व्यक्तिगत सुरक्षा विचार किए जाने वाले प्वाइंट्स कार्रवाई गाइड: महत्वपूर्ण अवसंरचना कर्मचारी

परिचय

आज के जोखिम भरे वातावरण में सभी महत्वपूर्ण अवसंरचना कर्मचारियों के लिए—काम के समय और काम के समय के बाद भी सतर्क रहना और अपनी व्यक्तिगत सुरक्षा की ज़िम्मेदारी लेना बहुत ज़रूरी है। महत्वपूर्ण अवसंरचना कर्मचारी विभिन्न तरह की सेवाएँ प्रदान करते हैं जो आधुनिक अमेरिकी जीवन के लिए ज़रूरी प्रमुख प्रणालियों और संपत्तियों का परिचालन, संचालन और रखरखाव करते हैं। अपने काम के क्षेत्र से जुड़े जोखिमों या खतरों के बारे में सतर्क रहने और सभी सुरक्षा प्रक्रियाओं को अपनाने से आपको खुद को, आपके करीबियों को और जिस अवसंरचना को आप सेवाएँ दे रहे हैं, उसे सुरक्षित करने में सहायता मिलेगी। व्यक्तिगत सुरक्षा को तीन प्रमुख हिस्सों में बाँटा जा सकता है—शारीरिक सुरक्षा, स्थिति के बारे में सतर्कता और ऑनलाइन सुरक्षा। इस गैर-विस्तृत कार्रवाई गाइड से आपको अपनी संपूर्ण सुरक्षा स्थिति का आकलन करने में सहायता मिल सकती है और इसमें आपको जोखिमों को कम करने के लिए विचार किए जाने लायक विकल्प दिए गए हैं।[1]

महत्वपूर्ण अवसंरचना संबंधी कर्मचारियों के लिए रक्षा के उचित स्तर का आकलन करना

इस गाइड में इस बारे में संक्षिप्त जानकारी दी गई है कि घर पर, कार्यस्थल पर, सार्वजनिक स्थलों पर और ऑनलाइन सुरक्षित कैसे रहें। यह निर्धारित करना आप पर निर्भर करता है कि आपकी जीवनशैली, सुरक्षा से जुड़े जोखिमों और आपके सामने आने वाली संभावित स्थितियों के लिए कौन से समाधान आपके लिए सबसे उचित हैं—उदाहरण के लिए कुछ कारक कार्यस्थल पर हिंसा की संभावना को बढ़ा सकते हैं:

- **अकेले** या सुनसान क्षेत्रों में काम करना।
- **व्यक्तिगत सेवाएँ** या देखभाल प्रदान करना।
- **खतरनाक सामग्री** या राष्ट्रीय सुरक्षा के लिए संवेदनशील जानकारी के साथ काम करना।
- **स्थानीय** या राष्ट्रीय महत्वपूर्ण अवसंरचना की रक्षा के लिए ज़िम्मेदारी।

अपनी सुरक्षा ज़रूरतों का आकलन करते समय, निम्नलिखित पर विचार करें:

- **आपका व्यवसाय और पेशेवर भूमिका।** क्या आपकी नौकरी या करियर आपको आकर्षक लक्ष्य बनाते हैं?
- **विशिष्ट खतरे।** क्या कोई ऐसा विश्वसनीय प्रमाण है जो इशारा करता है कि आपको कोई जोखिम है?
- **आपका व्यक्तिगत इतिहास।** क्या आपको पहले भी निशाना बनाया गया है या धमकाया गया है?
- **आपके व्यक्तिगत दृश्य पहचानकर्ता।** क्या आप किसी भी ऐसे समूह के साथ संबद्धता रखते हैं जो आपको आकर्षक लक्ष्य बनाता है?

आज महत्वपूर्ण अवसंरचना कर्मचारी—आम आपराधिक गतिविधि से लेकर हिंसक उग्रवादी साज़िशों तक बहुत तरह के खतरों का सामना कर रहे हैं। अगर आपने उपर्युक्त प्रश्नों में से किसी या सभी का उत्तर हाँ में दिया है, तो इसका मतलब हो सकता है कि आप और संभवत: जिन दूसरे महत्वपूर्ण अवसंरचना कर्मचारियों के साथ आप काम करते हैं, वे भी जोखिम पर हैं और आपको अपनी सुरक्षा ज़रूरतों का मूल्यांकन करना चाहिए। जब आप अपनी व्यक्तिगत सुरक्षा का आकलन करते हैं, तब संतुलित दृष्टिकोण अपनाना और अपने घर और कार्यस्थल के जीवन को ध्यान में रखना ज़रूरी है—**अपनी व्यक्तिगत सुरक्षा पद्धतियों, आदतों में सतर्क रहें और निरंतर अपने आसपास के वातावरण का आकलन करें।** आपके द्वारा किए जाने वाले समाधान संभावित खतरों के अनुरूप होने चाहिए। ज़रूरत से अधिक सुरक्षा कार्रवाइयाँ अनावश्यक तनाव और असुविधा उत्पन्न कर सकती हैं; हालाँकि अपर्याप्त प्रयास आपको जोखिम में डाल सकते हैं।

जोखिमपूर्ण स्थितियों से बचने या उनके उत्पन्न होने पर उनका सामना करने के लिए तैयार रहने के लिए उन्हें पहचानने की क्षमता महत्वपूर्ण है। जोखिम ऐसी भौतिक विशेषता या प्रचालनात्मक विशिष्टता है जो किसी इकाई, संपत्ति, प्रणाली, नेटवर्क या भौगोलिक क्षेत्र को शोषणा या किसी निर्धारित खतरे के लिए खोल देता है।[2] जब हमलावर व्यक्तियों पर निशाना साधते हैं, तब वे रचनात्मक हो सकते हैं। किसी हमलावर का लक्ष्य शर्मसार करना, असुविधा, तनाव पैदा करना हो सकता है या उनका इरादा शारीरिक चोट पहुँचाना, स्वास्थ्य को नुकसान पहुँचाना या इंसानी ज़िंदगियों को खतरे में डालना हो सकता है।

1 UK की रक्षा करें. 2022. सार्वजनिक रूप से सुलभ स्थल (PALs) मार्गदर्शन: व्यक्तिगत सुरक्षा। 8 अगस्त, 2023 को देखा गया। protectuk.police.uk/personal-security.

2 U.S. होमलैंड सुरक्षा विभाग। जोखिम संचालन समिति। 2010. DHS जोखिम कोश 2010 संस्करण। 8 अगस्त, 2023 को देखा गया। cisa.gov/resources-tools/resources/dhs- risk-lexicon.

शारीरिक सुरक्षा

अपने घर को सुरक्षित बनाना

विचार करने के लिए ऐसे विभिन्न आसान समाधान हैं जो आपकी और आपके घर की रक्षा करने में सहायक हो सकते हैं। अपने निवास या संपत्ति के चारों ओर की सुरक्षा व्यवस्थाओं को स्थापित करने या इन्हें बेहतर बनाने से शुरू करें। दरवाजों या खिड़कियों को तालों, चाबियों, अलार्म्स, लाइट्स से सुरक्षित करें और क्लोज़्ड-सर्किट टेलीविज़न (CCTV) सिस्टम के लिए अपनी ज़रूरत का आकलन करें। प्रवेश के रास्तों और खिड़कियों पर मॉनिटर किए जाने वाले (मल्टी-व्यू सक्षम) वीडियो निगरानी सिस्टम के साथ उन्नत लॉकिंग सिस्टम के उपयोग पर विचार करें।

दीवारों और बाड़े जैसी बाहरी संपत्ति संरचनाओं का रखरखाव करें और सुनिश्चित करें कि आपके घर में प्रवेश के लिए उपयोग किए जा सकने वाले किन्हीं उपकरणों या सीढ़ियों को सुरक्षित ढंग से स्टोर में रखा जाए। नुकसान पहुंचाने के लिए उपयोग की जाने वाली किसी भी चीज जैसे खुली ईंट, बड़े पत्थर और बगीचे की सजावट के सामान को हटाने पर विचार करें। सुनिश्चित करें कि झाड़ियों, खरपतवार आदि को छंटवा दिया गया है और इनका रखरखाव किया जा रहा है ताकि

- इन झाड़ियों का उपयोग हमलावरों द्वारा छुपने या घर में घुसने के लिए **न किया जा सके।**
- झाड़ियाँ घर के अंदर से बाहर के दृश्य को देखने में **रुकावट न डालें।**

बाहरी दरवाजों और खिड़कियों को उचित लॉकिंग उपकरणों से सुरक्षित करें जिनमें इलेक्ट्रोनिक और कोडेड लॉकिंग प्रणालियाँ शामिल हो सकती हैं। आपातकाल की स्थिति में उपयोग के लिए चाबियों का अतिरिक्त सेट या प्रवेश कोड्स रखना सबसे अच्छा है। प्रवेश कोड्स के किसी को पता चलने या चाबियाँ खो जाने पर पूरे लॉकिंग सिस्टम को बदलने पर विचार करें।

उस बाहरी लाइटिंग में निवेश करें और इनका रखरखाव करें जिससे बाहरी दरवाजों, पार्किंग क्षेत्र और घर के आस-पास पैदल-मार्गों में रोशनी होती है। दरवाजों और खिड़कियों के दृश्यों के साथ कैमरे स्थापित करने पर विचार करें। व्यक्ति पहचाने जाने से बच सकें, ऐसे कोई भी ब्लाइंड स्पॉट्स न छोड़ते हुए इन लाइट्स और कैमरों को उचित स्थानों पर रखें।

अगर आपके पास कोई वाहन है और आप इसे किसी गैराज या लॉक्ड क्षेत्र में नहीं रख सकते, तो इसे ऐसी जगह खड़ा करने की कोशिश करें जहाँ यह लोगों की नजर में रहे। अच्छी रोशनी वाले क्षेत्र CCTV कैमरा के व्यू वाले या स्टाफ पार्किंग स्थल में वाहन पार्क करें। हमेशा सभी खिड़कियों को बंद करें, कीमती चीज़ों को नज़र में आने से हटाएँ और अपनी कार को लॉक करें, चाहे आप कुछ मिनटों के लिए ही बाहर जा रहे हों। जानें कि आपके वाहन के अंदर चोरी से बचने वाले अलार्म सिस्टम का उपयोग कैसे करना है। ऐसे सिस्टम्स हैं जिनमें पुलिस कार्रवाई में तेज़ी लाने में सहायता करने के लिए वाहन लोकेटर सेवाओं के अलावा सुनने वाले और देखने वाले नोटिफ़िकेशंस होते हैं।

आगे की योजना बनाएँ

परिवार आपातकाल कार्य योजना तैयार करने और इसका अभ्यास करने पर विचार करें कि आपातकाल की स्थिति में क्या करना है। योजना तैयार करने में सहायता के लिए, इस पर जाएँ:

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

बंदूक आदि से हमले

एक्टिव शूटर को किसी भीड़-भाड़ वाले इलाके में लोगों को मारने या मारने का प्रयास करने वाले एक या अधिक व्यक्तियों के रूप में परिभाषित किया जाता है।[3] एक्टिव शूटर वाली घटनाएँ प्राय: अप्रत्याशित होती हैं और बहुत तेज़ी से घटित हो जाती हैं। इस अफरा-तफरी में कोई भी व्यक्ति एक्टिव शूटर घटना के प्रभावों को कम करने में अभिन्न भूमिका निभा सकता है।

एक्टिव शूटर स्थितियाँ अधिकतर 10 से 15 मिनट के अंदर खत्म हो जाती हैं - इसलिए कानून प्रवर्तन यूनिट के घटनास्थल पर पहुँचने से पहले ही – व्यक्तियों को किसी एक्टिव शूटर घटना के समय कार्रवाई करने के लिए मानसिक और शारीरिक रूप से तैयार रहना चाहिए।

एक्टिव शूटर घटना की स्थिति में, अभ्यास की गई कार्रवाई रणनीति पर काम करने पर विचार करें—जैसे अपनी संगठन सुरक्षा नीतियों के अनुसार—भागें, छुपें, लड़ें प्रतिमान। अतिरिक्त जानकारी और संसाधन एक्टिव शूटर के लिए तैयार रहना के लिए CISA के होमपेज पर देखे जा सकते हैं।

हथियार के रूप में आग

आगजनी को किसी रिहायशी घर, सार्वजनिक इमारत, मोटर वाहन, एयरक्राफ़्ट या किसी अन्य व्यक्तिगत संपत्ति को धोखाधड़ी करने के इरादे से या इसके बिना किसी भी जान-बूझकर या गलत इरादे से जलाने या जलाने की कोशिश करने के रूप में परिभाषित किया गया है।[4] आगजनी करने वाले व्यक्ति का उद्देश्य अन्य बातों के साथ-साथ बदला लेना, गुंडागर्दी करना, धोखाधड़ी करना या अपराध को छुपाने का हो सकता है। आग लगाने के लिए त्वरक और लपटों या आग लगाने वाले उन्नत उपकरण (IID) का उपयोग किया जा सकता है।

हथियार के रूप में आग के खतरे का पता लगाना मुश्किल हो सकता है जब तक कि हमला जारी न हो। अगर आपको धुएँ की बू आए या कुछ जलता हुआ दिखाई दे, तो उस स्थिति में उठाए जाने वाले कदमों को समझने की ज़रूरत है।

3 संघीय अन्वेषण ब्यूरो, n.d. एक्टिव शूटर सुरक्षा संसाधन। 1 दिसंबर, 2023 को देखा गया, fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 साइबर सुरक्षा और अवसंरचना सुरक्षा एजेंसी। 2021. 'हथियार के रूप में आग' के लिए कार्रवाई गाइड। 8 अगस्त, 2023 को देखा गया। cisa.gov/resources-tools/resources/fire-weapon-action-guide.

आग से हमले की स्थिति में 9-1-1 पर कॉल करें और आपातकाल कर्मचारियों से मिले निर्देशों का पालन करें। आग से प्रभावित क्षेत्र से तुरंत दूर चले जाएँ और अगर संभव हो, तो दूसरों को भी सतर्क करें। जिन क्षेत्रों में आप धुएँ को सूंघ पा रहे हैं या आग देख पा रहे हैं, उनमें न जाएँ। अंदरूनी जगहों से बाहर आ जाएँ; आग को आगे फैलने से रोकने के लिए अपने पीछे सभी दरवाजे बंद कर दें। अगर आप बाहर निकलने में असमर्थ हैं, तो खतरे से जितना संभव हो उतना दूर जाएँ और ज़रूरत पड़ने पर अग्निशामक यंत्रों का प्रयोग करें। स्थिति के प्रति सतर्क बने रहें और संदिग्ध गतिविधि या और खतरों के प्रति सावधान रहें।

आग को हथियार के रूप में प्रयोग किए जाने पर इससे होने वाले नुकसान को कम से कम करने के संबंध में अधिक सुझावों के लिए CISA की हथियार के रूप में आग कार्रवाई गाइड देखें।

उन्नत विस्फोटक उपकरण (IED)

IED नष्ट करने, अशक्त बनाने, आतंकित करने या ध्यान भटकाने के लिए तैयार किया गया विनाशक, जानलेवा, हानिकारक, आतिशबाज़ी करने वाले या आग भड़काने वाले रसायनों से बना उन्नत तरीके से रखा गया या बनाया गया उपकरण होता है।[5] बम बनाने वाले के लक्ष्यों और उसके पास उपलब्ध सामग्री के आधार पर IEDs विस्फोटक पाउडर से भरे गए ओवरप्रेशर उपकरणों या पाइप बमों जैसे छोटे, अपरिष्कृत उपकरणों से लेकर बड़ी मात्रा में विस्फोटक वाले बड़े वाहन पर ले जाए जाने वाले उपकरणों तक के आकार के होते हैं।

खतरे अलग-अलग तरह के हो सकते हैं। अगर आप कभी भी किसी स्थिति या संदिग्ध वस्तु के बारे में चिंतित होते हैं, तो तुरंत अपनी स्थानीय कानून प्रवर्तन यूनिट को कॉल करें। बम की ओर इशारा करने वाले उदाहरणों में बेवजह के तार या इलेक्ट्रोनिक्स, अन्य दिखाई देने वाले बम जैसे घटक, और असामान्य आवाजें, भाप, धुंध या गंध आना शामिल हैं। किसी संदेहजनक उपकरण वाली उन्नत विस्फोटक उपकरण घटनाओं से निपटने के लिए बम स्क्वाड प्रतिक्रिया और पता लगाने की क्षमता और इसे 'सुरक्षित बनाने वाले' व्यवहार्य उपकरणों की ज़रूरत होती है।

संदिग्ध वस्तुओं की पहचान के बारे में अधिक जानकारी के लिए लावारिस बनाम संदिग्ध वस्तु पोस्टकार्ड और पोस्टर देखें और क्या करें: संदिग्ध या लावारिस वस्तु" वीडियो देखें।

विरोध और प्रदर्शन

मिशन या इरादा कुछ भी हो, लेकिन अगर आपके घर, व्यवसाय के स्थान या यहाँ तक कि आपकी संपत्ति के आसपास भी कोई सार्वजनिक विरोध या प्रदर्शन होता है, तो शांत बने रहें। विरोध प्रदर्शन डराने वाले लग सकते हैं लेकिन इनसे शारीरिक खतरा होने की संभावना बहुत कम है। अगर स्थिति खराब भी हो जाती है, तब भी शांत बने रहें। अंदर रहें, अपने दरवाजे और खिड़कियाँ बंद कर लें, और परदे/ब्लाइंड्स बंद कर लें। अगर आप असुरक्षित महसूस कर रहे हैं या स्थिति बदतर हो जाती है, तो अपनी स्थानीय कानून प्रवर्तन इकाई को कॉल करें।

अगर ज़रूरी हो, तो मौजूद व्यक्तियों और वाहनों का विवरण नोट करें। पुलिस को कोई वीडियो निगरानी फुटेज, सेल फ़ोन वीडियो या फोटो दें, क्योंकि इससे जाँच करने में सहायता मिल सकती है।

CISA की सार्वजनिक प्रदर्शनों के दौरान अवसंरचना की रक्षा करने संबंधी फ़ैक्ट शीट में सार्वजनिक प्रदर्शनों के दौरान गैर-कानूनी गतिविधियों के संभावित निशाने पर आने वाले व्यवसायों के लिए सुरक्षा संबंधी सिफ़ारिशें दी गई हैं।

स्थिति के प्रति सतर्कता

स्थिति के बारे में सतर्कता का मतलब है आपके आसपास होने वाली चीज़ों के बारे में सतर्क रहना, हर बात को ध्यान में रखना और आपको, आपके परिवार को या आपके सहकर्मियों को नुकसान का जोखिम कम करने के लिए अपने व्यवहार को बदलना।

आगंतुक (विज़िटर)

