי מספר כרטיס האשראי שלכם נחשף או נגנב ונמצא בשימוש על ידי גורמים עברייניים, פעלו לבטלו באופן מיידי מול חברת כרטיסי האשראי שלכם.

קישורים ומידע נוסף:

CERT Australia: Protect your business from spear phishing

US-CERT: Recognizing and Avoiding Email Scams

CPNI: Spear Phishing Microsoft: Email and web scams: How to help protect yourself

PayPal: Can you spot phishing?

Apple: Identifying fraudulent "phishing" email