



אלו המתקפות הנפוצות בתקופת משבר הקורונה

קיבלתם עוד המלצה על תוכנה מגניבה שמביאה את החדשות האחרונות בנושא הקורונה? גיליתם אתר חדש שמציג גרפים בנושא וירוס הקורונה? התקשרו מארגון הבריאות העולמי וביקשו תרומה דחופה? אין ספק כי משבר הקורונה הכניס הרבה יצירתיות לעולם מתקפות הסייבר. המשותף לכולן הוא השימוש במשבר לצורך ניסיונות הונאה של ארגונים ואנשים פרטיים. כדי לעזור לכם להתגונן, ריכזנו עבורם את שיטות התקיפה הנפוצות והמלצות כיצד להתמודד עמן.

פישוינג

הסיכון העיקרי: גניבת פרטי הזדהות (שם משתמש וסיסמא), מידע אישי ופיננסי או התקנת נזקה **האימים** (הודעת דוא"ל)

- הודעת דוא"ל מגורם רפואה שמבקש מכם משהו
- הודעה מטעם גורם ממשלתי או בין לאומי (כמו ארגון ה WHO או ה UN)
- הודעה שמביאה לכם חדשות אודות הקורונה ומבקשת ללחוץ על קישור להמשך קריאה
- הודעות בנוגע לשירותי שיחות וידאו (זום, סקיפ ועוד) או שירותי סטרימינג פופולאריים (נטפליקס, דיסני+ ועוד)
- ניסיונות סחיטה הקשורים לצפייה בתוכן פורנוגרפי או איום להדבקה בנגיף

המלצות

- אם השולח אינו מוכר - חשדו בתוכן ההודעה
- אם התוכן נראה לכם מוזר, התייעצו עם חבר לגבי
- מומלץ להימנע מלחיצה על קישורים והורדה של קבצים מצורפים
- הקפידו לגלוש רק לאתרים רשמיים ולבחון בדקדוק מיילים והודעות הקשורות לנושא.
- בדקו תמיד את שם השולח, זהותו וכתובתו - העדיפו תמיד לפתוח דפדפן, להקליד את שם החברה/האתר ולגלוש כך ליעדכם.
- שימו לב לניסיונות מינפולציה ריגשית, להודעות בעל נוסח מאיים, מאיץ, מפחיד או מפתה. בכל הנוגע לניסיונות סחיטה, יש לפנות אל המשטרה.



וישינג

הסיכון העיקרי: גניבת פרטי הזדהות, מידע אישי ופיננסי, גניבת כספים.

האימים (שיחת טלפון)

- שיחות מגורם רפואה שמבקש מכם משהו
- שיחות מטעם חבר או קרוב משפחה רחוק שנפגע מהקורונה ומבקש עזרה
- שיחות מארגונים חברתיים שתומכים בחולי קורונה
- שיחות לכאורה מבכירים בארגון המבקשים לבצע פעולה

המלצות

- השיחה חשודה? נתקו וודאו את אמתותה באמצעות מדיה אחרת או באמצעות המספר הרשמי של החברה המפורסם באינטרנט.
- התייעצו עם לפחות שני אנשים אמינים לפני קבלת החלטה פיננסית
- מומלץ לא להילחץ מדחיפות האירוע כפי שהוא מוצג בשיחת הטלפון



סמישינג

הסיכון העיקרי: הפנייה לאתר זדוני לצורך גניבת פרטי הזדהות ומידע אישי ופיננסי

האימים (הודעת SMS או שירות מסרים מדי)

- שיחות מגורם רפואה שמבקש מכם משהו
- שיחות מטעם חבר או קרוב משפחה רחוק שנפגע מהקורונה ומבקש עזרה
- שיחות מארגונים חברתיים שתומכים בחולי קורונה
- שיחות לכאורה מבכירים בארגון המבקשים לבצע פעולה

המלצות

- מומלץ להימנע מלחיצה על קישורים בהודעה
- עלה חשש? בררו טלפונית או באתר עם הגורם שפנה אליכם בהודעה
- מומלץ לא להילחץ מדחיפות האירוע כפי שהוא מוצג בהודעה



הונאות פיננסיות (BEC)

הסיכון העיקרי: התחזות לספק/לקוח/בכיר וגניבת כספים

האימים (שיחת טלפון או הודעת דוא"ל)

- גורמים רשמיים עסקיים או ממשלתיים המבקשים לבצע העברה בנקאית
- התחזות לבכיר בארגון המבקש לבצע פעולה פיננסית
- ספק או לקוח של הארגון שמבקש תשלום מידי או מתלונן על איחור בתשלום

המלצות

- עלה חשש? בררו טלפונית או במדיה שונה את אמיתות הבקשה עם הגורם שפנה אליכם בהודעה
- פעלו בהתאם לנהלי העברת הכספים של החברה
- היו ערניים לשינויים בפרטי התשלום
- חשדו בהודעות המבקשות להעביר כסף באופן בהול.



אתרים זדוניים

הסיכון העיקרי: גניבת פרטי הזדהות ומידע אישי ופיננסי

האימים (גלישה לאתר)

- אתרים המתחזים לאתרי חדשות רשמיים בנושא וירוס הקורונה
- מודעות זדוניות או מוצרים/תרופות לנגיף קורונה באתרים מוכרים
- קישורים זדוניים בכתבות המפורסמות באתר
- אתרים המתחזים לשירותי סטרימינג (נטפליקס וכו') או לשירותי שיחות וידאו

המלצות

- העדיפו הקלדה ישירה של שם האתר בדפדפן או גישה מרשימת המועדפים בלבד
- שימו לב היטב בשורת הדפדפן לשם האתר ולכתובתו, וודאו את אמתותם. בנוסף, חפשו את סימן המנעול בשורת כתובת האתר (סימן שהאתר משתמש בהצפנה)
- מומלץ להתקין תוסף דפדפן לחסימת פרסומות באתרים

אפליקציות חשודות

הסיכון העיקרי: התחזות לספק/לקוח/בכיר וגניבת כספים

האימים (גניבת מידע רגיש. תתכן גם השתלטות על המכשיר או נעילתו)

- אפליקציות מתחזות לאפליקציות חדשות בנושא וירוס הקורונה
- מודעות זדוניות המוצגות בזמן שימוש באפליקציה
- אפליקציות המציגות כתבות בנושא קורונה עם קישורים לאתרי אינטרנט
- אפליקציות בנושא קורונה המבקשות הרבה הרשאות

המלצות

- הורידו אפליקציות לטלפון הנייד רק מחנויות רשמיות (גוגל, אפל, סמסונג וכו')
- המנעו מהתקנת אפליקציות צד שלישי שהורדתם מאתר אינטרנט
- הסירו אפליקציות שאינן בשימוש
- התקינו תוכנות אבטחת מידע בטלפון הנייד



שיחות ועידה

הסיכון העיקרי: דלף מידע רגיש, הדבקה בנוזקה, חשיפה לתוכן לא ראוי

האימים

- הסתננות לשיחות והצגת תוכן לא ראוי
- הסתננות לשיחות וגניבת מידע רגיש
- תוכנות מתחזות לשירותי וידאו פופולאריים
- חשיפת שיחות פרטיות

המלצות

- ודאו עדכניות גרסאות התוכנה, מערכת ההפעלה, הדפדפן והאנטי וירוס שלכם
- הגנו על הועידה בסיסמא חזקה
- שילחו קישור לשיחה באופן פרטי
- מנעו כל אפשרות להצטרף לפני המארז
- הגדירו חדר המתנה לשיחה ואשרו כל משתתף
- דאגו לצאת מהשיחה באופן מסודר



בכל חשש או שאלה - פנו לאבטחת המידע