आगंतुकों को अपने घर के अंदर आने देने से पहले हमेशा उनकी पहचान करें। दरवाजे की उस तरफ कौन है, इसकी पहचान करने के लिए दरवाजे में पीपहोल बनवाने या डोर कैमरा लगवाने पर विचार करें। अनजाने आगंतुकों के लिए दरवाजा खोलने से पहले उन्हें स्वयं की पहचान की पुष्टि करने के लिए कहें। उनके आपके घर के अंदर आने के बाद उन्हें अपने आसपास रखें, जहाँ तक हो सके अपने सामने या ऐसी जगह पर रखें जहाँ उन पर नज़र रखी जा सके। अपने पास हर समय मोबाइल फ़ोन रखने पर विचार करें।

संवेदनशील सामग्री

संवेदनशील या व्यक्तिगत रूप से पहचानी जा सकने वाली जानकारी (PII) वाली गोपनीय सामग्री का हमेशा उचित ढंग से निपटान करें या इसे नष्ट करें। PII में ऐसी कोई भी जानकारी शामिल है जो व्यक्तिगत प्रकृति की हो, जिसका प्रयोग आपकी पहचान करने के लिए किया जा सकता है।

पैदलयात्री की सुरक्षा

सार्वजनिक स्थानों पर यात्रा करते समय, चलते या जॉगिंग करते समय अपनी व्यक्तिगत सुरक्षा को प्राथमिकता दें। उचित सावधानियाँ बरतने से आप कमजोर पक्षों को और हिंसा या आक्रामकता का सामना करने के जोखिम को कम कर सकते हैं। समय से पहले सुरक्षित मार्ग प्लान करने, नियमित स्थानों पर जाते समय अपने मार्ग को बदलते रहने, और सुनसान या कम रोशनी वाले रास्तों, एकांत पार्किंग गैराज़ और दूर-दराज स्थित पार्किंग स्थलों जैसे संभावित खतरनाक स्थानों से बचने जैसे आसान तरीकों पर विचार करें।

5 U.S. होमलैंड सुरक्षा विभाग। संघीय अन्वेषण ब्यूरो। n.d. ***सुरक्षा और लचीलापन गाइड: अधिक उन्नत विस्फोटक उपकरण (C-IED) संकल्पनाएँ, सामान्य लक्ष्य, और उपलब्ध सहायता।*** 8 अगस्त, 2023 को देखा गया। पृष्ठ 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

जब भी आप सार्वजनिक स्थान पर हों, काम से जुड़ी किसी भी सामग्री या व्यक्तिगत जानकारी को छुपाने के लिए अपने विवेक का प्रयोग करें और सावधानी बरतें। सार्वजनिक स्थानों पर बैज पहनते हुए या पासवर्ड दर्ज करते हुए सावधानी बरतें। अधिक तथ्यों और सुझावों के लिए पैदल यात्री सुरक्षा के संबंध में राष्ट्रीय राजमार्ग ट्रैफ़िक सुरक्षा प्रशासन की वेबसाइट पर जाएँ।

स्थिति के संबंध में सतर्कता बनाए रखें

अगर आप सार्वजनिक क्षेत्र/परिवेश में होते हुए चिंतित हो जाते हैं या असुरक्षित महसूस करना शुरू कर देते हैं, तो लोगों के समूह के पास जाएँ। अगर यह संभव नहीं है, तो अपनी स्थिति संबंधी सतर्कता को बढ़ाने के लिए अपने मूवमेंट्स को समायोजित करें और निम्नलिखित सावधानियाँ बरतें:

- **अपने मोबाइल फ़ोन** को आपातकालीन कॉल करने की स्थिति में रखें।
- **सतर्क रहें** और अपनी सटीक लोकेशन और चारों ओर के वातावरण के प्रति सचेत रहें।
- **किन्हीं भी गहनों** या कीमती चीजों का प्रदर्शन करने से बचें।
- **क्षेत्र में रोशनी की व्यवस्था, लोकेशन** और अन्य स्थानीय व्यवसायों से नजदीकी पर विचार करें।
- **पीछे से आने वाले वाहनों से बचने** के लिए चलते समय सामने से आ रहे ट्रैफ़िक की ओर चलें।
- **अपने हाथों को खाली रखें** और अपने आसपास के वातावरण के प्रति सचेत रहें।
- **फ़ोन पर बात करने**, हैडफ़ोन्स पहनने या लंबे टेक्स्ट मैसेज भेजने से बचें।
- **चलते समय सचेत रहें** और अधिक समय लगाने से बचें।
- **बैंकिंग** ATM का प्रयोग करते समय, सबके सामने करेंसी को प्रदर्शित करने से बचें।

राइडशेयर सेवाएँ

किसी राइडशेयर एप्लिकेशन का प्रयोग करते हुए किसी मित्र या सहकर्मी को अपनी लोकेशन और गंतव्य स्थल के विवरण के बारे में सूचित करने पर विचार करें। राइड को स्वीकार करने और वाहन में प्रवेश करने से पहले चालक और वाहन का विवरण जाँचें।

संदिग्ध गतिविधि को पहचानें और रिपोर्ट करें

संदिग्ध गतिविधि को पहचानें और रिपोर्ट करें – जैसे आपके घर, कार्यस्थल या वाहन के आसपास लोगों का बिना किसी कारण के घूमना-फिरना, या लोगों का छुपकर आपकी तस्वीरें लेने की कोशिश करना। अगर आप किसी को अपने घर, कार्यस्थल या वाहन के पास कोई वस्तु या पैकेट छोड़ते हुए देखते हैं, तो इसकी जानकारी तुरंत पुलिस को दें। इस पर जाकर संदिग्ध गतिविधि को रिपोर्ट करने के बारे में अधिक जानकारी प्राप्त करें, "अगर आप कुछ देखते हैं, तो कुछ कहें®" अभियान।

व्यक्तिगत सुरक्षा उपकरण

किसी हमलावर को भटकाने के लिए पेप्पर स्प्रे, सुनने योग्य अलार्म, या अतिरिक्त व्यक्तिगत सुरक्षा उपकरण रखने पर विचार करें, ताकि आप आसपास के लोगों को सूचित कर सकें और स्वयं को बचकर भागने का अवसर दे सकें। जहाँ आप सक्षम हों, और संघीय और स्थानीय कानूनों और विनियमों के अनुसार व्यक्तिगत सुरक्षा उपकरण रखें और इनका इस्तेमाल करें।

निम्नलिखित चेतावनी संकेतों पर सावधानीपूर्वक ध्यान देना और तुरंत रिपोर्ट करना किसी संभावित घटना को नियंत्रित करने में सहायक हो सकता है:

- आपके, आपके घर, आपकी वस्तुओं या रोज़गार के स्थान के विरुद्ध **मौखिक या लिखित धमकियाँ।**
- **क्षतिग्रस्त या छेड़छाड़** की गई प्रणालियाँ और उपकरण।
- बैग्स, बॉक्सेज़, छुपा कर ले जाए जा रहे डिब्बों सहित—**संदिग्ध या लावारिस वस्तुएँ**—जिनमें खतरनाक सामग्री हो सकती है।
- इमारत के फ़्लोर प्लान, प्रवेश/निकास, एलेवेटर्स, अग्निशमन उपकरणों, जलापूर्ति की लोकेशन, और ताप, हवादारी और वातानुकूलन (HVAC) प्रणालियों के बारे में **संदिग्ध पूछताछ।**
- आग लगाने वाली सामग्री, पेंट्स, डीग्रीज़र्स, एल्कोहोल-बेस्ड क्लीनर्स, एयरोसोल्स और प्रोपेन गैस टैंकों सहित **ज्वलनशील या दहनशील सामग्री की असामान्य मात्रा या लोकेशन।**
- ऐसी **सोशल मीडिया मैसेजिंग** जो हमला करने वाले किसी भी चिह्न या विचारों को बढ़ावा देती है।

अधिक जानकारी के लिए संदिग्ध गतिविधि रिपोर्टिंग संकेतक और उदाहरण देखें।

टकराव

स्वयं को टकराव की स्थिति में पाना तनावग्रस्त कर सकता है। स्पष्ट दिखाई देने वाले ऐसे व्यवहार पर ध्यान केंद्रित किया जाना चाहिए जो किसी संभावित हिंसा का इशारा हो सकता है। इन स्थितियों में शांत रहना और यह निर्धारित करने के लिए स्थिति का आकलन करना महत्वपूर्ण है कि क्या बीच में आना सुरक्षित है। अपनी स्वयं की क्षमताओं की सीमाओं को समझें और तब सुरक्षा कर्मचारियों या कानून प्रवर्तन इकाई से सहायता माँगें जैसे ही ऐसा करना सुरक्षित हो।

अगर आप प्रशिक्षित और दक्ष हैं, तो गर्मागर्मी वाली स्थितियों को उद्देश्यपरक कार्रवाइयों के माध्यम से सुरक्षित ढंग से शांत करने पर विचार करें जिनमें कारगर ढंग से सुनना और संवाद करना शामिल है। याद रखें आप "मामले को शांत करने" का काम नहीं करते हैं; बल्कि यह लक्ष्य है।

सतर्क बने रहने और संभावित रूप से उग्र स्थितियों से निकलने के लिए सुझावों के बारे में जानने के लिए CISA की तनावग्रस्त स्थिति को शांत करने संबंधी शृंखला देखें।

