دليل تصرف لاعتبارات الأمن الشخصي: العاملين في البنية التحتية الحيوية

مقدمة

في بيئة التهديدات الحالية اليوم، لا غنى عن البقاء حذرًا وتولي مسؤولية أمنك الشخصي وذلك لجميع العاملين في البنية التحتية الحيوية–أثناء الدوام وخارجه. حيث يؤدي العاملون في البنية التحتية الحيوية نطاقًا واسعًا من الخدمات التي تُشغّل الأنظمة الأساسية والأصول الضرورية للحياة الأمريكية الحديثة وتديرها وتصونها. وسيساعد البقاء متيقظًا لأية مخاطر أو تهديدات مرتبطة بطبيعة عملك واتباع إجراءات الأمان في حمايتك وحماية المقربين منك والبنية الأساسية التي تخدمها. ويمكن تقسيم الأمن الشخصي إلى ثلاثة أجزاء رئيسية–الأمن الجسدي والوعي الظرفي والأمن على الإنترنت. ويمكن لدليل التصرف غير الشامل هذا مساعدتك في تقييم وضعك الأمني ويوفر لك خيارات لتفكر فيها للتقليل من التهديدات.[1]

تقييم مستوى الحماية المناسب للعاملين في البنية التحتية الحيوية

يُقدِّم هذا الدليل لمحة عامة عن كيفية البقاء آمنًا في المنزل، وفي العمل، وفي الأماكن العامة، وعبر الإنترنت. ويبقى الأمر لتقديرك لتقرر ما المعايير الأكثر ملائمة لنمط حياتك ونقاط ضعفك الأمنية والمواقف التي قد تواجهها–على سبيل المثال، قد تزيد بعض العوامل من احتمالية وقوع أعمال العنف في محل العمل:

- **العمل بمفردك** أو في مناطق منعزلة.
- **التواجد شخصيًا لتقديم خدمات** أو رعاية شخصية.
- **التعامل مع المواد الخطرة** أو المعلومات الحساسة للأمن القومي.
- **مسؤولية الحماية** للبنية التحتية الحيوية المحلية أو القومية.

عند تقييم احتياجات الأمن الخاصة بك، فكر في الأمور التالية:

- **دورك الوظيفي والمهني.** هل وظيفتك ومهنتك تجعلك هدفًا جذابًا؟
- **تهديدات محددة.** هل هناك أدلة موثوقة تشير إلى أنك في خطر؟
- **تاريخك الشخصي.** هل تم استهدافك أو تهديدك في السابق؟
- **محدداتك البصرية الشخصية.** هل تعرض أي انتماءات لمجموعات تجعلك هدفًا جذابًا؟

اليوم، يواجه العاملون في البنية التحتية الحيوية نطاقًا واسعًا من التهديدات – من النشاط الإجرامي الشائع إلى المخططات المتطرفة العنيفة. إذا أجبت بنعم عن أي من الأسئلة أعلاه أو كلها، قد يشير هذا إلى أنك وغيرك من الموظفين الآخرين المحتملين في البنية التحتية الذين تعمل معهم معرضون للخطر وينبغي أن تقيّم احتياجاتك من الأمن. بينما تقيّم أمنك الشخصي، من المهم اتخاذ منهج متوازن وأن تتذكر مراعاة كل من حياتك في المنزل والعمل–**كن حذرًا في ممارساتك للأمن الشخصي وعاداتك وقيّم محيطك باستمرار**. ينبغي أن تكون الإجراءات التي تتخذها ملائمة للتهديدات المقدّرة. قد تسبب إجراءات الأمن المبالغ فيها ضغطًا وإزعاجًا غير ضروريين؛ لكن، المجهودات غير الكافية يمكن أن تعرضك للخطر.

إن القدرة على التعرف على مواقف الاستهداف أساسية لتجنبها أو للاستعداد لها عندما تحدث. إن الاستهداف سمة جسدية أو خاصية تشغيلية تترك أحد الكيانات أو الأصول أو الأنظمة أو الشبكات أو المناطق الجغرافية معرضة للاستغلال أو قابلة للاستهداف من أحد المخاطر المحددة.[2] ويمكن أن يكون المعتدون مبتكرون عندما يستهدفون الأفراد. قد يكون هدف المعتدي التسبب في الإحراج أو الإزعاج أو التوتر أو قد يرغب في التسبب في إصابة جسدية أو تقويض السلامة أو تهديد حياة البشر.

1 ProtectUK. 2022. دليل إرشادي حول الأماكن العامة القابلة للوصول (PALS): الأمن الشخصي. تم الوصول في أغسطس 8، 2023. protectuk.police.uk/personal-security.

2 إدارة الأمن الوطني الأمريكية (U.S. Department of Homeland Security). لجنة توجيه المخاطر. 2010. قاموس DHS للمخاطر إصدار 2010. تم الوصول إليه في أغسطس 8، 2023. cisa.gov/resources-tools/resources/dhs-risk-lexicon.

الأمن الجسدي

حماية منزلك

هناك مجموعة متنوعة من الإجراءات البسيطة يمكنك أخذها في الاعتبار لحماية نفسك ومنزلك. ابدأ بتركيب أو تحسين أنظمة الأمن المحيطة بمنزلك أو عقارك. أمّن أي أبواب أو نوافذ بالأقفال والمفاتيح والأضواء وقيّم الحاجة إلى نظام التلفزيون مغلق الدائرة (CCTV). فكّر في استخدام نظام قفل متقدم للمداخل والنوافذ بنظام مراقبة بالفيديو متّصل بشاشة متابعة (مزود بزوايا متعددة).

قم بصيانة الهياكل الخارجية للعقار مثل الحوائط والأسوار وتأكد من أن أية أدوات أو سلالم يمكن استخدامها للوصول إلى منزلك مخزنة بأمان. فكر في إزالة أي شيء يمكن استخدامه لإحداث الضرر، مثل الطوب المنحل والحجارة الكبيرة وزينة الحديقة. تأكد من أن الشجيرات والحشائش، إلخ مشذبة ومهذبة بحيث تكون أوراق الشجر:

- **غير قابلة للاستخدام** بواسطة الدخلاء للاختباء فيها أو التمكن من الوصول إلى المنزل.
- **لا تحجب** المنظر الخارجي عمّن بداخل المنزل.

أمّن الأبواب الخارجية والنوافذ بأجهزة قفل ملائمة، التي قد تشمل آليات قفل إلكترونية ومشفرة. ومن المستحسن تأمين مجموعة إضافية من المفاتيح وأرقام الدخول للاستخدام أثناء الطوارئ. وفكر في تغيير نظام القفل بأكمله في حالة تعرض أرقام الدخول للكشف أو فقدان المفاتيح.

استثمر في الإضاءة الخارجية التي تضيء الأبواب الخارجية ومناطق وقوف السيارة والممرات حول المنزل وقم بصيانتها. وفكر في تركيب كاميرات مع مناظر للأبواب والنوافذ. ضع هذه الأضواء والكاميرات في أماكن استراتيجية لاستبعاد أي مناطق عمياء حيث قد يتمكن الأفراد من تجنب الكشف.

إذا كان لديك سيارة ولا يمكنك تأمينها في جراج أو منطقة مغلقة، جرب تركها في منطقة مكشوفة لعامة الناس. اركن السيارة في منطقة مضاءة جيدًا، ومكشوفة لكاميرا CCTV أو في موقف سيارات مؤمن بموظفين. اغلق دائمًا أي نوافذ وأبعد الأشياء الثمينة عن مرمى البصر واقفل سيارتك، حتى لو كنت ستبعد عنها لبضع دقائق فحسب. وافهم كيفية استخدام نوع نظام الإنذار ضد السرقة في سيارتك. هناك أنظمة تشمل إشعارات صوتية وبصرية بالإضافة إلى خدمات تحديد موقع السيارة للمساعدة في تسريع استجابة الشرطة.

التخطيط مسبقًا

فكّر في تطوير خطة طوارئ للعائلة والتدريب على ما يمكن عمله في حالة الطوارئ. للحصول على مساعدة في تطوير خطة، ترجى زيارة:

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

الاعتداءات بالأسلحة النارية

تعرف حالة القناص النشط بأنها فرد واحد أو أكثر يقومون فعليًا بقتل أو محاولة قتل الناس في منطقة مزدحمة بالأفراد.[3] حالات القناص النشط غالبًا لا يمكن توقعها وتتطور بسرعة. في وسط الفوضى، يمكن لأي أحد لعب دور حيوي في تقليل آثار حالة القناص النشط.

لأن حالات القناص النشط غالبًا تستمر بين 10 إلى 15 دقيقة - قبل وصول قوات تنفيذ القانون إلى مسرح الجريمة - ينبغي على الأفراد الاستعداد ذهنيًا وجسديًا للاستجابة إلى أي حالة من حالات القناص النشط.

في حالة معتدٍ بالقنص، فكر في تطبيق استراتيجية استجابة تم التدريب عليها–مثل نموذج "اركض، اختبئ، قاتل"–وفقًا للسياسات الأمنية لمنظمتك. يمكن العثور على معلومات وموارد إضافية في الصفحة الرئيسية لـ CISA من أجل الاستعداد لحالات القناص النشط.

الحريق سلاحًا

الحريق المتعمد يعرّف بأنه أي حريق أو محاولة للحريق متعمدة أو كيدية–مع أو بدون نية مبيتة أو احتيال–لمنزل سكني أو مبنى عام أو سيارة أو طائرة أو أي ممتلكات شخصية أخرى.[4] قد يشمل دافع الحارق الانتقام أو التخريب أو إخفاء غش أو جريمة، من بين أشياء أخرى. يمكن استخدام المسرعات واللهب أو أي أجهزة إحراق مرتجلة (IID) لبدء الحريق.

قد يكون من الصعب تحديد خطر الحريق المستخدم للتسليح حتى يبدأ الاعتداء. ينبغي عليك فهم الخطوات اللازم اتباعها إذا شممت الدخان أو رأيت شيئًا يحترق.

3 مكتب التحقيقات الفيدرالية (Federal Bureau of Investigation). بلا تاريخ. موارد الأمان في حالات القناص النشط (Active Shooter Safety Resources). تم الوصول في ديسمبر 1، 2023. fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 وكالة الأمن السيبراني وأمن البنية التحتية (Cybersecurity and Infrastructure Security Agency). 2021. دليل التصرف في حالات استخدام الحريق سلاحًا (Fire as a Weapon Action Guide). تم الوصول إليه في أغسطس 8، 2023. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

في حالة الهجوم بحريق، اتصل برقم 9-1-1-واتبع توجيهات موظفي الطوارئ. غادر منطقة نشاط الحريق على الفور ونبّه الآخرين، إن أمكن. تجنب المناطق التي تشم فيها الدخان أو ترى الحريق. قم بإخلاء المقرات الداخلية؛ أغلق الأبواب خلفك لكي تمنع انتشار الحريق. إذا كانت غير قادر على الإخلاء، ابتعد قدر الإمكان عن الخطر واستخدم مطفأة الحريق حسب الحاجة. حافظ على إدراكك للموقف وانتبه للأنشطة المريبة أو التهديدات الإضافية.

قم بزيارة صفحة CISA الخاصة بـ دليل التصرف في حالة استخدام الحريق سلاحًا للمزيد من النصائح حول تقليل المخاطر في حالات استخدام الحريق سلاحًا.

أجهزة التفجير المرتجلة (IED)

الـ IED هو جهاز يوضع أو يصنع بطريقة مرتجلة تتضمن مواد كيميائية مدمرة أو مميتة أو سامة أو نارية أو حارقة وهو مصمم للتدمير أو الإضعاف أو الاعتداء أو الإلهاء.[5] وحسب أهداف صانع القنبلة والمواد المتوفرة له، تتراوح الـ IED بين أجهزة صغيرة وبدائية، مثل أجهزة الضغط الزائد أو القنابل الأنبوبية المملوءة عادة بمساحيق متفجرة، إلى أجهزة كبيرة محمولة على سيارات تحتوي على كميات كبيرة من المواد المتفجرة.

وقد تأخذ التهديدات أشكالًا متعددة. إذا شعرت في أي وقت بالقلق حيال موقف ما غرض مثير للريبة، اتصل بقوات تنفيذ القانون المحلية على الفور. والأمثلة التي تشير إلى قنابل تشمل أسلاكًا غير مبررة أو إلكترونيات، وأجزاء أخرى ظاهرة من مكونات تشبه القنبلة، وأصوات أو أبخرة أو رذاذ أو روائح غير عادية. تتطلب حوادث الجهاز المتفجر المرتجل التي تتضمن جهازًا مشتبهًا به استجابة فريق متفجرات وقدرة على تشخيص الأجهزة النشطة و"جعلها آمنة".

للمزيد من المعلومات حول التعرف على الأشياء المثيرة للريبة، ارجع إلى الملصق والبطاقة البريدية الخاصة بالأشياء غير المقصودة مقابل الأشياء المثيرة للريبة وشاهد الفيديو بعنوان "ماذا تفعل: شيء مثير للريبة أم غير مقصود."

الاحتجاجات والمظاهرات

بغض النظر عن المهمة أو النية، حافظ على هدوءك إذا حدث احتجاج أو مظاهرة عامة بالقرب من منزلك أو أماكن عملك أو حتى في عقارك. قد تبدو الاحتجاجات مخيفة لكن من غير المرجح أن تؤدي إلى تهديد جسدي. حتى لو أصبح الموقف غير مستقر، ابقَ هادئًا. وابقَ في الداخل وأغلق الأبواب والنوافذ واقفلها، وأسدل الستائر/حواجز الضوء. إذا شعرت بعدم الأمان أو تصاعد الموقف، اتصل بقوات تنفيذ القانون المحلية.

إذا لزم الأمر، دوّن أوصاف للأفراد والسيارات الموجودة. قدّم أي تصوير مراقبة بالفيديو أو فيديوهات من الهاتف النقال أو صور إلى الشرطة، لأنها قد تساعد في حالة حدوث تحقيق.

تقدم لائحة البيانات حول حماية البنية التحتية أثناء المظاهرات العامة الخاصة بـ CISA توصيات أمنية للأنشطة التي قد تكون هدفًا للأفعال غير القانونية أثناء المظاهرات العامة.

