התנהלות בטוחה ברשתות החברתיות וזיהוי פרופילים מזויפים

השימוש ברשתות חברתיות הפך לחלק בלתי נפרד מחיינו, אך הוא גם טומן בחובו סיכונים רבים, ברמה האישית והעסקית. לצד היתרונות, חשוב להגן על המידע האישי, הביטחוני והעסקי ועל הפרטיות שלנו ושל בני משפחותינו.

עובדי חברות ותעשיות ביטחוניות הנן יעד לתקיפות סייבר בידי גורמים עוינים ביטחוניים או יריבים עסקיים, המעוניינים לחדור לרשתות החברה או לטלפונים הסלולאריים.

שימו לב!

- אין להירשם לרשתות חברתיות, אתרי הכרויות ואתרים הדורשים מידע אישי עם המייל הארגוני.
- הימנעו משיתוף מידע על תפקידכם, ו-ודאו כי פירוט מידע אודות פעילות החברה מאושר לפרסום בהתאם לנהלי החברה.
- הימנעו מחשיפת מיקומים בארץ ובחו"ל. דגש מיוחד יש לשים על אי העלאה שיתוף של תמונות בעת נסיעת עבודה עסקית, המעידה על קיום הפעילות במדינה רגישה ו/או לקוח ועל שהות העובד.ת במדינה בזמן אמת.
- צמצמו חשיפת מידע אישי כזה העלול לשמש "משטח תקיפה" שלכם (זיהוי סיסמאות, הנדסה חברתית, פעילות שיטוי וכו').
- בדקו תמונות לפני שיתוף, ודאו שלא קיים בהם מידע רגיש או מסווג.
- נהלו רשימת חברים מוכרים בלבד.
- הגדירו הגדרות פרטיות קפדניות.
- השתמשו בסיסמאות חזקות ושונות לכל שירות, אפליקציה או אתר.

טיפים מרכזיים - איך להיזהר?

בדיקת אמינות תמונות פרופיל.

זהירות וחשדנות מפרופילים דלי מידע או חדשים.

הצלבת מידע עם פרופילים ברשתות / אתרים.

תשומת לב לפרופילים עם מעט חברים או לייקים (Likes) קנויים.

בכל חשד, דווחו לאגף הביטחון או לממונה הביטחון החטיבתי.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC