

מגזין עצות מודעות

סיכום שנת 2022

הראל
ביטוח ופיננסים



תוכן עניינים

- 4..... משתמשי הסמארטפונים צריכים להישאר בטוחים מפני הונאות QRishing
- 5..... סכנה מעבר לכתף: מושגים של הנדסה חברתית
- 8..... הונאות ברשתות חברתיות ואתרי הכרויות
- 9..... גניבת זהות ברשתות חברתיות
- 11..... האיום המצולם - מצלמות רשת ביתיות חשופות לתוקפים
- 12..... קצרים, ויכולים לגרום נזק גדול
- 13..... ריגול או נוחות - סיכוני סייבר במכשירים לבישים
- 15..... חמש דרכים באמצעותן גונבים לכם את האשראי - וכיצד ניתן למנוע אותן
- 16..... איך תזהו שהמחשב שלכם נדבק?
- 17..... כך האקרים מנטרים את המידע שלכם - בלי שאתם יודעים
- 19..... לחיצה על קישור תמים גרמה להונאה פיננסית של למעלה מ-10 אלף עסקים



טיפ מודעות

מס' 1

משתמשי הסמארטפונים צריכים להישאר בטוחים מפני הונאות QRishing

מתקפות מבוססות קודי QR הפכו להיות נפוצות בשנים האחרונות כאשר הן מאפשרות גניבת מידע אישי, **פיתיון קליקים** ועד הונאות כספיות. השימוש בקודי QR מאפשר לתוקף להסתיר את הקישור לאתר אליו מפנה הקוד ובכך מספק מעטפת מצוינת להתל בקורבן.



קוד QR הוא תמונה מרובעת בצבעי שחור לבן המשמש להטמעת הפניה לאתר אינטרנט. בעת סריקת הקוד על ידי המצלמה של הטלפון הנייד, נפתח הדפדפן עם הקישור המוטמע בקוד והגולש מופנה לאתר היעד. קודים כאלו משמשים במוצרי פרסום, עיתונים, מגזינים, עלונים, פוסטרים ועוד. מלבד הפניה לאתר, קודים אלו יכולים לשמש לשמירת אנשי קשר, פתיחת יישומים או ביצוע תשלומים. פושעי סייבר, כאמור, מנצלים קודים אלו. אחת הדרכים לניצול קוד זה היא לשנות את קודי ה-QR שנסרקים בעת ביצוע רכישת

שירות או מוצר. עד שנחשפו פרטי המקבל, התשלום כבר בוצע. להונאות על בסיס קודים אלו קוראים QRishing (שילוב של **פישיונג** וקוד QR). אלו כוללות מגוון צורות של **הנדסה חברתית** כמו הדבקת מעטפת QR זדונית שקופה על גבי קוד QR אמיתי או שינוי פרטי החברה מעל קוד ה-QR במטרה לרמות את המשתמשים להאמין שהם סרקו קוד לגיטימי. קודי QR יכולים לשמש גם כשובר הנחה. בצורה כזו המשתמש מתפתה לסרוק את הקוד שמוביל אותו לפעולה זדונית.

כיצד ניתן להתגונן?

ובכן, ראשית העדיפו לא לסרוק קודים כאלו. אם אין ברירה, סירקו רק קודים במקומות שאתם סומכים עליהם. אם הקוד מוצב בפלטפורמה שאתם לא מכירים - עדיף לא לסרוק בכלל.

אם החלטתם לסרוק, הקפידו לבחון את הקוד מקרוב. חפשו אם מודבקת עליו מדבקה

שקופה עם קוד נוסף. יש חשש? אל תסרוק אותו. אם סרקתם קוד ונפתח לכם אתר, העדיפו להימנע מהזנת פרטים אישיים כמו שם משתמש או סיסמה. אם אתם מזהים את בעלי האתר, העדיפו לגלוש לאותו אתר ישירות מחלון חדש בדפדפן באמצעות הקלדת הכתובת בשורת הדפדפן.

אם האתר שנפתח לאחר הסריקה אינו מתחיל בתחילת https, המנעו בגלישה בו. המשמעות היא שהתקשורת עם האתר אינה מוצפנת ותוקף פוטנציאלי יכול לבצע מניפולציות על הגלישה באתר.

אין ספק כי התוקפים מנסים בכל עת למצוא דרכים להתל בנו המשתמשים. מודעות ותשומת לב הם קו ההגנה הראשון. גם כאשר מדובר בקוד QR. נכון, זה נוח, אך טומן בחובו סיכונים. ההגנה הכי טובה היא להעדיף להימנע מסריקת קודים כאלו ככל הניתן.



טיפ מודעות

מס' 2

סכנה מעבר לכתף: מושגים של הנדסה חברתית

"סליחה, למה אתה מסתכל לי על הסלולרי?", נשמע קולה של גברת שעמדה בתור בסניף הבנק וחיכתה לתורה. מאחוריה, עמד אדם, גבוה ממנה וצפה בצג הסלולרי שלה. במקרה אחר, אדם שהלך ברחוב הרגיש דחיפה קלה מגבר שעמד לצידו. כעבור מספר דקות, נוכח לדעת שהוא נגנב מכיסו.

במקרה שלישי, צוות האבטחה של חברה מסוימת הריץ אחורה את הקלטת הוידאו וראה כיצד העובד מכניס התקן "דיסק און

קי" למחשב, מושך אותו החוצה לאחר מספר דקות, קם ויוצא ממשרדי החברה. אותו עובד לא חזר מעולם לעבודה.

מרביתנו, כאשר חושבים על מתקפת סייבר, חושבים על מתקפה המבוססת על מערכות מחשב בלבד. תוקף פורץ למערכת או משיג גישה מרחוק. אולם, חלק ממתקפות הסייבר משלבות גם פעולות פיזיות. כפי שמראות הדוגמאות לעיל. מהן שיטות הפעולה הפיזיות הנפוצות בעולם הסייבר? ריכזנו עבורכם רשימה התחלתית.

הפתרון | לא מתפתים, מפעילים היגיון בריא ובוחנים כל הבטחה לעומקה.

Dumpster diving



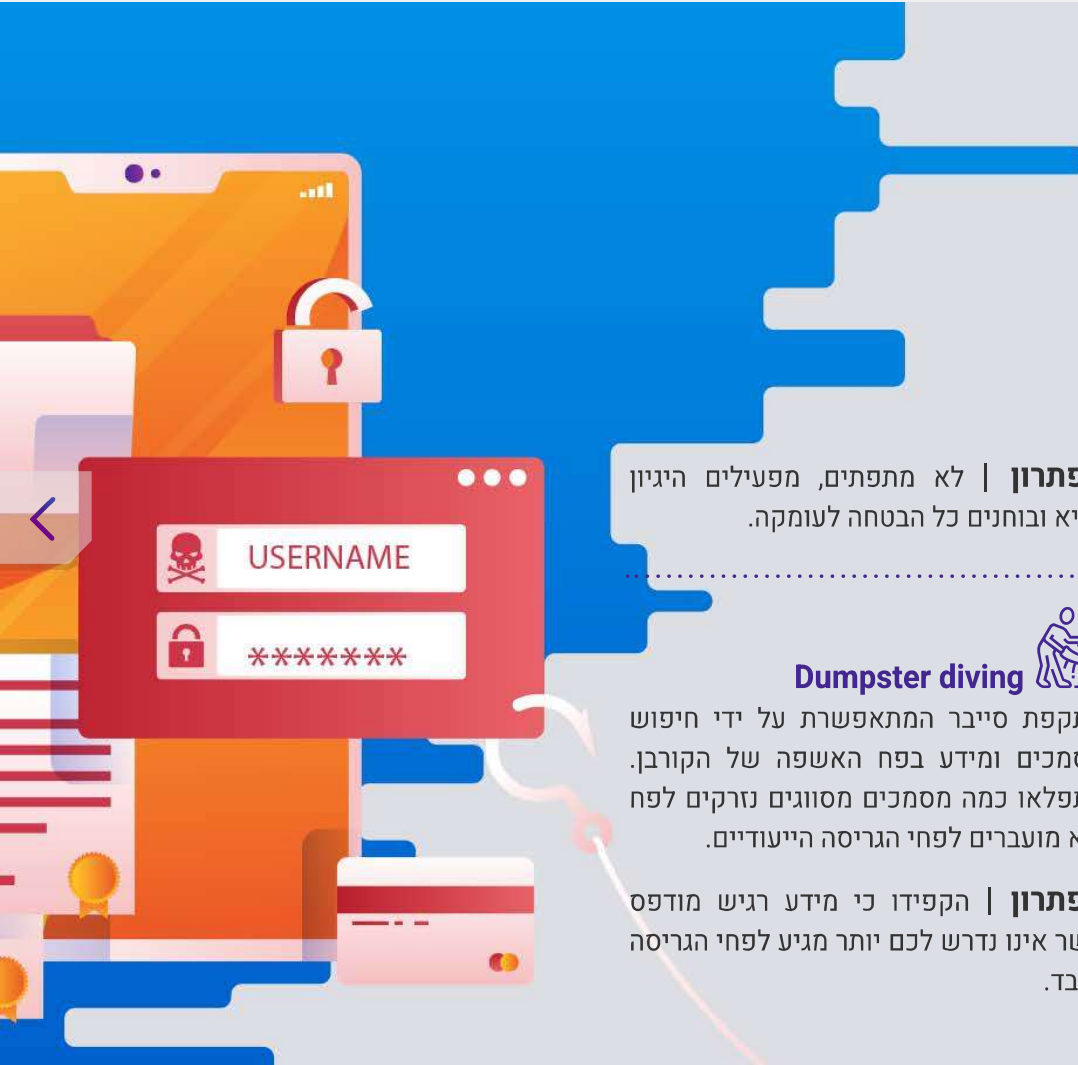
מתקפת סייבר המתאפשרת על ידי חיפוש מסמכים ומידע בפח האשפה של הקורבן. תתפלאו כמה מסמכים מסווגים נזרקים לפח ולא מועברים לפחי הגריסה הייעודיים.

הפתרון | הקפידו כי מידע רגיש מודפס אשר אינו נדרש לכם יותר מגיע לפחי הגריסה בלבד.

Baiting



טכניקה שבה תוקף משתמש בהבטחת שווא כדי לפתות קורבן למלכודת. למשל השארת USB זדוני בלובי או בחניון עם כיתוב מפתה עליו. במקרה זה התוקף מקווה שסקרנות של אחד מעובדי חברה המטרה של התוקף תגרום לו להכניס את ההתקן למחשב החברה על מנת לצפות בתוכן המפתה.



Pretexting

מונח זה הינו שם כולל למתקפות בהן התוקף משתמש במניפולציות שונות על מנת לבקש מהקורבנות מידע רגיש. ניתן להגיד ש- Pretexting הינו בעצם בניית הסיטואציה או ההונאה שבאמצעותה רוצה התוקף להשיג את המידע מן המשתמש.

הפתרון | היו ערניים, בחנו כל סיטואציה בעיניים פקוחות, עצרו וחשבו לפני שאתם פועלים באופן "אוטומטי". לא בטוחים? התייעצו, אל תילחצו וקחו את הזמן שלכם לבחינת המידע שאתם מוסרים ולמי אתם מוסרים אותו.

Diversion theft

הונאה במסגרתה תוקפים משכנעים חברות משלוח להפנות את המשלוח ליעד אחר מהיעד המקורי.

הפתרון | ודאו את זהות מבקש השינוי של כתובת היעד מעל לכל ספק.

Over-Helpfulness of Help Desk

התוקף מתקשר למוקד תמיכה של חברה, מעמיד פנים שהוא משהו בכיר / עובד / לקוח / ספק של החברה ומנסה לחלץ מידע רגיש מהמוקד. במקרים מסוימים ומתוחכמים יותר, יכול להיות שבשיחת הטלפון הוא ינסה לגרום למוקד לפתוח דוא"ל עם קישור או קובץ זדוני שהוא שלח אליהם מבעוד מועד.

הפתרון | ודאו תמיד את זהות המתקשר. אם קיים חשש, נתקו והתקשרו חזרה אל הגוף שיצר עמכם קשר, לפי פרטי הקשר הרשמיים המופיעים באתר החברה. במקרה של חשש להתחזות לעובד הארגון, נתקו את השיחה וצרו עימו קשר ישירות.

Quid Pro Quo

טכניקת מניפולציה בעולם ההנדסה החברתית אשר בה יתחזה התוקף למישהו שבכוונתו לסייע לכם בכל דבר שהוא. דוגמה לכך תהיה כאשר תוקף מתקשר לטלפון שלך ומעמיד פנים שהוא נציג תמיכה טכנית.

הפתרון | בחנו כל בקשה לעומקה, אל תמסרו מידע רגיש כגון סיסמאות או קודים לאף אחד שיוצר עמכם קשר בכל תואנה שהיא.

Shoulder surfing

טכניקת הנדסה חברתית בעולם הפיזי המשמשת להשגת מידע על ידי הסתכלות על מסך המחשב או הטלפון מעבר לכתפו של הקורבן.

הפתרון | שימו לב לסביבתכם כאשר אתם גולשים לאתרים רגישים או מתחברים לרשת העבודה במיוחד במקומות ציבוריים.

Tailgating

מתקפת הנדסה חברתית המאפשרת להאקרים לקבל גישה למערכת מוגנת בסיסמה באמצעות מעקב צמוד אחר אדם מורשה אל אזור גישה מוגבל. דמיינו את המצב הבא: אתם עובדים במקום שדורש כניסה

באמצעות כרטיס מגנטי ורק בצורה הנ"ל הדלת תיפתח. ליד הדלת משהו/י שמדברים בטלפון ונראים עסוקים. מיד כשהעברתם כרטיס ופתחתם את הדלת התוקף תופס את הדלת, מחייך אליכם וממלמל משהו כגון: תודה רבה, באמת שכחתי את הכרטיס או רק מהנהן ומחייך אליכם. כך התוקף נכנס למתחם החברה ואתם ממשיכים ליום עבודתכם בלי להבין שבזה הרגע הכנסתם תוקף לתוך משרדי החברה.

הפתרון | אין להכניס אף אחד למתחמי החברה ללא כרטיס עובד. שאלו את האורח למי הוא מגיע ולוו אותו אל יעדו או אל עמדת הקבלה שם יוכל להמתין למארחו.

גניבה

גניבת מחשב, טלפון סלולרי, שעון חכם וכל התקן אחר המשמש אותנו. התקנים אלו יכולים להכיל מידע רגיש או סודי-עסקי. גניבה ופתיחה שלהם מספקת לתוקף מודיעין ולעיתים אף יותר מכך. גניבת ארנק עם כרטיס אשראי תספק לתוקף מרווח זמן לבצע רכישות.



איש ביטחון או רפואה

בשיטה זו התוקף יתחזה לדמות סמכותית ויבקש לבצע פעולה דחופה לכאורה. בקשו אישור מקב"ט החברה או וודאו למי הוא מגיע ובדקו זאת מולו.



הפיתוי

בשיטה זו אדם זר פונה אליכם באמתלה של שיחת חולין. במסגרתה הוא מבקש לדעת פרטים אודות התפקיד שלכם בחברה. אל תתפתו לזרים מתנחמדים.



"אתה אח של דוד?"

בשיטה זו זר שאסף מידע אודותיכם פותח בשיחה מקרית, לכאורה, ובה הוא מקשר אתכם למישהו שאתם מכירים. הטילו ספק בכל שיחה מקרית עם אדם זר.



"תעביר את זה לבוס"

בשיטה זו, זר יזדהה כקולגה לעבודה ויבקש מכם להעביר חבילה למנהל שלכם (ינקוט בשמו הנכון). סרבו באדיבות והמציאו תירוץ שאינכם בדרך למשרד.



מצלמות בכספומטים וקוראי שפתיים

מצלמות חשאיות במכשיר הכספומט (סקימרים) יכולות לצלם את פרטי האשראי לשימוש עתידי של הפושע. קוראי שפתיים יכולים לגנוב פרטי אשראי מהפס המגנטי של חלק מכרטיסי האשראי.



שולחן נקי

הלכתם הביתה, לשירותים או להכין קפה? פושע יכול "לגלח" לכם מסמכים המפוזרים על שולחן העבודה. קמתם מהשולחן? שימו הכל במגירות. מסמכים רגישים עדיף לנעול או לאחסן בכספת.



"באתי לתקן את המדפסת"

בשיטה זו התוקף מתחזה לאיש תחזוקה ומבקש להיכנס למשרד. הקפידו לוודא את זהות האדם מולכם.



Pop up window attack

הודעות הונאה ש"צצות" למשתמשים כחלונות קופצים במהלך גלישה באינטרנט. דוגמה לכך הינה חלונות קופצים אשר מתריעים שהמחשב שלכם "נדבק" בוירוס ועליכם לחחוץ לאישור כדי לטפל בנושא - במקרה זה לחיצה על האישור היא זו אשר תדביק את מחשבכם. **בנוזקה**



הפתרון | לא לוחצים על חלונות קופצים. התקינו חוסם פרסומות.



דיסק און קי

פשוט וקל. לוקחים התקן זיכרון נייד, מכניסים לסלולרי (לשקע הטעינה), למחשב או לשרת, שואבים מידע - ובורחים מהמקום.





טיפ מודעות

מס' 3

הנאות ברשתות חברתיות ואתרי הכרויות

ערכת פרופילים ברשתות החברתיות

זכרו שיש קשר ישיר בין אתרי היכרויות לרשתות חברתיות. כמעט כל אחד שתפגשו באתר היכרויות, יחפש אתכם ברשתות חברתיות. לכן, טרם הרישום לאתר היכרויות, ערכו את הפרופילים החברתיים שלכם בהתאם. הקפידו על הגדרות הפרטיות בפרופיל, מחקו את פרטי מקום מגוריכם ואת מספר הטלפון שלכם, סירקו אחר תמונות בפרופיל והסירו כאלו שמסגירים מיקום, מקום עבודה, בני משפחה, ילדים ופרטים מזהים אחרים.

שיחת וידאו חי

נוכלים או רמאים לא ירצו לחשוף את עצמם באתר היכרויות. התחלתם שיח פרטי עם מישהו מהאתר? בחנו את האפשרות לבקש ממנו שיחת וידאו חי. אם הוא מסרב - זו יכולה להיות נורה אדומה.

מפגש פיזי? תזהרו

הגעתם לשלב של מפגש פיזי? מזל טוב. לצד המיחושים בבטן מהתרגשות, זכרו שזהו מפגש ראשון וצריך להיזהר. קיבעו להיפגש

במקום ציבורי (לא רק שניכם), עדיף בשעות האור, במקום מרוחק מאזור מגורים. הקפידו להגיע למיקום 15-30 דקות לפני. כך תוכלו לבחור שולחן במיקום נוח. בסיום המפגש, אם יש חשש, סרבו בעדינות להצעת ליווי הביתה. ליתר ביטחון, תכינו מראש ידיד או בן משפחה שיתקשר אליכם במהלך המפגש וישאל אם הכל בסדר. יש בעיה במפגש? תגידו שזה טכנאי הטלוויזיה ושאתם חייבים לזוז הביתה.

העברת כספים

אתם מאוהבים? יש פרפרים בבטן? מצוין. נוכלים מתוחכמים פועלים לבסס אמון. ככאלו, הם יעדיפו להמתין בסבלנות במשך מספר שיחות ומפגשים, במטרה "לנעול" את הקורבן. כאשר הקורבן "נעול רגשית" לנוכל, ניתן לנצל אותו פיננסית. בן הזוג החדש שלכם ביקש העברה כספית כי הוא במצוקה? אולי להעביר אליו זכות על נכס? שימו לב: זו נורה אדומה.

תמונת הפרופיל מופיעה באתרים נוספים?

לעיתים, נוכלים משתמשים בתמונה שמצאו ברשת האינטרנט. ניתן, באמצעות מנועי חיפוש לתמונות כמו גוגל או TinEye, לבצע חיפוש של התמונה ברשת. אם היא מתגלה גם באתרים אחרים, תחת שמות או הקשרים אחרים, זו נורה אדומה.

"נעבור לווטסאפ?"

בחלק מההונאות באתרי היכרויות, הצד השני מבקש, לאחר שיח קצר באתר, לעבור לערוץ יותר פרטי. כמו ווטסאפ, מסנג'ר, סיגנל או אחרים. זכרו שגם בשיח הפרטי, אתם עדיין לא תמיד יודעים מי עומד בצד השני. לכן, הקפידו לשים לב לכל פרט מחשיד בשיח.

אין עקבות דיגיטליים?

בימינו, כמעט לכל אחד (אלא אם הוא סוכן חשאי) כנראה יש נוכחות מסוימת ברשת. אם תכתבו את שם פלוני או תחפשו את תמונתו, בעברית או אנגלית, משהו אמור לצופ. אם ניסיתם ולא צפץ כלום, תטילו ספק בזהותו של הצד השני.

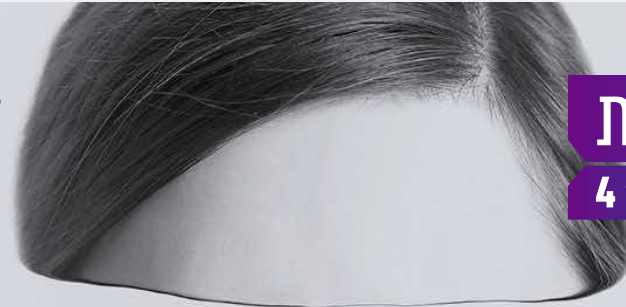


טיפ מודעות

מס' 4

גניבת זהות ברשתות חברתיות

המציאות של ימינו מכתובה נוכחות במרחב הפיזי והווירטואלי. אנו נדרשים "לחיות" בשני העולמות במקביל, באותה זהות. לעיתים, הזהות שלנו הופכת להיות עקב אכילס במרחב הווירטואלי. את הזהות שלנו אפשר לגנוב. כלומר, להתחזות לנו במרחב הווירטואלי באמצעות שימוש בסמנים פיזיים כמו תעודת זהות, דרכון, כרטיס אשראי או באמצעות סמנים וירטואליים כמו הפרופיל בפייסבוק, טוויטר או ווטסאפ. ריכזנו מספר דוגמאות לגניבות זהות נפוצות ואין אפשר להתגונן מפני תרחישים כאלו.



כרטיס אשראי



גניבת זהות יכולה להוביל לשימוש בכרטיס האשראי שלנו. תוקף יכול לבצע חיובים, במדינות שונות, בשמנו, ועל חשבוננו.

כיצד מתגוננים? בודקים את תרשים ההוצאות באשראי כל חודש ומחפשים חיובים מוזרים. אם אפשר להגדיר בחשבון שלנו התראות ב-SMS על חיובי אשראי, כדאי להפעיל. כך נדע בכל פעם שבוצעה עסקה משמעותית בכרטיס.

נפלתם קורבן? התקשרו לחברת האשראי, בטלו את הכרטיס והזמינו חדש. חלופה נוספת היא להשתמש בחו"ל בכרטיס נטען. אם הוא נגנב, לפחות הסכום מוגבל. השתדלו להימנע מכרטיסי דביט, במקרה כזה, כל סכום שיורד מקטין מיידית את היתרה בעו"ש ולוקח זמן לקבל את הכסף חזרה מחברת האשראי. בכל מקרה, מומלץ גם להגיש תלונה במשטרה.

מספר הטלפון הסלולרי



מספר הטלפון הנייד שלנו הוא חד ערכי ומהווה חלק מהזהות שלנו. יתרה מכך, אל מספר זה מגיעות גם הודעות @ **אימות כפול** בניסיון כניסה לחשבון הבנק, הדוא"ל ועוד. תוקפים יכולים לחטוף בעלות על מספר הטלפון (מתקפה הידועה בשם Sim Swap) ולפעול בשמנו. במקרי עבר, תוקפים הצליחו גם לגנוב בעלות על חשבון ווטסאפ של בעל המספר ולהעביר מסרים בשמו.

כיצד מתגוננים? שמים לב לאינטרנט הסלולרי בטלפון. היו ערניים אם פתאום אין חיבור סלולרי לאינטרנט, יש בעיית כניסה לווטסאפ או משהו שחיפש אתכם פונה אליכם בדוא"ל וטוען שאתם לא עונים או שענה לו משהו שאינו מוכר.

נפלתם קורבן? מתקשרים לספק הסלולרי ומדווחים על הבעיה. מומלץ גם להגיש תלונה במשטרה.





מסרים ברשת חברתית

הפרופיל שלנו ברשת חברתית כמו פייסבוק או טוויטר הוא חלק מהזהות שלנו. המסרים שנכתבים יוצאים מפינו. כך רואים זאת אחרים. אם האקר משתלט על חשבון כזה, הוא יכול, באופן מעשי, לכתוב ולהעלות תמונות בשמנו.

ניצד מתגוננים? בודקים לפחות אחת ביום את הפיד האישי שלנו לראות שכל מה שכתוב שם, שלנו. מגדירים אימות דו שלבי כדי לדעת אם מישהו ניסה להתחבר בשמנו. מגבילים בהגדרות הפרטיות את מעגלי התפוצה של ההודעות שלנו. כך אם מישהו יכתוב משהו בשמנו, פחות אנשים יחשפו למסר.

נפלתם קורבן? מדווחים לרשת החברתית (לכל רשת יש הוראות באתר למי לדווח. חפשו בגוגל). רצוי להודיע לכל החברים בווטסאפ (הודעה לכל אנשי הקשר) שהחשבון שלכם נפרץ. כמו גם, מומלץ לכתוב הודעה בפרופיל שיש לכם שליטה עליו ולספר מה קרה. כך

העוקבים שלכם יוכלו לדעת שאין לכם שליטה על חשבון מסוים.



תמונה ופרטים מזהים

אם מישהו משיג תמונה, כתובת ועוד מספר פרטים מזהים, הוא יכול להקים נוכחות ברשת על שמנו. בלוג וחשבון ברשת חברתית הן דוגמאות לפלטפורמות מקוונות בהן מישהו יכול להתחזות אלינו. עבור אנשים שלא מכירים אותנו אישית (מעטים), החשבון יראה לגיטימי והם יחשבו כי מדובר בנו.

ניצד מתגוננים? מפחיתים את חשיפת הפרטים שלנו ברשת ככל הניתן. כתובת מגורים, תמונות, קשרים לבני משפחה, פירוט מקום העבודה והתפקיד, כל אלו יכולים לעזור לתוקף להרכיב פרופיל מזויף, איכותי, שלנו.

נפלתם קורבן להונאה או עקיצה? תעשו בדיק בית אילו חומרים גלויים יש ברשת אודותיכם. זכרו: אפשר למחוק את הפרופיל שלכם בכל רשת חברתית ולבנות אחד חדש "נקי". אם יש לכם אלבומי תמונות חשופים לכל אחד

- שנו את הגדרות הפרטיות. אם יש לכם בלוג, תראו שאתם לא חושפים שם יותר מידי פרטים אישיים. אם גיליתם שמישהו פתח פרופיל מתחזה עם פרטיכם - דווחו לרשת החברתית על הפרופיל.

איך אפשר להמנע מחטיפת זהות?

באופן כללי, ניתן לומר כי הפושעים מנצלים את המידע הגלוי אודותינו על מנת להתחזות לנו, וככל שיש יותר מידע כזה בנמצא, כך התוקפים מצליחים יותר.

תמיד צריך לחשוב איך הצד השני יכול לנצל את מה שאני עושה, וזה תמיד מסתכם בפרטים הקטנים: בהודעת הדוא"ל שקיבלתם משולח לא ידוע עם קישור זדוני. מהצד השני שראית תמימה ומכילה **8 נזקה.** מהסיסמה '123456' שקל לנחש. מהמודעה ששלחה אתכם לטופס מילוי פרטים ועוד.

בשביל להקשות על התוקף להתחזות לנו, אנו נדרשים להטיל ספק בריא בכל פעולה שאנו מבצעים ברשת, בכל שיתוף של תמונה, וידאו או כל פרט אישי אחר. ככל שנקפיד על כללי התנהגות בסיסיים בסייבר, כך התוקף יתקשה לשכנע אחרים בזהות השאולה.





ייחודית לנתב.

מיקום המצלמה

מומלץ להציב את המצלמות במקום שיצמצם את הפגיעה בפרטיות במקרה של פריצה.

כיסוי עינית המצלמה

כשאינן במצלמה צורך, מומלץ לנתק או לכסות אותה פיזית.

המצלמה והקפידו לבחור יצרנים ידועים. התקנת מוצרי תוכנה צד שלישי יכולה לחשוף את המחשב שלכם ל**לנוזקות**.

עדכוני תוכנה

כמו במערכות הפעלה ותוכנות אחרות, כך גם צריך לעדכן את התוכנה של המצלמה. עדכוני תוכנה מכילים לרוב תיקוני אבטחה אשר מעלים את רמת ההגנה של המוצר מפני תקיפות ומומלץ לבצעם עם הוצאתם בהתאם להמלצת היצרן.

וידוא ההגדרות

לאחר כל עדכון תוכנה, ביקור טכנאי/ת, טיפול או שדרוג יש לוודא שההגדרות או הסיסמאות לא שוננו או הוחזרו לברירת המחדל.

נתב ביתי

פריצה למצלמות האבטחה יכולה להתאפשר גם באמצעות הנתב הביתי. מומלץ לשנות את שם הרשת כך שלא יעיד על מאפייני הנתב כגון דגם, יצרן, בעלים ומיקום, ולהגדיר סיסמה

לצד היתרונות בטכנולוגיה זו, סיכון הסייבר שהן מהוות גובר.

מצלמות ביתיות הן אמצעי נפוץ היום לבקרה על הנעשה בבית, בעסק ואף בגני ילדים, אך הן לרוב מגיעות עם סיסמת ברירת מחדל שידועה לכל. מעבר לפגיעה בפרטיות, ההשתלטות על המצלמה מאפשרת הקלטת מידע ושמירת תמונות למטרות של גניבת נתונים, שיבושם, התחזות ואף סחיטה. באמצעות הפריצה למצלמה ניתן לראות מי נמצא בבית ומתי, תכולת הבית, שגרת היום ומידע נוסף שפוגע בפרטיות.

אז כיצד מתמודדים? אספנו עבורכם מספר עצות להקטנת הסיכון

החלפת סיסמת ברירת המחדל

בחרו סיסמה קשה לפיצוח עבור מצלמות האבטחה והן עבור הנתב הביתי.

התקנת מוצרי תוכנה של יצרן המצלמות

העדיפו להתקין תוכנות ניטור מבית יצרן



טיפ מודעות

מס' 5

האיום המצולם - מצלמות רשת ביתיות חשופות לתוקפים

מצלמות אבטחה ביתיות הפכו להיות מוצר שגור בבתיים של כולנו. שמירה על תינוקות בזמן שינה, שמירה על הבית בזמן חופשה בחו"ל או כאמצעי ניטור אבטחתי בלובי של הקומה או הבניין. אמצעים שהיו בעבר נחלתן של חברות אבטחה מקצועיות בלבד, הפכו להיות זמינים לכל אחד מאיתנו, כולל חיבור לחשמל ושידור אלחוטי לכל טלפון סלולרי או מחשב נייד.

חשוב לציין כי קישורים מקוצרים אינם תמיד זדוניים. פעמים רבות הם משמשים עבור מעקב אחר נתונים או מתוך רצון לייצר קישור קצר ונוח לשימוש. אם אינכם בטוחים, תוכלו תמיד לחפש את זהות השולח ולהיכנס באופן יזום לאתר שלו, במקום לחיצה על הקישור.

והוסיפו את המילה "Preview" לפני הקישור המקוצר לדוגמה: <https://preview.tinyurl.com/y62ova> לחיצה על Enter תוביל אתכם לאתר Tinyurl שיציג בפניכם את הקישור המקורי.

Cut.ly - העתיקו את הקישור

הוסיפו את התו @ בסוף הקישור, לדוגמה:

[@https://cutt.ly/vTLisiH](https://cutt.ly/vTLisiH), לחיצה על Enter תוביל אתכם לאתר Cut.ly שיציג בפניכם את הקישור המקורי.

Tiny.cc - העתיקו את הקישור

שימו לב שאתם מעתיקים ולא מקליקים על הקישור. הדביקו את הקישור בשורת ה-URL ובסוף הכתובת הוסיפו את הסימן "=" לדוגמה: <http://tiny.cc/2lvuz=> לחיצה על Enter תוביל אתכם לאתר Tiny.cc שיציג בפניכם את הקישור המקורי.

אז כיצד מתמודדים עם קישורים מקוצרים? להלן מספר פעולות אותן תוכלו לבצע

חלק משירותי קיצור הקישורים מציעים דרך פשוטה יחסית להבין מה הקישור האמיתי מאחורה. בנוסף, תוכלו להשתמש בשירותים מקוונים ייעודיים לבדיקת קישור. ביניהם, getlinkinfo.com, unshorten.it ו-urlxray.com.

Bit.ly - העתיקו את הקישור

שימו לב שאתם מעתיקים ולא מקליקים על הקישור. הדביקו את הקישור בשורת ה-URL ובסוף הכתובת הזינו את התו "+" לדוגמה: <https://bit.ly/3kTf2YL>, לחיצה על Enter תוביל אתכם לאתר bit.ly שיציג בפניכם את הקישור המקורי.

Tinyurl - העתיקו את הקישור

שוב, שימו לב שאתם מעתיקים ולא מקליקים על הקישור. הדביקו את הקישור בשורת ה-URL

טיפ מודעות

מס' 6



קצרים, ויכולים לגרום נזק גדול

קישורים מקוצרים הפכו נפוצים בשנים האחרונות בשל יכולתם להפוך קישור ארוך ומסורבל לקצר ונוח. הקישור המקוצר פשוט יותר לשיתוף, מאשר קישור ארוך שיכול להכיל מאות תווים. הוא גם מאפשר לבעלי אתרים מעקב אחר נתונים שונים כגון מספר הלחיצות על הקישור.

לצד היתרונות שיש לקישורים המקוצרים, ניתן להשתמש בהם גם לפעולות זדוניות. לעיתים, גורמים עוינים עושים שימוש בקישורים מקוצרים על מנת להסתיר את הקישור האמיתי המסתתר מאחור. לחיצה על הקישור האמיתי תוביל לאתר מזויף או מתחזה לכריית פרטים אישיים או להורדת תוכן זדוני להתקן המחשב.



טיפ מודעות

מס' 7

ריגול או נוחות - סיכוני סייבר במכשירים לבישים

מכשירים לבישים מציבים איומים פוטנציאליים על אבטחת המידע של ארגונים, מכיוון שככל שהם הופכים קטנים יותר, פחות נראים ועם יותר יכולות, קשה יותר לראות אותם ולקוב אחריהם. מכשירים אלו כוללים, לעיתים, את המידע הכי רגיש שלנו - רפואי, פיננסי, משפחתי. לעיתים מכשירים אלו משמשים לשמירת מסמכים רגישים.

סיכוני הסייבר מצד מכשירים אלו מגוונים. ישנו סיכון לנתונים המועברים באמצעותם. בזווית התוכנה, היצרנים לא תמיד מפרסמים עדכוני אבטחה תקופתיים. דליפות מידע ממכשירים אלו יכולות לגרום לחברות לעמוד בפני תביעות ייצוגיות, קנסות יקרים ופגיעה במוניטין שלהן.

**האם אנו, המשתמשים,
יכולים להגן על עצמנו
מפני איומי סייבר
מצד מכשירים לבישים?**

טכנולוגיה לבישה (טכנולוגיה המאפשרת להטמיע אמצעים טכנולוגיים, כמו חיישנים, מצלמות ומסכים בפריטי לבוש וגאדג'טים שאנו עושים בהם שימוש יומיומי כמו בגדים, משקפיים, נעליים, שעונים ועוד) מניעה כמה חידושים מדהימים במיזוג עולמות פיזיים ווירטואליים כדי לשפר כל הבט בחיינו, החל בקניות דרך שירותי בריאות וכלה בביצועים אתלטיים. אבל הטכנולוגיה היא חרב פיפיות. יכולות חדשות גם פותחות את הדלת לאמצעי תקיפה חדשים.



הגבילו את מה שאתם משתפים באמצעות המכשיר. רוב הציוד הלביש לא צריך גישה לכל פיסת מידע עליכם. אם אתם נכנסים לפעילות אינטימית, פגישה רגישה, ביקור אצל רופא או מיקום סודי, הסירו את המכשירים הלבשים והשאירו אותם ברכב. אם אתם רוצים שלא יעקבו אחריכם למיקום מסוים - השאירו אותם בבית.

לסיכום, זכרו שבכל מכשיר לביש קיים פוטנציאל למכשיר ריגול. כזה שיכול לשדר את המיקום והנתונים שלכם לצד ג', בלי שאתם יודעים מכך. התנהגו בהתאם. לבשו את המכשיר רק כאשר אין סיכון בנוכחותו. הכירו את המכשיר והגדירו אותו בהתאם לצרכים שלכם. לימדו את סיכוני הסייבר הטמונים במכשיר.

אין ספק כי מכשירים לבישים יכולים לשפר לנו את החיים, השאלה באיזה מחיר.

כאמור, עלינו להכיר את הגדרות המכשיר. אם יש אפשרות להגן עליו בסיסמה או בקוד - עדיף להפעיל ולקבוע סיסמה חדשה, אישית, במקום זו שהגדיר היצרן. במידה והמכשיר מתחבר לרשת אלחוטית, יש לחבר אותו רק לרשתות מוגנות בסיסמה. רשתות ציבוריות פתוחות יכולות להוות סיכון לדלף מידע. אם המכשיר מתחבר לרשת אלחוטית (תקן פתוח הנועד לחבר התקנים חיצוניים למחשב ללא כבלים, אלא על גבי תקשורת רדיו), יש לוודא שהוא עבר התאמה רק להתקן מחשוב בבעלותנו.

אם קיימת אפשרות להצפין את נתוני המכשיר, יש להפעיל אותה. במידה ואפשר לעדכן את תוכנת המכשיר, באופן ישיר באמצעות חיבור לרשת או דרך חיבור למחשב נייד או שולחני – יש לבצע זאת כל תקופה מוגדרת. רצוי לעדכן גם את מערכת ההפעלה בהתקן המחשוב ממנו מתחברים למכשיר הלביש. באותו התקן, רצוי שיותקן גם מוצר אבטחת מידע כמו אנטי וירוס.

ובכן, אחריות האבטחה על מכשירים אלו מתחלקת בין ספקי הרכיבים, היצרן והמשתמש. בעוד השניים הראשונים אינם בשליטתנו, כמשתמשי קצה אנו יכולים לבצע מספר פעולות שיכולות להפחית סיכון למתקפת סייבר או דלף מידע נגד המכשירים הלבשים שלנו.

ראשית, עלינו לקרוא על המכשיר שאנו רוצים לרכוש או להשתמש בו. מחקר מקדים ברשת האינטרנט, כולל קריאת סקירות עליו, יכול לחשוף בעיות אבטחה ידועות וגם לבאר מהן הגדרות האבטחה או הפרטיות הכלולות במכשיר. בנוסף, במידה וישנה אפשרות בחירה, רצוי לבחור יצרן ידוע עם תמיכה נגישה (אתר מסודר, מוקד טלפוני, צ'אט) ובשפה ידועה. מחקר בשלב הרכש יפחית הרבה בעיות בהמשך.



תמיד לפתוח דפדפן, להקליד את שם נותן השירות ולגלוש ליעדכם בצורה זו. בנוסף, אל תמסרו פרטים לאף אחד שמתקשר אליכם ולא משנה איך הם מציגים את עצמם או מה המספר שמופיע על צג הטלפון אלא אם אתם בטוחים ב 100% בהותם. אם אינכם בטוחים, העדיפו לחפש את המספר של הספק / נותן השירות בגוגל ולהתקשר אליהם ישירות.

נוזקות

נוזקה היא קוד זדוני המאפשר להאקר לבצע פעולות במחשב הקורבן ללא ידיעתו או הסכמתו. ישנם סוגים שונים של קוד זדוני. חלקם נועדו לגנוב מידע. חלק מתעדים את ההקשות על המקלדת, למשל, כאשר מזינים את פרטי כרטיס האשראי באתר סחר מקוון או באתר הבנק.

הודעות דיג הן אחת השיטות הנפוצות להפצת נוזקות. מודעות מקוונות הן דרך נוספת. במקרים אחרים, הפושעים עלולים להדביק אתרים פופולריים לגיטימיים ולהמתין שגולשים יבקרו בהם ויכנסו לדף מסוים באתר. פושעי סייבר גם נוטים להסתיר נוזקות בתוך אפליקציות המתחזות ללגיטימיות.

פשינג

דיוג (Phishing) או פשינג היא אחת הטכניקות הנפוצות ביותר לגניבת נתונים. ככלל, זוהי תרמית, שבה ההאקר מתחזה לישות לגיטימית (כמו בנק, אתר מסחר או חברה טכנולוגית) כדי לשכנע את הקרבן למסור פרטים אישיים או להוריד **נוזקות**. במרבית המקרים האקרים מעודדים את המשתמשים ללחוץ על קישור או להוריד קובץ מצורף בהודעת דוא"ל.

לעיתים הלחיצה הזו מובילה את המשתמש לדף מתחזה - בו ינסו לגרום לו להזין פרטים אישיים ופיננסיים. כיום מתקפות אלו כוללות גם הודעת SMS זדונית לחברת שליחויות, רשות ממשלתית או כל ארגון אחר. וקטור נוסף הוא מתקפות דיג קוליות (**Vishing**).

כיצד מתמודדים? הימנעו מלחיצה על קישורים או הורדת צרופות בהודעות בדוא"ל או ב SMS. במקרים של קישורים, העדיפו

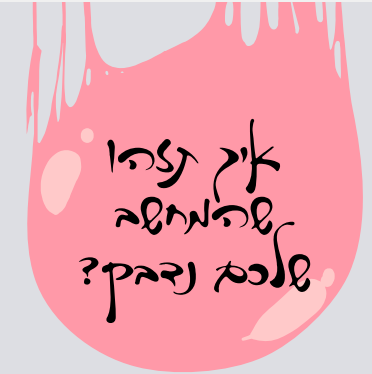


טיפ מודעות

מס' 8

חמש דרכים באמצעותן גונבים לכם את האשראי - וכיצד ניתן למנוע אותן

רובנו רוכשים מידי פעם מוצר או שירות ברשת באמצעות כרטיס האשראי. ובכן, לצד היתרונות כמו נוחות, זמינות ומהירות הטמונים בכך, ישנם לא מעט איזמים במרחב הסייבר שעלולים לגרום לנו לנזק. העיקרי בהם הוא האיום שמישהו יגנוב לנו את פרטי כרטיס האשראי. על פי חברת אבטחת המידע ESET ישראל, אלו הדרכים הנפוצות בהן האקרים גונבים כרטיסי אשראי:



- ! הייתה תקלה במחשב ובעקבותיה קיבלתם שגיאה על מסך כחול ("מסך כחול")
- ! המחשב התחיל לעבוד באיטיות שאינה אופיינית לו
- ! הגלישה שלכם איטית, לא משנה באיזו רשת אתם גולשים
- ! יישומים נפתחים באופן עצמאי
- ! הסמן של העכבר זז בלי שהזזתם אותו
- ! גיליתם יישומים חדשים שלא אתם התקנתם

- ! בזמן גלישה נפתחים לכם חלונות/טאבים באופן אוטומטי או שקופצים לכם הרבה פופ-אפים במסך
- ! נוספו לדפדפן שלכם תוספים שאתם לא זוכרים שהתקנתם
- ! תוכנת האנטי וירוס שלכם מנותקת ואי אפשר להפעילה מחדש
- ! קיבלתם דוא"ל / SMS מוזר או חשוד ופתחתם את הצרופה / לחצתם על הקישור
- ! חברים שלכם מקבלים מכם פרטי דוא"ל שלא שלחתם

ניצד מתמודדים? הטלת ספק היא הנשק הטוב ביותר של המגן:

- 👍 קיבלתם הודעה? ביקשו מכם לעשות משהו? עצרו. בררו את זהות הצד השני. חפשו את ההיגיון בהודעה.
- 👍 המחשב מתנהג מוזר? נתקלתם במשהו חשוד? דווחו מייד לאבטחת המידע.

👍 בנוסף, התקינו מוצרי אבטחת מידע, ועקבו אחר החיובים בחברת האשראי.

קצרה דיגיטלית

לעיתים האקרים יתקינו נוזקות בדפי התשלום של אתרי סחר מקוון. המשתמש לא יכול לראות את הנוזקות האלו, אך לאחר התקנתן, אלו יקצרו את פרטי כרטיס האשראי ברגע שמכניסים אותם במקום ייעודי באתר. אחת הדרכים להתמודד עם תופעה זו היא לרכוש מאתרים ומותגים גדולים, שככל הנראה, מאובטחים יותר.

ניצד מתמודדים? רכשו רק באתרים מהימנים המוכרים שלכם ועקבו אחרי החיובים שלכם בחברת האשראי.

דליפות מידע

לעיתים, פרטי כרטיסי האשראי נגנבים ישירות מהחברות שאיתן עושים עסקים. זה עלול להיות ספק שירותי בריאות, חנות מקוונת או סוכנות טיולים. מנקודת המבט של ההאקר, זוהי דרך יעילה יותר לגנוב פרטי אשראי, מכיוון שבמתקפה אחת הם מקבלים גישה לכמות עצומה של נתונים.

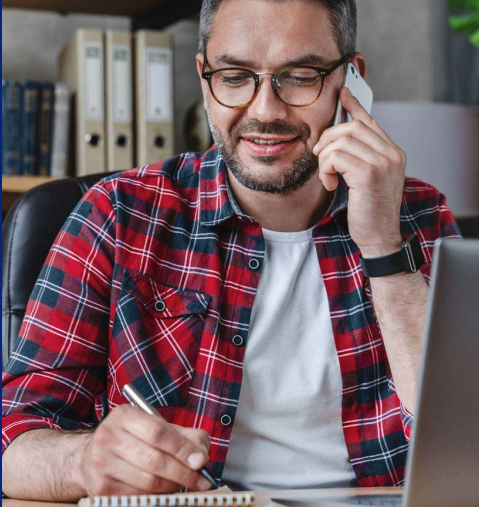
ניצד מתמודדים? היו ערניים להודעות מספקי שירותים המבקשים מכם פרטים אישיים או כאלו הכוללות קישורים או צרופות. קיבלתם הודעה בדוא"ל מספק שירות? העדיפו להתקשר למוקד השירות שלו ביוזמתכם ולשאל לפרט ההודעה.

רשתות אלחוטיות ציבוריות

בנמלי תעופה, מלונות, בתי קפה ומרחבים משותפים נוספים, ישנן רשתות אלחוטיות ציבוריות. תיירים, סטודנטים ולקוחות נוטים להשתמש ברשתות אלו לצרכי עבודה וצרכים אישיים. עם זאת, רשתות ציבוריות אלו, בין אם ניתנות בחינם או בתשלום, אינן מאובטחות ואיננו יודעים מי חשוף לנתונים העוברים בהן. האקרים מנצלים רשתות אלו כדי להגיע למידע.

ניצד מתמודדים? מומלץ להשתמש ברשת הסלולרית בטלפון (נקודה חמה) או ב-VPN שמגן על הפרטיות שלנו ברשת במיוחד כאשר אתם גולשים לאתרים רגישים כמו לחשבון הבנק שלכם.



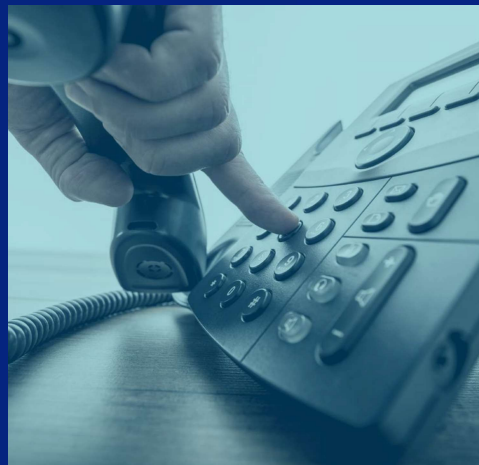


שיחות טלפון קווי

שיחות מטלפון קווי נחשבות למאובטחות יחסית מכיוון שהתוקף צריך להתחבר לתשתית ספק התקשורת כדי להאזין להן. ספקי תקשורת הם לרוב גופים בעלי ממון המשקיעים באבטחת מידע יותר מעסק ממוצע. מתקפות כאלו קשה מאד לאתר ללא ציוד מתאים. במידה וניהלתם שיחת טלפון פרטית וגיליתם שצד שלישי יודע את פרטיה, התחילו לחשוד. במידה ומתעורר חשד, רצוי להזמין אנשי מקצוע שיבדקו האם מאזינים לכם לקו הטלפון.

תקשורת סלולרית

כאשר אנו מדברים בטלפון הסלולרי, החיבור בין הטלפון לרשת הסלולר מתבצע לתא הסלולרי הקרוב לטלפון וזה שמשרד בהספק הגדול ביותר. פושעים יודעים להשתמש בתאים מזויפים, כאלו המתחזים לתא סלולרי לגיטימי, על מנת לבצע מתקפת MITM. אחת הדרכים להתמודד עם סיכון זה היא לקיים שיחה מוצפנת בשירות כמו ווטסאפ או סיגנל. כך, גם אם מישהו מאזין לשיחה, היא מוצפנת.



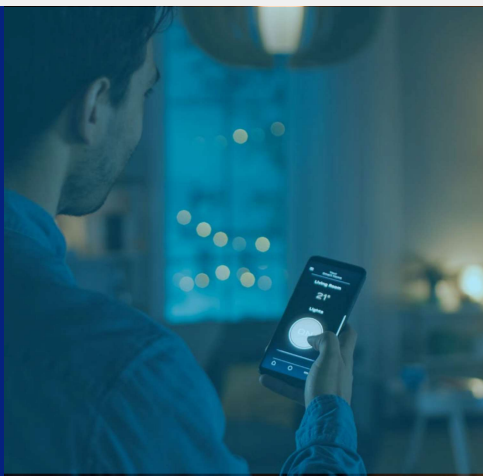
טיפ מודעות



מס' 9

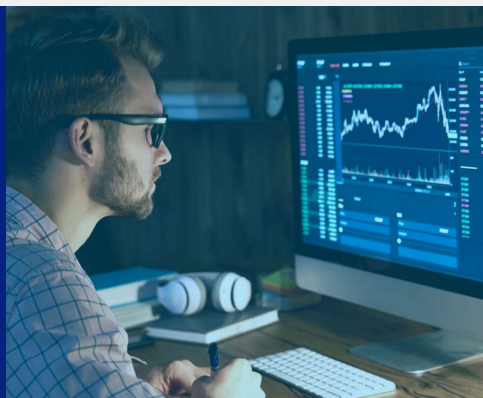
כך האקרים מנטרים את המידע שלכם - בלי שאתם יודעים

דמיינו שיחת טלפון שאתם מבצעים עם חבר או בן משפחה ומישהו שלישי, שאינכם מודעים לקיומו, מקשיב לשיחה. עכשיו, קחו את הדוגמא הזו לכל סוג תקשורת המשלב קול או נתונים. פעולה זו נקראת מתקפת Man-in-the-middle או בקיצור **MITM** - מתקפה שבה התוקף מצליח לנטר ולהאזין לתקשורת בין שני צדדים ללא ידיעתם. להלן סוגים אפשריים של מתקפות MITM וכיצד מתמודדים עימן:



דליפת מידע

האם דליפת מידע מארגון נחשבת למתקפת MITM? ובכן, במתקפה כזו פושע פורץ לארגון עימו ניהלנו תקשורת. אותו ארגון מחזיק בנתונים אודותינו שאמורים להיות חשופים רק לו והנה, עכשיו הם חשופים גם לצד שלישי. אמנם ניטור הנתונים לא בוצע בזמן אמת במהלך השיחה או העברת הנתונים, אך נעשה באופן א-סינכרוני. כלומר, אנחנו העברנו נתונים לצד השני והפושע פרץ אליו וגנב אותם במועד מאוחר יותר. כיצד מתמודדים? בעיקר יש לעקוב אחרי המקומות עמם אנחנו משתפים את המידע שלנו. במידה ואין צורך בשמירת הנתונים שלנו בצד השני, רצוי לבקש ממנו שימחק אותם אצלו.



העברת נתונים בין מחשבים

מתקפות MITM אפשריות גם בהעברת נתונים. כאשר המחשב שלנו בבית מחובר ברשת למחשבים אחרים או מחובר לרשת האינטרנט, פושע יכול לנטר את הנתונים היוצאים ונכנסים אליו. הנתונים הללו, אם אינם מוצפנים, יכולים לספק לפושע מידע רב. כולל מידע טכני על המחשב והרשת שלנו בבית ועד תוכן המידע העובר ברשת. למשל, תוכן הודעת דוא"ל ששלחנו למישהו. הדרך להתמודד עם סוג זה של מתקפה היא לעבוד עם תקשורת מוצפנת באמצעות שימוש בכלים כמו **VPN**.



שיחה בעל פה

מתקפת MITM נכונה גם לשיחות בעל פה שאנחנו מנהלים בעמדת הקפה בעבודה או בבית קפה עם חבר או לקוח. במצבים כאלו, אנשים סביבנו יכולים להאזין לדברים. כמו גם, פושעים מקצועיים יכולים להשתמש במיקרופון מיוחד המאפשר להם להאזין לשיחות גם ממרחק. הדרך להתמודד היא לדבר במקום רועש ולהקשות על אחר להבין מה נאמר. דרך נוספת היא לבחור מקום מבודד לנהל בו שיחה רגישה.

האיש ב- Internet Of Things (IoT)

פורץ יכול להשתלט או ליירט מידע מהתקנים חכמים בבית כולל הטלוויזיות, תרמוסטטים, מקררים, קומקומים, מכונות ושלל אביזרים אחרים שלכם אשר מתחברים לאינטרנט. יש לזכור כי כל אביזר המתחבר לאינטרנט הוא מטרה מצוינת וניתן לשלוף את אמצעי הזיהוי שלכם גם מהמקרר שלכם או מהקומקום החשמלי. איך מתמודדים? הקפידו להגדיר שם וסיסמה נפרדים לכל התקן, כמו גם, במידה ונדרש רישום לשירות IoT, הגדירו כתובת דוא"ל נפרדת לכל שירות.



מה ניתן ללמוד מהמקרה?

מתקפות **פשינג** נפוצות מאד והן, לרוב, ערוץ הכניסה הראשוני של התוקף למחשב של הקורבן. קיבלתם קישור בהודעה? העדיפו להקליד את הכתובת ידנית בשורת החיפוש בדפדפן מאשר ללחוץ עליו. כמו כן, הימנעו מהשארת פרטים אישיים באתר שאינו מוכר. בנוסף, הקפידו לבדוק תקופתית את הגדרות תיבת הדוא"ל שלכם. אילו חוקים מוגדרים בה? האם יש תיקיות שאנחנו לא מכירים? כנסו לתיבת הדואר שנשלח ולפח האשפה וראו אם אין שם תכתובות חשודות.



מקור: MICROSOFT.COM

לדוא"ל שלהם במקום העבודה. כל הפרטים הללו הגיעו לידי התוקפים.

בשלב השני התוקפים חיפשו תכתובות בדוא"ל של מקום העבודה הקשורות לנושאים פיננסיים. כאלו שאפשר להשתמש בהן להונאות פיננסיות. ברגע שמצאו אחת כזו, הם השתלטו על התכתובת עם הצד השני וענו בשם הקורבן. זאת, על מנת לגרום לצד השני להעביר להם כספים (הונאה הידועה כ-**BECC**). האתגר בהונאות פיננסיות הוא לצור אמון עם הצד השני. במקרה זה, התוקף השתלט על תכתובות קיימות בין הקורבן (בעל תיבת הדוא"ל) לבין הצד השני (הקורבן הפוטנציאלי של ההונאה הפיננסית). כאשר הצד השני קיבל את ההודעות, הוא חשב שאלו לגיטימיות ומגיעות מבעל תיבת הדוא"ל. הוא לא חשד שתוקף עונה בשם בעל התיבה. כדי להסתיר את הפעולות שביצעו בתיבת הדוא"ל של הקורבן, התוקפים הגדירו חוק חדש בתיבה. עבור כל הודעה נכנסת המכילה כתובת שולח (שם הדומיין של יעד ההונאה), העבר את הדואר לתיקיית "ארכיון" וסמן אותו כ"נקרא". בצורה כזו, התוקפים חשבו להסתיר את המשך התכתובות עם הצד השני. בסוף התהליך, הם מחקו גם את ההודעות המסוימות מתיבת דואר נשלח ומפח האשפה כדי לא להשאיר עקבות במחשב הקורבן.

מדובר במתקפה גדולה שכוונה נגד כ-10,000 עסקים. לא ברור מהפרסום של מיקרוסופט כמה הונאות פיננסיות הצליחו בפועל בשיטה זו או כמה כסף נגנב.

טיפ מודעות



מס' 10

לחיצה על קישור תמים גרמה להונאה פיננסית של למעלה מ-10 אלף עסקים

נכון תמיד מספרים לכם שאם לא תשמרו על הדוא"ל הפרטי שלכם, יהיה אפשר להשתמש בו כדי לפרוץ למעסיק שלכם? זה בדיוק מה שקרה במחקר של חברת מיקרוסופט בו נחשפו תקיפות פיננסיות כנגד ארגונים רבים ברחבי העולם. במקרה המדובר, התוקפים שלחו לעובדי החברה דוא"ל פשינג עם קישור זדוני. עובדי החברה לחצו על הקישור, הופנו לאתר מתחזה ושם השאירו את שם המשתמש והסיסמה