मोटर वाहन और यात्रा

अपने घर या कार्यस्थल से निकलने से पहले अपने आसपास देखें और किन्हीं भी संदिग्ध वाहनों पर ध्यान दें जो वहाँ घात लगाए बैठे हों या बेवजह घूम रहे हों। वाहन के चारों ओर के क्षेत्र को जाँचें और देखें कि वहाँ कोई ऐसी चीज़ तो नहीं है जो आपके वाहन में या इसके आसपास नहीं होनी चाहिए। अगर कोई प्रतिकूल स्थिति उत्पन्न होती है, तो यह जानकारी पुलिस के लिए सहायक हो सकती है।

अगर संभव हो, तो अपनी यात्रा व्यवस्थाओं में दोहराए जाने वाले पैटर्न्स से बचें ताकि संभावित दुर्भावनापूर्ण व्यक्ति आपके कहीं होने के बारे में पूर्वानुमान न लगा सकें। जहाँ तक संभव हो, अपने मार्ग बदलते रहें और निकलने का समय बदलते रहें। सुनिश्चित करें कि आपकी यात्रा के दौरान वाहन के सभी दरवाजे और डिक्की लॉक हो। केवल हवादारी के लिए पर्याप्त खिड़कियाँ खोलें। सुरक्षित ढंग से वाहन चलाएँ और अपने आगे के वाहन से सुरक्षित दूरी बनाए रखें। और हमेशा सुनिश्चित करें कि आपके वाहन में आपकी यात्रा के लिए पर्याप्त ईंधन हो (या, अगर इलेक्ट्रिक वाहन है, तो पर्याप्त रूप से चार्ज हो)।

अगर आपको लगता है कि आपका पीछा किया जा रहा है, तो शांत रहने का प्रयास करें और अपने वाहन को चलाते रहें। सभी खिड़कियाँ बंद कर दें और सुनिश्चित करें कि आपके दरवाजे लॉक हैं। तुरंत कानून प्रवर्तन इकाई से संपर्क करें। अगर संभव हो तो नजदीकी पुलिस स्टेशन की ओर जाएँ—घर की ओर न जाएँ। किसी भी संदिग्ध वाहन का लाइसेंस प्लेट नंबर, मेक और मॉडल नोट करने का प्रयास करें।

अगर आप वाहनों के टकराने की किसी घटना में शामिल हैं या आपके वाहन में कोई मैकेनिकल गड़बड़ हो गई है, तो अपने आसपास देखें और तुरंत आपातकाल कर्मचारियों और वाहन टो सेवा से संपर्क करें। कानून प्रवर्तन इकाई के निर्देशों का पालन करें।

गुमनाम फ़ोन कॉल्स और धमकियाँ[6]

गुमनाम फ़ोन कॉल्स और धमकियाँ सामान्यत: डराने, चेतावनी देने और तनावग्रस्त करने के इरादे से दी जाती हैं। हमेशा निम्नलिखित काम करना याद रखें:

- **शांत रहें** और फ़ोन न काटें।
- **कॉलर को** जितनी देर संभव हो उतनी देर **लाइन पर बनाए रखें**। विनम्र बने रहें और उससे बात करने में रुचि दिखाएँ। वह ऐसी महत्वपूर्ण जानकारी दे सकता है जो पुलिस की जांच-पड़ताल की स्थिति में सहायक हो सकती है।
- अगर संभव हो, तो अपने आसपास किसी(किन्हीं) अन्य व्यक्ति(यों) को **सुनने और प्राधिकरणों को सूचित करने** में सहायता करने के लिए संकेत करें या नोट पास करें।
- जितनी संभव हो, उतनी जानकारी **लिखें**—कॉलर आईडी नंबर, धमकी के सटीक शब्द, आवाज या व्यवहार का प्रकार आदि—इससे जाँचकर्ताओं को सहायता मिलेगी।
- अगर संभव हो और कानूनी रूप से अनुमत हो, तो **कॉल को रिकॉर्ड करें।**

धमकी भरे या अपशब्द का प्रयोग करने वाले फ़ोन कॉल्स करना संघीय कानून के विरुद्ध है। अगर आपको ऐसे कोई कॉल्स प्राप्त होते हैं, तो अपनी स्थानीय कानून प्रवर्तन इकाई से संपर्क करें। इसके अतिरिक्त, आप धमकी के बारे में FBI को रिपोर्ट कर सकते हैं। सुझावों के लिए FBI धमकी और डराने संबंधी गाइड देखें।

बम से मारने की अधिकतर धमकियाँ टेलीफ़ोन के माध्यम से दी जाती हैं, इसलिए DHS की बम धमकी जाँच सूची और CISA की बम धमकी गाइड देखें, जिनमें इस बारे में निर्देश दिए गए हैं कि किसी बम धमकी पर कैसे प्रतिक्रिया करें और सूचना की ऐसी व्यापक सूची दी गई है जिससे कानून प्रवर्तन इकाई को बम धमकी के अन्वेषण में सहायता मिलेगी।