الوعي الظرفي

الوعي الظرفي هو أن تكون واعيًا لما يحدث حولك، وتأخذ كل شيء في الحسبان، وتعدّل سلوكك لتقلل مخاطر الإصابة على نفسك وعائلتك وزملائك في العمل.

الزوار

حدد من هم الزوار دائمًا قبل السماح لهم بدخول منزلك. فكر في تركيب وصواص (عين سحرية) أو كاميرا للباب لمساعدتك تحديد من يقف على الجانب الآخر من الباب. واطلب من الزائرين غير المعروفين التعريف بأنفسهم قبل فتح بابك. عند الدخول إلى منزلك، ابقهم بالقرب منك، أو يفضل أن يكونوا أمامك أو في وضع يمكن فيه متابعتهم بصريًا. فكر في حمل هاتف متنقل في جميع الأوقات.

المواد الحساسة

تخلص دائمًا بطريقة مناسبة أو قم بتدمير المواد السرية التي قد تحتوي على معلومات حساسة أو معلومات يمكن تحديد الهوية من خلالها (PII). تشمل الـ PII أي معلومات شخصية بطبيعتها يمكن استخدامها لتحديد هويتك.

أمن المشاة

فضّل أمنك الشخصي عند السفر أو السير أو الركض في الأماكن العامة. يمكن أن يساعدك اتخاذ الاحتياطات المناسبة في تقليل الثغرات ومخاطر التعرض إلى العنف أو الاعتداء. فكر في تدابير بسيطة مثل التخطيط المسبق لطريق آمن، وتغيير طريقك عند الذهاب إلى أماكن معتادة، وتجنب نقاط الخطر المحتملة، مثل الممرات الهادئة أو ضعيفة الإضاءة، والجاراجات المهجورة، ومواقف السيارات البعيدة.

5 إدارة الأمن الوطني الأمريكية (U.S. Department of Homeland Security). المكتب الفيدرالي للتحقيقات. بلا تاريخ. دليل الأمن وسرعة الاستجابة: مفاهيم مكافحة الأجهزة المتفجرة المرتجلة *(C-IED)* والأهداف المشتركة والمساعدة المتوفرة. تم الوصول في أغسطس 8، 2023. صفحة 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

كلما كنت في مكان عام، استخدم الحذر وخذ احتياطات لإخفاء أي وثائق خاصة بالعمل أو معلومات شخصية. واحترس عند ارتداء شارات أو إدخال كلمات سر بينما تتواجد في أماكن عامة. للمزيد من الحقائق والنصائح، قم بزيارة صفحة موقع إدارة أمن المرور على الطرق السريعة القومية (National Highway Traffic Safety Administration) حول أمن المشاة.

حافظ على الوعي الظرفي

إذا شعرت بالقلق أو بدأت تشعر بعدم الأمان أثناء تواجدك في منطقة/حدث عام، اقترب من مجموعة من الناس. إن لم يكن ذلك ممكنًا، عدّل حركتك لزيادة وعيك الظرفي لأقصى حد واتخذ **التدابير الاحتياطية الآتية:**

- **أبقِ هاتفك المتنقل** في وضع يسمح بإجراء اتصال الطوارئ.
- **كن حذرًا** وابقَ على دراية بموقع المحدد ومحيطك.
- **تجنب استعراض** أي مجوهرات أو أشياء قيمة.
- **فكّر في إضاءة المنطقة وموقعها وقربها** من الأنشطة المحلية الأخرى.
- **واجه السيارات القادمة أثناء السير** لتجنب اقتراب السيارات من الخلف.
- **ابقِ يديك خاليتين** وابقَ على دراية بمحيطك.
- **تجنب الحديث في الهاتف**، أو ارتداء سماعات الأذن أو إرسال رسائل نصية طويلة.
- **ابقَ حذرًا** عند السير وتجنب التباطؤ.
- **عند استخدام ماكينة الصراف الآلي**، امتنع عن إظهار العملات أمام الناس.

خدمات مشاركة التوصيل

عند استخدام تطبيق مشاركة التوصيل، فكر في إخطار صديق أو زميل بتفاصيل موقعك ووجهتك. تحقق من تفاصيل السائق والسيارة قبل قبول التوصيلة ودخول السيارة.

تعرف على النشاط المثير للريبة وأبلغ عنه

تعرف على النشاط المثير للريبة وأبلغ عنه - مثل الأشخاص الذين يتسكعون من دون سبب محدد حول منزلك أو محل عملك، أو الأشخاص الذين يحاولون أخذ صور لك بطريقة مستترة. إذا لحظت أحدًا يترك غرضًا أو طردًا بالقرب من منزلك أو محل عملك أو سيارتك، أبلغ عن الأمر إلى الشرطة على الفور. تعرف على المزيد حول الإبلاغ عن النشاط المثير للريبة بزيارة حملة "If You See Something, Say®".

يمكن للانتباه بعناية إلى العلامات التحذيرية التالية والإبلاغ عنها بسرعة أن يساعد في التخفيف من حدة حادثة محتملة:

- **تهديد لفظي أو مكتوب** ضدك أو ضد منزلك أو ممتلكاتك أو محل عملك.
- **تضرر أو العبث** بالأنظمة والمعدات.
- **الأغراض المثيرة للريبة أو المهملة**– بما في ذلك الحقائب والصناديق والحاويات المخفية–التي قد تحتوي على مواد خطرة.
- **التساؤلات المريبة حول** مخططات أدوار المباني ومواقع المداخل/المخارج والمصاعد ومطفآت الحريق ومصادر إمداد الماء بالإضافة إلى أنظمة التدفئة والتهوية وتكييف الهواء (HVAC).
- **الكميات غير المعتادة أو مواقع المواد القابلة للاشتعال أو القابلة للانفجار**، بما في ذلك المسرعات ومواد الطلاء ومواد إزالة الشحم والمنظفات الكحولية والبخاخات وخزانات غاز البروبين.
- **رسائل وسائل التواصل الاجتماعي** التي تروج لأي صور أو أفكار للقيام باعتداءات.

تفقد مؤشرات وأمثلة الإبلاغ عن الأنشطة المريبة للحصول على المزيد من المعلومات.

أجهزة الحماية الشخصية

فكر في حمل بخاخ الفلفل أو إنذار صوتي أو جهاز حماية شخصي إضافي لإرباك المعتدي وإخطار المتفرجين وإعطاء نفسك فرصة للهرب. حيثما أمكن، ووفقًا للقوانين واللوائح الفيدرالية والمحلية، احمل أجهزة الحماية الشخصية واستخدمها.

المواجهات

يمكن لتواجدك في موقف مواجهة أن يكون مسببًا للتوتر. ينبغي أن ينصب التركيز على السلوكيات الملحوظة التي قد تشير إلى عنف محتمل. في تلك المواقف، من المهم أن تبقى هادئًا وتقيم الموقف لتحديد ما إذا كان من الآمن أن تتفاعل. فكر في حدود قدراتك واطلب المساعدة من طاقم الأمن أو قوات تنفيذ القانون حالما يصبح من الآمن فعل ذلك.

إذا كنت مدربًا وماهرًا، فكر في تخفيف التصعيد بأمان من المواقف المحتدمة من خلال التصرفات الهادفة التي تتضمن الإصغاء والتواصل الفعالين. تذكر أن "تخفيف التصعيد" ليس شيئًا تفعله؛ إنه الهدف.

قم بزيارة سلسلة CISA عن تخفيف التصعيد لتعلم النصائح حول البقاء حذرًا والتحرك في المواقف ذات العنف المحتمل.

السيارات والسفر

قبل مغادرة منزلك أو محل عملك، انظر حولك ولاحظ أي سيارات قد تبدو متربصة أو متلكئة. افحص المنطقة المحيطة بالسيارة لتحديد أي شيء لا يفترض أن يوجد على سيارتك أو بالقرب منها. إذا حدث موقف ما، هذه المعلومة قد تكون مفيدة للشرطة.

إن أمكن، تجنب الأنماط المتكررة في ترتيبات السفر لكي لا يتوقع أصحاب النوايا الكيدية المحتملون أماكن تواجدك. غير طرق تحركك ونوّع في مواعيد مغادرتك قدر الإمكان. تأكد من أن جميع أبواب السيارة وصناديقها مقفلة أثناء رحلتك. افتح النوافذ بما يكفي فقط للتهوية. قُد بأمان وحافظ على مسافة آمنة من السيارة التي أمامك. وأيضًا—احرص دائمًا على أن يكون في سيارتك ما يكفي من الوقود (أو، إذا كانت سيارة كهربائية، أن تكون مشحونة بما يكفي) لرحلتك.

إذا كنت تظن أن هناك من يتبعك، حاول الحفاظ على هدوءك وابقِ سيارتك متحركة. أغلق جميع النوافذ وتأكد من قفل الأبواب. اتصل بقوات تنفيذ القانون على الفور. إذا كنت تستطيع، توجه نحو أقرب محطة شرطة–لا تقد سيارتك إلى المنزل. حاول ملاحظة أي أرقام على لوحة الترخيص ونوع وموديل أي سيارة مثيرة للريبة.

إذا تورطت في صدام سيارات أو واجهت عطلًا ميكانيكيًا، فكر في محيطك واتصل بمختصي الطوارئ وخدمة قطر السيارات على الفور. اتبع التعليمات من قوات تنفيذ القانون.

الاتصالات مجهولة المصدر والتهديدات[6]

عادة تكون المكالمات مجهولة المصدر والتهديدات مقصود بها إثارة الخوف والتنبيه والانزعاج. تذكر أن تقوم دائمًا بعمل الآتي:

- **ابق هادئًا** ولا تغلق الهاتف.
- **أبقِ المتصل على الخط** لأطول وقت ممكن. كن مهذبًا وأبدِ الاهتمام لتجعلهم يستمرون في التحدث. قد يكشفون معلومات مهمة قد تساعد في حالة تحقيق الشرطة.
- إذا أمكن، **أعطِ إشارة أو ملاحظة** إلى الشخص (الأشخاص) المحيط (المحيطين) بك لينصتوا ويساعدوا في إخطار السُلطات.
- **دوّن** أكبر قدر ممكن من المعلومات—رقم المتصل، الكلمات المحددة للتهديد، نوع الصوت أو السلوك، إلخ. — التي ستساعد المحققين.
- **سجّل الاتصال**، إذا أمكن وكان مسموحًا قانونيًا.

يحظر القانون الفيدرالي عمل مكالمات تهديدية أو مسيئة. إذا تلقيت أي اتصالات كهذه، اتصل بقوات تنفيذ القانون. بالإضافة إلى ذلك، يمكنك الإبلاغ عن التهديد إلى الـ FBI. تفقد دليل FBI للتهديدات بالتخويف للحصول على نصائح.

لأن معظم تهديدات القنابل تتم عبر الهاتف، اطّلع على قائمة DHS للتحقق من تهديدات القنابل و دليل CISA لتهديدات القنابل، التي تقدم تعليمات عن كيفية الاستجابة إلى تهديدات القنابل، بالإضافة إلى قائمة شاملة للمعلومات التي ستساعد قوات تنفيذ القانون في التحقيق عن تهديد بالقنابل.

الأمن على الإنترنت

لا تثبت التطبيقات سوى من "متاجر التطبيقات" حسنة السمعة لتجنب التنزيلات محتملة الضرر. لا تحمل التطبيقات من مصادر غير معروفة أو غير متحقق منها. كن متيقظًا للصلاحيات التي تأخذها التطبيقات للوصول إلى المعلومات الأخرى على هاتفك.

أنشئ كلمة سر قوية وحافظ عليها بحيث تكون فريدة من نوعها لكل من أجهزتك أو حساباتك واعتمد على مدير كلمات سر لتنظيمها. شغّل التحقق متعدد العوامل (MFA) لكل حساب أو تطبيق يقدمه. يساعد تفعيل MFA في حماية معلوماتك الشخصية مثل بريدك الإلكتروني ووسائل التواصل الاجتماعي والمعلومات المالية والمعلومات المهمة الأخرى.

التحديثات البرمجية

أبقِ البرامج محدثة لكي لا يستغل المهاجمون المعلومات الحساسة والثغرات. تقدم العديد من أنظمة التشغيل تحديثات تلقائية. إذا كان هذا خيارًا، شغّل التحديثات الأوتوماتيكية في إعدادات أمان تطبيقات الجهاز.

في متصفح الإنترنت الخاص بك، ابحث عن محددات الموارد الموحدة (URLs) التي تبدأ بـ "https"—لتكون مؤشرًا على أن المواقع تستخدم التشفير— بدلًا من "http". بروتوكول النقل الآمن للنصوص التشعيبية (HTTPS) هو بروتوكول تواصل على الإنترنت يستخدم لتشفير المعلومات ونقلها بأمان بين متصفح أحد المستخدمين والموقع المتصل به. إنه مصمم لحماية سلامة بيانات المستخدم وسريتها عندما يزور المواقع.[7]

تفقد صفحة CISA عن تأمين عالمنا لتعرف المزيد من المعلومات حول البقاء آمنًا على الإنترنت.

6 مكتب التحقيقات الفيدرالية (Federal Bureau of Investigation). بلا تاريخ. دليل تهديدات التخويف (Threat Intimidation Guide). تم الوصول في أغسطس 8، 2023. fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 إدارة الأمن الوطني الأمريكية (U.S. Department of Homeland Security). 2018. بروتوكول النقل الآمن للنصوص التشعيبية (HTTPS). تم الوصول في فبراير 12، 2024. cisa.gov/resources-tools/resources/hyper-text-transfer-protocol-secure-https.

استخدام الأجهزة الإلكترونية

يمكن أن تحمل الهواتف المتنقلة والشبكات الكثير من التفاصيل الشخصية، مثل المعلومات البنكية المرسلة عبر الإنترنت والبريد الإلكتروني والرسائل النصية وجهات الاتصال ووسائل التواصل الاجتماعي والصور. للحفاظ على أمان جهازك، استخدم جميع خصائص الأمان واحرص على تحديث برمجيات جهازك باستمرار. أنشئ أرقام سر قوية لهاتفك وبطاقات SIM الخاصة بك وعطّل خدمات تحديد الموقع غير الضرورية.[8]

غير دائمًا رمز PIN الافتراضي للوصول إلى البريد الصوتي. فكر في تقييد خدمات المواقع على هاتفك وراجع خدمات الخصوصية لمنع الآخرين من تتبع حركتك وتحديد موقع منزلك أو محل عملك من خلال تطبيقات الأطراف الثالثة. راجع وسائل حماية الخصوصية والأمان في أجهزة أبل وأندرويد لتحسين أمن جهازك (أجهزتك).

وسائل التواصل الاجتماعي

يمكن أن يكون الإنترنت مصدرًا قيمًا للمعلومات والتثقيف والترفيه. لكن، من الضروري البقاء حذرًا وأخذ الاحتياطات لتحديد مقدار المعلومات التي تنشرها على الإنترنت—خصوصًا على وسائل التواصل الاجتماعي.

تسمح وسائل التواصل الاجتماعي الرائجة للأفراد بإنشاء ملفات شخصية والتفاعل مع الآخرين عبر الإنترنت. على شبكات التواصل للعمل، يمكن للأشخاص إضافة المزيد من التفاصيل إلى ملفاتهم وتضمين سجل العمل وبيانات أخرى عن خلفيتهم. بينما تسمح لك تلك الأدوات بالتواصل مع الآخرين والإعلان عن خلفيتك المهنية، يمثل نشر معلومات شخصية على الإنترنت مخاطر محتملة.

كن حذرًا عند نشر معلومات شخصية. يمكن لأصحاب النوايا الكيدية استخدام معلومات الموقع من صورك وأعياد ميلادك والأسماء الكاملة وعناوين المنازل وتفاصيل البريد الإلكتروني عند اختراق أو ارتكاب سرقة الهوية. بالإضافة إلى ذلك، فإن المعلومات حول التوظيف أو أفراد العائلة أو الهوايات أو تفاصيل السيارة قيمة للمجرمين والأطراف العدوانية. يمكن لعائلتك وأصدقاءك أيضًا مشاركة معلومات حولك إذا لم يتخذوا إجراءات ملائمة لحماية معلومات حساباتهم الخاصة. تذكر، لا يوجد زر "حذف" على الإنترنت. شارك بعناية، لأنك لو حذفت منشورًا أو صورة من ملفك، هناك فرصة أن أحد ما قد رآها بالفعل.

بعض مواقع الشبكات الاجتماعية تمتلك البيانات التي تنشرها وستبيع بياناتك إلى الأطراف الثالثة. راجع بانتظام إعدادات خصوصيتك والوسم على تلك المواقع وإلا فأنت تخاطر برؤية جمهور كبير، غير معروف لك، لبعض أو كل بيانات ملفك الشخصي.[9,10]

---

8 لجنة الاتصالات الفيدرالية (Federal Communications Commission). 2019. احمِ جهازك الذكي. تم الوصول في سبتمبر 20، 2023. fcc.gov/consumers/guides/protect-your-mobile-device.

9 حكومة المملكة المتحدة. المركز القومي للأمن السيبراني (National Cyber Security Center). 2019. وسائل التواصل الاجتماعي: كيفية استخدامها بأمان. تم الوصول في سبتمبر 20، 2023. ncsc.gov.uk/guidance/social-media-how-to-use-it-safely.

10 وكالة الأمن السيبراني وأمن البنية التحتية، تحالف الأمن السيبراني (National Cyber Alliance). 2019. الأمن السيبراني على وسائل التواصل الاجتماعي. تم الوصول في سبتمبر 20، 2023. cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

راجع إعدادات الخصوصية على وسائل التواصل الاجتماعي وإعدادات الموقع

X، المعروف سابقًا باسم Twitter

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

Instagram

- help.instagram.com/811572406418223
- IOS: help.instagram.com/171821142968851
- **أندرويد:** على جهاز أندرويد الخاص بك، توجه إلى الإعدادات > التطبيقات > إنستغرام > الصلاحيات > الموقع

Facebook

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

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Priva-cy-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

استقاء المعلومات الشخصية

يشير استقاء المعلومات الشخصية إلى ممارسة جمع المعلومات التي يمكن تحديد الهوية من خلالها (PII)–أو المعلومات الحساسة لإحدى المنظمات–من المصادر المفتوحة أو المواد المكشوفة ونشرها على الملأ أو استخدامها لأغراض كيدية.[11،12] يمكن للمجرمين استخدام هذه المعلومات كوسيلة ابتزاز أو لإحداث الخوف عند الأهداف المحتملة.

وأنت تنشر على الإنترنت، من المهم أن تكون مدركًا لما تنشره وكيف تنشره. إذا نشرت الكثير من المعلومات من دون تطبيق إعدادات الخصوصية الملائمة، قد تضع سلامتك الشخصية في خطر. يمكن للناس استخدام هذه المعلومات لبناء صورة عن علاقاتك وآرائك وأماكن اهتمامك والمواضيع الأخرى التي يمكنهم استغلالها في المستقبل.

ويمكن أيضًا لسماسرة البيانات تجميع هذه المعلومات الشخصية وبيعها إلى الشركات الأخرى. لتقليل جمع بياناتك لدى سماسرة البيانات:

- **تجنب** مشاركة PII.
- **لا تقبل** الأشخاص الذين لا تعرفهم في الحياة الواقعية على وسائل التواصل الاجتماعي.
- **تأكد** من أن التطبيقات التي تستخدمها لديها تشفير من طرف إلى طرف.
- **حدد** صلاحيات التطبيقات.
- **قم بإعداد** تنبيهات جوجل (Google Alerts) لاسمك.
- **فكر في أخذ بعض الوقت** لاختيار الخروج من مواقع سماسرة البيانات الكبرى والبحث عن الأشخاص أو اشترك في خدمة تفعل ذلك نيابة عنك.

يمكن نشر المعلومات القائمة على الموقع على وسائل التواصل الاجتماعي، خاصة من الهواتف النقالة المفعل فيها خدمة GPS والأجهزة المتنقلة. هذه المعلومات ليست آمنة ويمكن لأي أحد رؤيتها بما في ذلك الأشخاص الذين قد يتمنون لك الأذى. احصر ما تنشره وانشر بمسؤولية لضمان عدم تعرض أحد للخطر من المعلومات التي تنشرها إلى العامة.

إذا ظننت أنك تتعرض لاستقاء المعلومات:

- **أبلغ عن الحادثة** لدى سلطات تنفيذ القانون المحلية وأي منصة على الإنترنت قد تكون بياناتك الشخصية نُشرت فيها.
- **وثق** ما حدث وخذ لقطات شاشة لمشاركتها مع المحققين.
- **حدد** ما المعلومات التي تم استغلالها ومدى خطورة التهديد ونقطة الكشف.
- **اعمل مع مديري الموقع** لإزالة المعلومة من المواقع أو التطبيقات.
- **اضبط إعدادات الخصوصية** لأكثر الاختيارات خصوصية.
- **انتبه لعلامات** سرقة الهوية وتابع الحسابات المالية وقم بإعداد تنبيهات الاحتيال وغيّر معلومات الدخول وكلمة السر لجميع المواقع على الإنترنت.

القانون ضد الاستقاء وفقًا للاختصاص، لذا من المهم البحث عنهم في منطقتك بينما تفكر في خيارات التقييد والمنع. إذا كنت قلقًا بشأن الحماية الجسدية، تواصل مع قوات تنفيذ القانون بشأن الخطوات التالية.

رصد محاولات التَصَيُّدِ والإبلاغ عنها

عادة يستخدم المجرمون تقنيات التصيد لكي تفتح وصلات مؤذية أو رسائل بريد إلكتروني أو مرفقات يمكن أن تطلب بياناتك الشخصية أو تصيب أجهزتك بالعدوى. هذه الرسائل مصممة عادة لكي تبدو كأنها أتت من شخص أو منظمة موثوق بهما.

يمكن أن تأتي رسائل التصيد في صورة بريد إلكتروني أو رسالة نصية أو رسالة مباشرة على وسائل التواصل الاجتماعي أو مكالمة هاتفية. كن على حذر من اللغة المتعجلة أو العاطفية وطلبات إرسال معلومات شخصية و URL المختصرة غير الموثوقة وعناوين البريد الإلكتروني غير الصحيحة والروابط.

إذا كنت تشك أنك كنت هدفًا لمحاولة تصيد لا تنقر على أي وصلات أو مرفقات. بدلًا من ذلك أبلغ عن الرسالة ثم احذفها.

11 إدارة الأمن الوطني (Department of Homeland Security). 2024. مكتب الشراكة والتفاعل (Office of Partnership and Engagement). موارد للأفراد عن مخاطر استقاء المعلومات. تم الوصول في فبراير 09، 2024. dhs.gov/publication/resources-individuals-threat-doxing.

12 المجلس الأوروبي للأبحاث الذرية (European Council for Nuclear Research). 2017. أمن الحاسوب: دخول المستوى التالي: برامج الاستقاء. تم الوصول في ديسمبر 12، 2023. home.cern/news/news/computing/computer-security-enter-next-level-doxware.

موارد

الأمن الجسدي

- دليل CISA للأمن والمرونة
- استعدادات CISA للقناص النشط
- دليل FBI لتهديد التخويف
- CISA تهديدات القنابل
- سلسلة CISA لتخفيف التصعيد

الوعي الظرفي

- مركز منع الترصد والتوعية به وبموارده (SPARC)

الأمن على الإنترنت

- CISA لنحمي عالمنا
- CISA الخصوصية وتطبيقات الهواتف المتنقلة
- تحليلات CISA: تخفيف آثار استقاء المعلومات على البنية التحتية الحيوية
- CISA الأمن السيبراني على وسائل التواصل الاجتماعي