הדרכת מודעות לאבטחת מידע וסייבר לסגל האקדמי ומנהלי

בשנים האחרונות חלה עלייה משמעותית בשימוש בטכנולוגיות בינה מלאכותית (AI), לצד גידול באיומי סייבר מתקדמים.

תוקפים משתמשים בכלי AI ליצירת הודעות פישינג אמינות, התחזות לעובדים ומנהלים, זיוף מסמכים, ושליחת קבצים מזויפים שנראים לגיטימיים לחלוטין.

❖ חשוב לשים לב

- להגביר מודעות לאיומי סייבר מבוססי AI.
- לצמצם סיכוני פישינג והתחזות.
- לחזק את אבטחת החשבונות הארגוניים.
- להטמיע שימוש נכון באימות רב־שלבי (MFA).

❖ איומי AI במכללה

☒ כיצד תוקפים משתמשים ב־AI?

תוקפים עושים שימוש בבינה מלאכותית לצורך:

- יצירת מיילים אמינים ללא שגיאות כתיב.
- התחזות למנהלים, מרצים או עובדים.
- יצירת הודעות WhatsApp מזויפות.
- זיוף קול ותמונות.
- יצירת קבצים וקישורים מתחזים.

☒ סימנים מחשידים

יש לשים לב ל:

- בקשות דחופות להעברת מידע או סיסמאות.
- קישורים לא מוכרים.
- קבצים מצורפים חריגים.
- הודעות המבקשות "לאשר כניסה" או "לעדכן סיסמה".
- כתובות דוא"ל הדומות לכתובת אמיתית אך שונות בפרטים קטנים.

❖ מתקפות פישינג

☒ מהו פישינג?

פישינג הוא ניסיון לגנוב מידע אישי או ארגוני באמצעות התחזות לגורם אמין.

דוגמאות:

- מייל המזדהה כ־Microsoft או מערכת המכללה.
- הודעה המבקשת לאפס סיסמה.
- קישור מזויף לעמוד התחברות.

☒ כללי זהירות

- אין ללחוץ על קישורים חשודים.
- אין למסור סיסמאות בטלפון או במייל.
- יש לבדוק את כתובת השולח במלואה.
- במקרה של ספק – לפנות לצוות המחשוב.

❖ אימות רב־שלבי (MFA)

☒ מהו MFA?

אימות רב־שלבי הוא מנגנון אבטחה המחייב בנוסף לסיסמה גם אמצעי אימות נוסף, כגון:

- קוד חד־פעמי בטלפון.
- אפליקציית אימות.
- הודעת אישור במכשיר הנייד.

☒ מדוע MFA חשוב?

גם אם סיסמה נגנבה, MFA מקשה משמעותית על חדירה לחשבון.

❖ הנחיות לעובדים

- אין לאשר בקשות MFA שלא בוצעו על ידכם.
- במקרה של בקשת התחברות לא מוכרת – לדווח מיד.
- יש להחזיק את אפליקציית האימות מעודכנת.
- אין לשתף קודי אימות עם אף גורם.

❖ אחריות העובדים

כל עובד אחראי:

- לשמור על סיסמאות חזקות.
- לנעול מחשב בעת עזיבת העמדה.
- לדווח על אירועים חריגים.
- להימנע מהתקנת תוכנות לא מאושרות.
- לפעול בהתאם להנחיות אבטחת המידע של המכללה.

❖ דיווח על אירוע חשוד

בכל חשד ל:

- הודעת פישינג,
- התחזות,
- קישור חשוד,
- או פעילות חריגה,

יש לפנות באופן מיידי לצוות המחשוב / אבטחת המידע של המכללה.

❖ סיכום

מודעות עובדים היא קו ההגנה המרכזי שלנו.
שילוב בין ערנות עובדים, הדרכות תקופתיות ושימוש ב־MFA מסייע בהגנה על מערכות המידע, המידע האקדמי והמידע האישי של כלל משתמשי המכללה.

בברכה,

גנזיאן אלפרד,

מנמ"ר מכללה אקדמית נתניה