BEC

(Business Email Compromise)

הונאת מיילים עסקיים כוזבים (BEC) היא סוג של הונאה מקוונת, שבה תוקפים מתחזים לאנשי מפתח בארגון כדי להונות עובדים ולגרום להם להעביר כספים או מידע רגיש. בהונאות מסוג זה, התוקפים משתמשים בטכניקות "הנדסה חברתית" כדי לזייף זהויות וליצור אמון עם הקורבנות שלהם. הונאות מסוג זה עלולות לגרום לארגונים להפסדים כספיים משמעותיים ולפגיעה במוניטין.

איך זה עובד?

- **הונאת מנכ"ל:** התוקפים מתחזים למנכ"ל או לבכיר אחר בארגון ושולחים הודעות דוא"ל לעובדים עם בקשות להעברת כספים דחופה לחשבון בנק מזויף.
- **הונאת חשבוניות:** התוקפים מתחזים לספקים, שולחים חשבוניות מזויפות לגורמי הכספים של הארגון ומבקשים תשלום לחשבון בנק שבשליטתם.
- **התחזות לעורך דין:** התוקפים מתחזים לעורכי דין ושולחים הודעות דוא"ל עם בקשות לתשלום או למסירת מידע רגיש.
- **גניבת נתונים:** התוקפים מתמקדים במחלקות משאבי אנוש כדי לגנוב מידע אישי על עובדים, כמו מספרי ביטוח לאומי ופרטי קשר, לשימוש בהונאות עתידיות.

טיפים מרכזיים - איך להיזהר?

אם אתם מקבלים הודעת דוא"ל ממקור לא מוכר או עם בקשות חריגות, גלו חשדנות. בדקו בקפדנות את כתובת הדוא"ל של השולח וודאו שהיא תואמת את הכתובת הרשמית של הארגון. שימו לב לשגיאות כתיב או ניסוח לא שגרתי.

אבל... אם התוקף השתלט על הדוא"ל של הגורם המוכר לכם, זה לא מספיק - לפני ביצוע פעולות כספיות או מסירת מידע רגיש, ודאו את זהות השולח באמצעות אמצעי תקשורת נוסף, כמו שיחת טלפון או פגישה פנים אל פנים. אל תסתמכו רק על הדוא"ל, שכן תוקפים יכולים לזייף כתובות דוא"ל.

אין להעביר כספים או מידע לחשבונות / גורמים חדשים ללא אישור מנהל בכיר.

השתמשו בסיסמאות חזקות וייחודיות לכל חשבון. אל תשתפו סיסמאות עם אחרים ו-ודאו שהן מתעדכנות באופן קבוע.

אם אתם חושדים שקיבלתם הודעת דוא"ל חשודה או שנפלתם קורבן להונאה, דווחו על כך מיד למוקד הסייבר או לממונה הביטחון. דיווח מהיר עשוי למנוע נזקים נוספים ולעזור באיתור התוקפים.

יש להקפיד שרק מורשים יהיו בעלי גישה למידע רגיש ולביצוע פעולות כספיות. שימוש במערכות ניהול גישה כדי לפקח על מי יכול לגשת לאילו נתונים.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC