מדריך פעולה לשיקולי אבטחה אישית: עובדי תשתיות קריטיות

מבוא

בסביבת האיומים הנוכחית של היום, שמירה על ערנות ולקיחת אחריות על הביטחון האישי שלכם הן חיוניות עבור כל עובדי התשתיות הקריטיות - גם בעבודה וגם מחוצה לה. עובדי תשתיות קריטיות מבצעים מגוון עצום של שירותים המפעילים ומתחזקים מערכות מפתח ונכסים הנחוצים לחיים האמריקאיים המודרניים. תשומת לב לכל הסיכונים או האיומים הקשורים לתחום העבודה שלכם וביצוע כל נהלי הבטיחות יסייעו להגן עליכם, על קרוביכם ועל התשתית שאתם משרתים. ניתן לחלק את הביטחון האישי לשלושה חלקים עיקריים - אבטחה פיזית, מודעות למצב ואבטחה מקוונת. מדריך פעולה בלתי ממצה זה יכול לעזור לכם להעריך את מצב האבטחה שלכם, והוא מספק אפשרויות שעליכם לשקול כדי להפחית איומים[1]

הערכת רמת ההגנה המתאימה לעובדי תשתיות קריטיות

מדריך זה מספק סקירה רחבה של דרכים לשמירה על הביטחון בבית, בעבודה, בציבור ובאינטרנט. אתם האחראיים להחלטה אילו אמצעים מתאימים ביותר לאורח החיים שלכם, לנקודות תורפה ביטחוניות ולמצבים שבהם אתם עלולים להיתקל - לדוגמה, גורמים מסוימים עלולים להגביר את הפוטנציאל לאלימות במקום העבודה:

- **עבודה לבד** או באזורים מבודדים.
- **מתן שירותים או טיפול** באופן אישי.
- **עבודה עם חומרים מסוכנים** או עם מידע רגיש הקשור לביטחון לאומי.
- **אחריות להגנה** על תשתיות קריטיות מקומיות או לאומיות.

בעת הערכת צורכי האבטחה שלכם, קחו בחשבון את הדברים הבאים:

- **העיסוק והתפקיד המקצועי שלכם.** האם העבודה או הקריירה שלכם הופכים אתכם ליעד אטרקטיבי?
- **איומים ספציפיים.** האם קיימות ראיות מהימנות המעידות על סיכון עבורכם?
- **ההיסטוריה האישית שלכם.** האם חוויתם רדיפה או איומים בעבר?
- **המזהים החזותיים האישיים שלכם.** האם אתם מפגינים השתייכות לקבוצה שהופכת אתכם ליעד אטרקטיבי?

כיום, עובדי תשתיות קריטיות עלולים להתמודד עם מגוון רחב של איומים - החל מפעילות פלילית שכיחה וכלה במזימות אלימות מצד גורמים קיצוניים. אם עניתם בחיוב על אחת מהשאלות שלעיל או על כולן, הדבר יכול להצביע על כך שאתם ועובדי תשתיות קריטיות אחרים שאיתם אתם עובדים נמצאים בסיכון, ושעליכם להעריך את צורכי האבטחה שלכם. בבואכם להעריך את הביטחון האישי שלכם, חשוב לנקוט בגישה מאוזנת ולזכור לתת את הדעת על חיי הבית והעבודה שלכם - **היו ערניים להרגלי האבטחה האישיים שלכם, והעריכו את סביבתכם באופן מתמשך**. האמצעים שאתם נוקטים צריכים להתאים לאיומים הנתפסים. פעולות אבטחה מופרזות עלולות לגרום ללחץ ואי נוחות מיותרים; עם זאת, מאמצים שאינם מספקים עלולים לסכן אתכם.

היכולת לזהות מצבים של פגיעות הינה חיונית להימנעות מהם או למוכנות אליהם עם התרחשותם. פגיעות היא תכונה פיזית או תפעולית אשר הופכת ישות, נכס, מערכת, רשת או אזור גאוגרפי לחשופים לניצול או לרגישים למפגע נתון.[2] תוקפים יכולים להפגין יצירתיות כאשר הם מתמקדים ביחידים. מטרתו של תוקף עשויה להיות לגרום מבוכה, אי נוחות או מצוקה, או שהוא עשוי להתכוון לגרום לפציעה פיזית, לשיבוש הרווחה או לאיום על חיי אדם.

1 ProtectUK. 2022. הנחיות למקומות נגישים לציבור (PAL): ביטחון אישי. הגישה בוצעה ב-8 באוגוסט 2023. protectuk.police.uk/personal-security.

2 המחלקה לביטחון המולדת של (Department of Homeland Security) ב"הרא. ועדת היגוי סיכונים. 2010. לקסיקון הסיכונים של ה-DHS (המחלקה לביטחון פנים), מהדורת 2010. הגישה בוצעה ב-8 באוגוסט 2023. cisa.gov/resources-tools/resources/dhs-risk-lexicon.

אבטחה פיזית

הגנה על ביתכם

קיימים מגוון אמצעים פשוטים שתוכלו לשקול, שיכולים לעזור להגן עליכם ועל ביתכם. התחילו בהתקנה או שיפור של מערכות אבטחה המקיפות את המגורים או הנכס שלכם. אבטחו את כל הדלתות או החלונות במנעולים, מפתחות, אזעקות ותאורה, והעריכו את הצורך במערכת טלוויזיה במעגל סגור (CCTV). שקלו להשתמש במערכת נעילה מתקדמת לדרכי כניסה ולחלונות עם מערכת מעקב וידאו מנוטרת (עם יכולות של ריבוי זוויות ראייה).

תחזקו את מבני הנכס החיצוניים, כמו קירות וגדרות, וודאו שכל הכלים או הסולמות שניתן להשתמש בהם כדי לגשת לביתכם מאוחסנים בצורה מאובטחת. שקלו להסיר כל דבר שיכול לשמש לגרימת נזק, כגון לבנים רופפות, אבנים גדולות וקישוטי גינה. הקפידו לגזום ולתחזק שיחים, עשבים שוטים וכדומה, כך שהעלווה:

- **לא תוכל לשמש** פולשים לצורך מסתור או גישה לבית.
- **לא תחסום** את הנוף החיצוני מאלה שבתוך הבית.

אבטחו דלתות וחלונות חיצוניים בהתקני נעילה מתאימים, שיכולים לכלול מנגנוני נעילה אלקטרונית. עדיף להחזיק סט נוסף של מפתחות או קודי כניסה לשימוש בזמן חירום. שקלו להחליף את כל מערכת הנעילה במקרה של חשיפת קודי הכניסה או אובדן המפתחות.

השקיעו בהתקנה ותחזוקה של תאורה חיצונית המאירה דלתות חיצוניות, אזורי חניה ושבילים ברחבי הבית. שקלו להתקין מצלמות הצופות על דלתות וחלונות. מקמו את האורות והמצלמות הללו באופן אסטרטגי, כדי לחסל כל שטח מת שבו אנשים יכולים להתחמק מגילוי.

אם יש לכם רכב, ואינכם יכולים לאבטח אותו בחנייה מקורה או באזור נעול, נסו להשאיר אותו במקום החשוף לעיני כול. חנו באזור מואר היטב, בשטח המכוסה במצלמת טלוויזיה במעגל סגור או בחניון עם שמירה. הקפידו לסגור את החלונות, להצניע חפצי ערך ולנעול את הרכב שלכם, גם אם אתם מתרחקים רק לכמה דקות. הבינו כיצד להשתמש בסוג מערכת האזעקה למניעת גניבה הקיימת ברכבכם. ישנן מערכות הכוללות התראות קוליות וחזותיות, בנוסף לשירותי איתור רכבים, המסייעים בזירוז תגובת המשטרה.

תכנון מראש

שקלו לפתח תוכנית פעולה משפחתית למקרי חירום ולתרגל מה לעשות במקרה חירום. לקבלת עזרה בפיתוח תוכנית, בקרו בכתובת:

.fema.gov/blog/have-emergency-plan-your-family

פיגועי ירי

יורה פעיל מוגדר כאדם אחד או יותר העוסקים באופן פעיל בהרג או בניסיון להרוג אנשים באזור מאוכלס.[3] תקריות יורה פעיל הן לרוב בלתי צפויות ומתפתחות במהירות. בתוך הכאוס, כל אחד יכול למלא תפקיד אינטגרלי בהפחתת ההשפעות של תקרית יורה פעיל.

מכיוון שמצבים של יורה פעיל מסתיימים לעתים קרובות תוך 10 עד 15 דקות - לפני הגעת גורמי אכיפת החוק לזירה - עליכם להיות מוכנים הן נפשית והן פיזית להגיב לתקרית יורה פעיל.

בתקרית של יורה פעיל, שקלו ליישם אסטרטגיית תגובה מתורגלת - כגון פרדיגמת ה'רוץ, התחבא, הילחם" (Run, Hide, Fight) - בהתאם למדיניות האבטחה של הארגון שלכם. מידע ומשאבים נוספים ניתן למצוא בדף הבית של CISA (הסוכנות לאבטחת סייבר ותשתיות) עבור מוכנות ליורה פעיל.

אש כנשק

הצתה מוגדרת ככל שריפה מכוונת או זדונית או ניסיון לשרוף - עם או בלי כוונה להונות - בית מגורים, מבנה ציבורי, רכב מנועי, כלי טיס או רכוש אישי אחר.[4] מניעיו של מצית עשויים לכלול נקמה, ונדליזם, הונאה או טשטוש עקבות פשע, בין היתר. כדי להדליק את האש, יכול להיעשות שימוש במאיצי בעירה או בלהבות, או בסוג של התקן תבערה מאולתר (IID).

איום האש כנשק עלול להיות קשה לגילוי טרם תחילת הפיגוע. עליכם להבין את הצעדים שיש לנקוט אם אתם מריחים עשן או רואים משהו עולה באש.

3 הבולשת (Federal Bureau of Investigation) תילדפה, ללא תאריך, משאבי בטיחות ליורה פעיל. הגישה בוצעה ב-1 בדצמבר 2023. fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 הסוכנות לאבטחת סייבר (Cybersecurity and Infrastructure Security Agency) תויתשתו. 2021. מדריך לאש כנשק. הגישה בוצעה ב-8 באוגוסט 2023. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

במקרה של פיגוע שריפה, חייגו 9-1-1, ופעלו בהתאם להנחיות צוותי החירום. עזבו את אזור פעילות האש מיד, והזהירו אחרים, במידת האפשר. הימנעו מאזורים שבהם אתם יכולים להריח עשן או לראות אש. פנו מתחמים מקורים; סגרו את כל הדלתות מאחוריכם כדי להכיל את האש. אם אינכם מצליחים להתפנות, התרחקו ככל האפשר מהמפגע, והשתמשו במטפים לפי הצורך. שמרו על מודעות מצבית, והיו ערניים לפעילות חשודה או לאיומים נוספים.

בקרו במדריך הפעולה לאש כנשק של CISA לקבלת טיפים נוספים להפחתת הנזק בתקריות שבהן האש משמשת כנשק.

מטעני חבלה מאולתרים (IED)

מטען חבלה מאולתר הוא התקן המוצב או מיוצר באופן מאולתר, המשלב כימיקלים הרסניים, קטלניים, מזיקים, פירוטכניים או מציתים, ונועד להרוס, להשבית, להטריד או להסיח את הדעת.[5] בהתאם למטרות ולחומרים הזמינים ליצרן הפצצות, מטעני חבלה מאולתרים נעים בין התקנים קטנים וגולמיים, כגון התקני לחץ יתר או פצצות צינור המלאות לרוב באבקות נפץ, להתקנים גדולים הנישאים ברכב המכילים כמויות גדולות של חומרי נפץ.

האיומים יכולים להגיע במגוון צורות. אם אי פעם תהיו מודאגים ממצב מסוים או מחפץ חשוד, התקשרו מיד לגורמי אכיפת החוק המקומיים שלכם. דוגמאות לסימנים המצביעים על פצצה כוללות חוטים או אלקטרוניקה שאין להם הסבר, רכיבים דמויי פצצה גלויים אחרים, וכן צלילים, אדים, נתזים או ריחות חריגים. תקריות מטעני חבלה מאולתרים הכוללות מטען חשוד דורשות תגובה של יחידת החבלנים ויכולת לאבחן ו"לנטרל" מטעני אמת.

למידע נוסף על זיהוי חפצים חשודים, עיינו בעלון וכרזה בנושא חפץ חשוד או ללא בעלים, וצפו בסרטון "מה לעשות: חפץ חשוד או ללא בעלים".

מחאות והפגנות

ללא קשר לייעודן או כוונתן, אם מחאה או הפגנה פומביות מתקיימות ליד ביתכם, מקום העסק שלכם או אפילו בנכס שלכם, הישארו רגועים. מחאות עלולות להיות דבר מאיים, אך לא סביר שהן יובילו לאיום פיזי. גם אם הרוחות סוערות, שמרו על קור רוח. הישארו בפנים, סגרו ונעלו את הדלתות והחלונות שלכם, והגיפו את הווילונות/התריסים שלכם. אם אתם מרגישים לא בטוחים, או אם המצב יסלים, התקשרו לגורמי אכיפת החוק המקומיים שלכם.

במידת הצורך, שימו לב לתיאורים של אנשים ורכבים במקום. ספקו את כל צילומי הווידאו ממצלמות במעגל סגור ואת הסרטונים והתמונות שצולמו בטלפון סלולרי למשטרה, שכן הדבר עשוי לסייע במקרה של חקירה.

גיליון המידע בנושא הגנה על תשתיות במהלך הפגנות פומביות של CISA מציע המלצות אבטחה לעסקים שעלולים להיות יעד לפעולות בלתי חוקיות במהלך הפגנות פומביות.

מודעות מצבית

המשמעות של מודעות מצבית היא להיות מודע למה שקורה סביבכם, לקחת הכול בחשבון ולהתאים את ההתנהגות שלכם, כדי להפחית את הסיכון לפגיעה בכם, במשפחתכם או בעמיתיכם לעבודה.

מבקרים

הקפידו לזהות מבקרים לפני שאתם מתירים להם להיכנס לביתכם. שקלו להתקין חור הצצה או מצלמת דלת כדי לעזור לכם לזהות את מי שנמצא בצד השני של הדלת. בקשו ממבקרים לא מוכרים להזדהות לפני שתפתחו את דלתכם. עם כניסתם לביתכם, הקפידו להישאר בקרבתם, רצוי מולכם או במצב שבו ניתן לפקח עליהם חזותית. שקלו לשאת טלפון נייד בכל עת.

חומרים רגישים

הקפידו להשליך או להשמיד חומרים סודיים שעלולים להכיל מידע רגיש או מידע המאפשר זיהוי אישי של PII (PII). כולל כל מידע שהוא אישי במהותו, שעלול לשמש לזיהויך.

בטיחות הולכי רגל

העניקו עדיפות לבטיחות האישית שלכם בעת נסיעה, הליכה או ריצה במרחבים ציבוריים. נקיטת אמצעי זהירות מתאימים יכולה לעזור לכם להפחית את הפגיעות ואת הסיכון לחוות אלימות או תוקפנות. שקלו אמצעים פשוטים כמו תכנון מסלול בטוח מבעוד מועד, שינוי המסלול שלכם ביציאה למקומות רגילים והימנעות מנקודות סכנה אפשריות, כמו סמטאות שקטות או שאינן מוארות היטב, חניונים מקורים שוממים וחניונים מרוחקים.

5 המחלקה לביטחון המולדת של ארה"ב. הבולשת (Federal Bureau of Investigation) תילרדפה. ללא תאריך. *מדריך אבטחה וחוסן: תפיסות של התמודדות עם מטעני חבלה מאולתרים (C-IED), יעדים שכיחים וסיוע זמין*. הגישה בוצעה ב-8 באוגוסט 2023. עמ' 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

בכל עת שאתם במרחב הציבורי, השתמשו בשיקול דעת ונקטו באמצעי זהירות כדי להסתיר פרטי כניסה לעבודה או מידע אישי. נקטו במשנה זהירות בעת עניידת תגים או בהזנת סיסמאות במרחבים ציבוריים. לעובדות וטיפים נוספים, בקרו באתר האינטרנט של המינהל הלאומי לבטיחות בדרכים (National Highway Traffic Safety Administration) בנושא בטיחות הולכי רגל.

שמרו על מודעות מצבית

אם אתם מתחילים להיות מודאגים או להרגיש חסר ביטחון בזמן שאתם נמצאים במרחב/בסביבה ציבוריים, התקרבו לקבוצת אנשים. אם הדבר אינו מתאפשר, התאימו את תנועותיכם למודעות מצבית מרבית, ו**נקטו באמצעי הזהירות הבאים:**

- **שמרו את הטלפון הנייד שלכם** במצב המאפשר ביצוע שיחת חירום.
- **היו ערניים,** והישארו מודעים למיקומכם המדויק ולסביבתכם.
- **הימנעו מחשיפת** כל תכשיט או חפצי ערך.
- **קחו בחשבון את התאורה באזור, את המיקום ואת הקרבה** לעסקים מקומיים אחרים.
- **הקפידו לפנות לעבר התנועה מהכיוון הנגדי תוך כדי הליכה,** כדי להימנע מהתקרבות של כלי רכב המגיעים מאחור.
- **הקפידו שהידיים שלכם יהיו פנויות,** והישארו מודעים לסביבתכם.
- **הימנע מדיבור בטלפון**, משימוש באזניות או משליחת הודעות טקסט ארוכות.
- **שמרו על ערנות** בהליכה, והימנעו משהייה באותו מקום.
- **בעת שימוש בכספומט בנקאי**, הימנעו מהצגת כספים לעיני הציבור.

שירותי נסיעה שיתופית

בעת שימוש באפליקציית נסיעה שיתופית, שקלו להודיע לחבר או לעמית לעבודה על פרטי המיקום והיעד שלכם. בדקו את פרטי הנהג והרכב לפני קבלת הנסיעה והכניסה לרכב.

זיהוי פעילות חשודה ודיווח עליה

זהו פעילות חשודה ודווחו עליה - כמו אנשים שמסתובבים ללא סיבה ספציפית בקרבת הבית, מקום העבודה או הרכב שלכם, או אנשים שמנסים לצלם אתכם בצורה סמויה. אם הבחנתם במישהו שנוטש חפץ או חבילה ליד הבית, מקום העבודה או הרכב שלכם, דווחו על כך מיד למשטרה. למידע נוסף בנושא דיווח על פעילות חשודה, בקרו בקמפיין "אם ראית משהו, תגיד משהו®".

התקני הגנה אישיים

שקלו לשאת תרסיס פלפל, אזעקה קולית או התקן הגנה אישי נוסף כדי לבלבל את התוקף, להודיע לעוברי אורח ולספק לעצמכם הזדמנות לברוח. היכן שניתן, ובהתאם לחוקים ולתקנות הפדרליים והמקומיים, שאו התקני הגנה אישיים והשתמשו בהם.

מתן תשומת לב מדוקדקת לסימני האזהרה הבאים ודיווח מיידי עליהם עשוי לסייע בהפחתת תקרית פוטנציאלית:

- **איום בעל פה או בכתב** נגדכם או נגד ביתכם, רכושכם או מקום העבודה שלכם.
- **מערכות וציוד** פגומים או שחיבלו בהם.
- **חפצים חשודים או ללא בעלים**-לרבות שקיות, קופסאות, מכלים סמויים - שעלולים להכיל חומרים מסוכנים.
- **תשאול חשוד** בנושא תוכניות קומה של בניין, מיקומי כניסות/יציאות, מעליות, מטפים ואספקת מים, וכן מערכות חימום, אוורור ומיזוג אוויר (HVAC).
- **כמויות או מיקומים חריגים של חומרים דליקים או נפיצים,** לרבות מאיצי בעירה, צבעים, מסירי שומנים, חומרי ניקוי על בסיס אלכוהול, תרסיסים ומכלי גז פרופאן.
- **מסרים ברשתות חברתיות** המקדמים תמונות או רעיונות לביצוע פיגועים.

למידע נוסף, עיינו בסמנים ודוגמאות לדיווח על פעילות חשודה.

עימותים

למצוא את עצמכם במצב של עימות יכול להיות דבר מלחיץ. יש למקד את תשומת הלב בהתנהגויות הניתנות להבחנה שיכולות להעיד על פוטנציאל לאלימות. במצבים אלה, חשוב לשמור על קור רוח, ולהעריך את המצב כדי לקבוע אם בטוח להתערב. קחו בחשבון את גבולות היכולות שלכם, ובקשו סיוע מצוות אבטחה או מגורמי אכיפת החוק ברגע שניתן לעשות זאת בבטחה.

אם אתם מאומנים ומיומנים, שקלו למנוע הסלמה בבטחה במצבים נפיצים באמצעות פעולות תכליתיות הכוללות הקשבה ותקשורת יעילה. זכרו ש"מניעת הסלמה" אינה פעולה שמבצעים; זו המטרה.

בקרו בסדרת מניעת ההסלמה של CISA כדי ללמוד טיפים לשמירה על ערנות ולניווט במצבים שעלולים להיות עוינים.

רכבים מנועיים ונסיעות

לפני שאתם יוצאים מהבית או ממקום העבודה שלכם, הביטו סביב, ושימו לב לכלי רכב חשודים שעלולים לארוב או לשהות במרחב. סרקו את האזור מסביב לרכב לאיתור כל דבר שלא אמור להיות על הרכב שלכם או לידו. אם אכן מתרחש מצב, מידע זה עשוי להועיל למשטרה.

במידת האפשר, הימנעו מדפוסים חוזרים ונשנים בסידורי הנסיעה שלכם, כדי שגורמים זדוניים פוטנציאליים לא יוכלו לחזות את מקום הימצאכם. החליפו את מסלולי ההגעה ושנו את זמני היציאה שלכם ככל האפשר. הקפידו שכל דלתות הרכב ותא המטען יהיו נעולות במהלך נסיעתכם. פתחו חלונות באופן שמספיק לאוורור בלבד. סעו בבטחה, ושמרו על מרחק בטוח מהרכב שלפניכם. כמו כן - ודאו תמיד שיש מספיק דלק ברכבכם (או, אם הוא חשמלי, רמת סוללה מספקת) לנסיעתכם.

אם אתם חושבים שעוקבים אחריכם, נסו לשמור על קור רוח ולהמשיך בנסיעה. סגרו את כל החלונות, וודאו שהדלתות שלכם נעולות. פנו מיד לגורמי אכיפת החוק. אם ניתן, עשו את דרככם לכיוון תחנת המשטרה הקרובה - אל תיסעו הביתה. נסו לשים לב למספר לוחית הרישוי, ליצרן ולדגם של כל רכב חשוד.

אם אתם מעורבים בהתנגשות בין רכבים או אם חוויתם תקלה מכנית, קחו בחשבון את סביבתכם, ופנו מיד לצוותי החירום ולשירותי הגרירה. פעלו בהתאם להנחיות מגורמי אכיפת החוק.

שיחות טלפון ואיומים אנונימיים[6]

שיחות טלפון ואיומים אנונימיים נועדו בדרך כלל לזרות פחד, בהלה ומצוקה. זכרו להקפיד על הפעולות הבאות:

- **שמרו על קור רוח ,**ואל תנתקו את השיחה.
- **השאירו את המתקשר על הקו** במשך זמן רב ככל האפשר. היו מנומסים והפגינו עניין כדי שימשיך לדבר. הוא עשוי לחשוף מידע חשוב שיכול לעזור במקרה של חקירה משטרתית.
- במידת האפשר, **סמנו או העבירו פתק** לאדם או אנשים אחרים סביבכם שיאזינו לשיחה ויעזרו להודיע לרשויות.
- **רשמו** מידע רב ככל האפשר - מספר הטלפון של המתקשר, ניסוח מדויק של האיום, סוג הקול או ההתנהגות וכדומה - מה שיסייע לחוקרים.
- **הקליטו את השיחה,** במידת האפשר ואם החוק מתיר זאת.

החוק הפדרלי אוסר על ביצוע שיחות טלפון מאיימות או פוגעניות. אם תקבלו שיחות מסוג זה, פנו לגורמי אכיפת החוק המקומיים שלך. בנוסף, באפשרותכם לדווח על האיום לבולשת הפדרלית (FBI). עיינו במדריך לאיומים והפחדות של הבולשת הפדרלית (FBI מדריך לאיומים והפחדות) לקבלת טיפים.

מכיוון שרוב איומי הפצצה מבוצעים באמצעות טלפון, עיינו ברשימת התיוג לאיומי פצצה של המחלקה לביטחון המולדת (DHS רשימת התיוג לאיומי) ובמדריך לאיומי פצצה של הסוכנות לאבטחת סייבר ותשתיות (מדריך לאיומי פצצה CISA), המספקים הנחיות לתגובה לאיום פצצה, כמו גם רשימה מקיפה של מידע שיסייע לגורמי אכיפת החוק בחקירת איום פצצה.

אבטחה מקוונת

התקינו אפליקציות מ"חנויות אפליקציות" מכובדות בלבד, כדי למנוע הורדות שעלולות להיות מזיקות. אין להוריד אפליקציות ממקורות בלתי ידועים או שאינם ניתנים לאימות. שימו לב להרשאות שיש לאפליקציות לגשת למידע אחר בטלפון שלך.

צרו ותחזקו סיסמה חזקה שהיא ייחודית לכל אחד מהמכשירים או החשבונות שלכם, והשתמשו במנהל סיסמאות כדי לארגן אותן. הפעילו אימות רב-גורמי (MFA) עבור כל חשבון או אפליקציה שמציעים זאת. הפעלת MFA עוזרת להגן על מידע אישי כמו הדואר האלקטרוני שלכם, מדיה חברתית, מידע פיננסי ומידע חשוב אחר.

עדכוני תוכנה

שמרו את התוכנה מעודכנת כך שתוקפים לא יוכלו לנצל מידע רגיש או נקודות תורפה. מערכות הפעלה רבות מציעות עדכונים אוטומטיים. אם יש אפשרות כזו, הפעילו את העדכונים האוטומטיים בהגדרות אבטחת האפליקציות של המכשיר.

בדפדפן האינטרנט שלכם, חפש מאתרי משאבים אחידים (URL) שמתחילים ב-"https" - אינדיקציה לכך שאתרים משתמשים בהצפנה - במקום ב-"http". פרוטוקול העברת היפר-טקסט מאובטח (Hyper Text Transfer Protocol Secure - HTTPS) הוא פרוטוקול תקשורת אינטרנט, המשמש להצפנה והעברת מידע בצורה מאובטחת בין דפדפן האינטרנט של המשתמש לאתר האינטרנט שאליו הוא מחובר. הוא נועד לספק הגנה טובה יותר על שלמות וסודיות המידע של המשתמש כאשר הוא מבקר באתרים.[7]

עיינו ב"למען עולם בטוח יותר" של הסוכנות לאבטחת סייבר ותשתיות (רתוי חוטב סלוע ועמל CISA's) לקבלת מידע נוסף על שמירה על בטיחות באינטרנט.

6 הבולשת (Federal Bureau of Investigation) תילרדפה. ללא תאריך. מדריך האיומים וההפחדות. הגישה בוצעה ב-8 באוגוסט 2023. fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 המחלקה לביטחון המולדת של (Department of Homeland Security) ב"הרא. 2018. פרוטוקול העברת היפר-טקסט מאובטח (Hyper Text Transfer Protocol Secure - HTTPS) הגישה בוצעה ב-12 בפברואר 2024. cisa.gov/resources-tools/resources/hyper-text-transfer-protocol-secure-https.

שימוש במכשירים אלקטרוניים

מכשירים ורשתות ניידים יכולים להכיל מגוון של פרטים אישיים, כגון מידע בנקאי מקוון, מיילים, הודעות טקסט, אנשי קשר, מדיה חברתית ותמונות. כדי לשמור על אבטחת המכשיר שלכם, השתמשו בכל תכונות האבטחה, והקפידו לעדכן באופן קבוע את תוכנת המכשיר. צרו קודי סיסמה חזקים עבור הטלפון וכרטיסי ה-SIM שלכם, והשביתו שירותי מיקום מיותרים.[8]

הקפידו להחליף את קוד PIN ברירת המחדל שלכם לגישה לדואר הקולי. שקלו להגביל את שירותי המיקום בטלפון שלכם ובדקו את הגדרות הפרטיות, כדי למנוע מאחרים לעקוב אחר התנועות שלכם ולזהות את כתובת הבית או מקום העבודה שלכם באמצעות אפליקציות צד שלישי. בדקו את הגנות הפרטיות והאבטחה של Apple ו-Android כדי לשפר את אבטחת המכשיר או המכשירים שלכם.

מדיה חברתית

האינטרנט יכול להיות מקור חשוב של מידע, חינוך ובידור. עם זאת, יש צורך לשמור על ערנות ולנקוט באמצעי זהירות כדי להגביל את כמות המידע האישי שאתם מפרסמים באינטרנט - במיוחד במדיה החברתית.

אתרי מדיה חברתית פופולריים מאפשרים לאנשים ליצור פרופיל אישי וליצור אינטראקציה עם אחרים באינטרנט. באתרי נטוורקינג עסקי, אנשים עשויים להוסיף פרטים נוספים לפרופילים שלהם ולכלול עבר תעסוקתי ופרטי רקע אחרים. בעוד שהכלים הללו עוזרים לכם לתקשר עם אחרים ולפרסם את הרקע המקצועי שלכם, פרסום מידע אישי באינטרנט טומן בחובו סיכונים פוטנציאליים.

היזהרו בעת פרסום מידע אישי. גורמים זדוניים יכולים להשתמש בנתוני מיקום מתמונות, בימי הולדת, בשמות מלאים, בכתובות בית ובפרטי אימייל למטרות פריצה או לביצוע גניבת זהות. בנוסף, מידע על תעסוקה, בני משפחה, תחביבים או פרטי רכב הם בעלי ערך לפושעים ולגורמים עוינים. גם המשפחה והחברים שלכם יכולים לשתף מידע עליכם שלא במתכוון, אם הם לא נוקטים באמצעים מתאימים כדי להגן על פרטי הפרופיל שלהם. זכרו, אין כפתור "מחק" באינטרנט. שתפו בזהירות, כי גם אם תמחקו פוסט או תמונה מהפרופיל שלכם, רוב הסיכויים שמישהו כבר ראה אותם.

חלק מאתרי המדיה החברתית מחזיקים בנתונים שאתם מפרסמים, והם ימכרו את הפרטים שלכם לצדדים שלישיים. בדקו באופן קבוע את הגדרות הפרטיות ותיוג המיקום שלכם באתרים אלה, אחרת אתם מסתכנים בכך שהפרופיל האישי שלכם, חלקו או כולו, ייראה על ידי קהל גדול, אותו אינכם מכירים.[9, 10]

8 ועדת התקשורת (Federal Communication Commission) תילרדפה. 2019. הגנו על המכשיר החכם שלכם. הגישה בוצעה ב-20 בספטמבר 2023. fcc.gov/consumers/guides/protect-your-mobile-device.

9 ממשלת הממלכה המאוחדת. המרכז הלאומי לאבטחת סייבר. 2019. מדיה חברתית: כיצד להשתמש בה בבטחה. הגישה בוצעה ב-20 בספטמבר 2023. ncsc.gov.uk/guidance/social-media-how-to-use-it-safely.

10 הסוכנות לאבטחת סייבר (Cybersecurity and Infrastructure Security Agency) תויתשתו, ברית הסייבר הלאומית. 2019. אבטחת סייבר במדיה חברתית. הגישה בוצעה ב-20 בספטמבר 2023. cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

בדקו את הגדרות הפרטיות והמיקום של מדיה חברתית

X, שנקראה בעבר Twitter

- twitter.com/settings/privacy_and_safety
- twitter.com/settings/location_information

Instagram

- help.instagram.com/811572406418223
- **iOS:** help.instagram.com/171821142968851
- **Android: במכשיר ה-**Android **שלכם, נווטו אל 'הגדרות' > 'אפליקציות' >** Instagram **> 'הרשאות' > 'מיקום'**

Facebook

- facebook.com/help/325807937506242/
- facebook.com/help/337244676357509

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Privacy-Settings
- help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I-turn-on-Ghost-Mode

TikTok

- tiktok.com/safety/en/privacy-and-security-on-tiktok/
- support.tiktok.com/en/account-and-privacy/account-privacy-set-tings/location-services-on-tiktok

דוקסינג

דוקסינג מתייחס לשיטה של איסוף מידע המאפשר זיהוי אישי (PII) של אדם - או מידע רגיש של ארגון - ממקורות פתוחים או מחומרים שנחשפו, ושחרורו לציבור או שימוש בו למטרות זדוניות.[11, 12] פושעים יכולים להשתמש במידע זה למטרות סחיטה או זריעת פחד בקרב יעדים פוטנציאליים.

כשאתם מפרסמים באינטרנט, חשוב להיות מודעים למה שאתם מפרסמים ולאופן שבו אתם מפרסמים את זה. אם תפרסמו יותר מדי מידע בלי להחיל את הגדרות הפרטיות המתאימות, אתם עלולים לסכן את ביטחונכם האישי. אנשים יכולים להשתמש במידע זה כדי לבנות תמונה של מערכות היחסים, הדעות ומקומות העניין שלכם, וכן נושאים אחרים שהם יכולים לנצל בעתיד.

גם ברוקרי נתונים יכולים לאסוף מידע אישי זה ולמכור אותו לחברות אחרות. כדי למזער את הגעת הנתונים שלכם לברוקרים:

- **הימנעו** משיתוף PII.
- **אל** תוסיפו אנשים שאינכם מכירים בחיים האמיתיים במדיה חברתית.
- **ודאו** שלאפליקציות שבהן אתם משתמשים יש הצפנה מקצה לקצה.
- **הגבילו** את הרשאות האפליקציות.
- **הגדירו** Google Alerts עבור שמכם.
- **שקלו להקדיש זמן** לביטול הסכמתכם לברוקרי הנתונים ולאתרי חיפוש האנשים המרכזיים, או הירשמו לשירות שיעשה זאת עבורכם.

מידע מבוסס מיקום יכול להתפרסם במדיה חברתית, במיוחד מטלפונים סלולריים התומכים ב-GPS וממכשירים ניידים. מידע זה אינו מאובטח, והוא חשוף לכולם, כולל אנשים שעלולים לרצות להזיק לכם. שימו לב למה שאתם מפרסמים ופרסמו באופן אחראי, כדי להבטיח שהמידע שאתם מפרסמים לא מסכן אף אחד.

אם אתם מאמינים שאתם חווים דוקסינג:

- **דווחו על התקרית** לגורמי אכיפת החוק המקומיים ולכל פלטפורמה מקוונת שבה ייתכן שהמידע האישי שלכם פורסם.
- **תעדו** את מה שהתרחש, וצלמו צילומי מסך שתוכלו לשתף עם החוקרים.
- **קבעו** איזה מידע נוצל, מהי חומרת האיום ומהי נקודת החשיפה.
- **עבדו מול מנהלי אתרים** כדי להסיר מידע מאתרים או מאפליקציות.
- **הגדירו את הגדרות הפרטיות** לאפשרויות בעלות הפרטיות הגבוהה ביותר.
- **חפשו סימנים** לגניבת זהות, עקבו אחר חשבונות פיננסיים, הגדירו התראות על הונאה והחליפו פרטי כניסה וסיסמה עבור כל החשבונות המקוונים.

החוקים נגד דוקסינג משתנים בין תחומי שיפוט, ולכן חשוב לבדוק מהם באזורכם כאשר אתם שוקלים אפשרויות הפחתה ומניעה. אם אתם מודאגים בנוגע לבטיחות פיזית, פנו לגורמי אכיפת החוק המקומיים לקבלת צעדים להמשך.

זיהוי דיוג ודיווח עליו

פושעים משתמשים לעתים קרובות בטקטיקות דיוג כדי לגרום לכם לפתוח קישורים, אימיילים או קבצים מצורפים מזיקים, שעלולים לבקש את המידע האישי שלכם או להדביק את המכשירים שלכם. הודעות אלו נועדו לרוב להיראות כאילו הגיעו מאדם או ארגון מהימנים.

הודעות דיוג יכולות להגיע בצורה של אימייל, טקסט, הודעה ישירה במדיה חברתית או שיחת טלפון. היזהרו משפה דחופה או רגשית, מבקשות לשלוח מידע אישי, מכתובות URL מקוצרות שאינן מהימנות ומכתובות אימייל וקישורים שגויים.

אם אתם חושדים שהייתם יעד לניסיון דיוג, אל תלחצו על קישורים או על קבצים מצורפים. במקום זאת דווחו על כך, ולאחר מכן מחקו את ההודעה.

11 המחלקה לביטחון המולדת של (Department of Homeland Security) ארה"ב .2024 . משרד השותפות והמעורבות. משאבים לאנשים פרטיים בנושא איום הדוקסינג. הגישה בוצעה ב-09 בפברואר 2024. dhs.gov/publication/resources-individuals-threat-doxing.

12 המועצה האירופית למחקר (European Council for Nuclear Research) גרעיני. 2017. אבטחת מחשבים: עברו לשלב הבא: Doxware. הגישה בוצעה ב-12 בדצמבר 2023. home.cern/news/news/computing/computer-security-enter-next-level-doxware.

משאבים

אבטחה פיזית

- מדריך האבטחה והחוסן של CISA
- מוכנות ליורה פעיל של CISA
- מדריך האיומים וההפחדות של ה-FBI
- איומי פצצות של CISA
- סדרת מניעת ההסלמה של CISA

מודעות מצבית

- המרכז למניעת ההטרדות, למודעות ולמשאבים (SPARC)

אבטחה מקוונת

- "למען עולם בטוח יותר" של CISA
- פרטיות ואפליקציות למכשירים ניידים של CISA
- תובנות CISA: הפחתת ההשפעות של דוקסינג על תשתיות קריטיות
- אבטחת סייבר במדיה חברתית של CISA