ऑनलाइन सुरक्षा

संभावित हानिकारक डाउनलोड्स से बचने के लिए केवल प्रतिष्ठित "ऐप स्टोर्स" से एप्लिकेशंस इन्स्टॉल करें। अज्ञात या सत्यापित न किए जा सकने योग्य स्रोतों से एप्लिकेशंस डाउनलोड न करें। इस पर ध्यान दें कि एप्लिकेशंस के पास आपके फ़ोन में अन्य जानकारी तक पहुँच रखने के लिए कौन-सी अनुमतियाँ हैं।

मज़बूत पासवर्ड बनाएँ और बनाए रखें जो आपके हर डिवाइस या खाते के लिए अलग हो और उन्हें व्यवस्थित करने के लिए पासवर्ड प्रबंधक का प्रयोग करें। जो भी खाता या ऐप मल्टीफ़ैक्टर सत्यापन (MFA) ऑफ़र करता है, उसके लिए इसे ऑन करें। MFA को इनेबल करने से आपके ईमेल, सोशल मीडिया, वित्तीय और अन्य महत्वपूर्ण जानकारी जैसी व्यक्तिगत जानकारी की रक्षा करने में सहायता मिलती है।

सॉफ्टवेयर अपडेट्स

सॉफ्टवेयर को अद्यतित (अपडेटित) रखें ताकि हमलावर संवेदनशील जानकारी या कमज़ोरियों का लाभ न उठा सकें। बहुत से ऑपरेटिंग सिस्टम्स ऑटोमेटिक अपडेट्स ऑफ़र करते हैं। अगर ऐसा विकल्प है, तो उपकरण की एप्लिकेशन सुरक्षा सेटिंग्स में ऑटोमेटिक अपडेट्स को ऑन करें।

अपने वेब ब्राउज़र में—"http" की बजाय यूनिफ़ॉर्म रिसोर्स लोकेटर्स (URLs) खोजें जो "https" से शुरू होते हैं—जो यह दर्शाता है कि वे साइट्स एनक्रिप्शन का प्रयोग करती हैं। हाइपर टेक्स्ट ट्रांसफ़र प्रोटोकॉल सिक्योर (HTTPS) ऐसा इंटरनेट संचार प्रोटोकॉल है जिसका प्रयोग किसी प्रयोक्ता के वेब ब्राउज़र और जिस वेबसाइट से वह कनेक्ट है, उनके बीच सूचना के प्रेषण को एनक्रिप्ट और सुरक्षित करने के लिए किया जाता है। इसे प्रयोक्ताओं द्वारा वेबसाइट्स पर जाने के दौरान उनकी जानकारी की अखंडता और गोपनीयता की बेहतर ढंग से रक्षा करने के लिए डिज़ाइन किया गया है।[7]

ऑनलाइन सुरक्षित बने रहने के बारे में अधिक जानकारी के लिए CISA के हमारे विश्व को सुरक्षित करें को देखें।

6 संघीय अन्वेषण ब्यूरो. n.d. धमकी और डराने संबंधी गाइड। 8 अगस्त, 2023 को देखा गया। fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 U.S. होमलैंड सुरक्षा विभाग। 2018. हायपर टेक्स्ट ट्रांसफर प्रोटोकॉल सिक्योर (HTTPS). 12 फरवरी, 2024 को देखा गया। cisa.gov/resources-tools/resources/hyper-text-transfer- protocol-secure-https.

इलेक्ट्रॉनिक उपकरणों का प्रयोग

मोबाइल उपकरणों और नेटवर्क्स में ऑनलाइन बैंकिंग जानकारी, ईमेल्स, टेक्स्ट मैसेज, कॉन्टेक्ट्स, सोशल मीडिया और पिक्चर्स जैसा विभिन्न तरह का व्यक्तिगत विवरण हो सकता है। अपने उपकरण को सुरक्षित रखने के लिए सभी सुरक्षा विशेषताओं का इस्तेमाल करें और सुनिश्चित करें कि आप उपकरण के सॉफ्टवेयर को लगातार अपडेट करते हैं। अपने फ़ोन और सिम कार्ड्स के लिए मज़बूत पासकोड्स बनाएँ और अनावश्यक लोकेशन सेवाओं को अक्षम कर दें।[8]

हमेशा वॉयसमेल एक्सेस के लिए अपने डिफ़ॉल्ट पिन को बदलते रहें। अपने फ़ोन पर लोकेशन सेवाओं को सीमित करने पर विचार करें और अन्य व्यक्तियो को थर्ड-पार्टी एप्लिकेशंस के माध्यम से आपकी मूवमेंट्स को ट्रैक करने और आपके घर या कार्यस्थल का पता जानने से रोकने के लिए गोपनीयता सेटिंग्स की समीक्षा करें। अपने उपकरण(णों) की सुरक्षा को बढ़ाने के लिए Apple और Android की गोपनीयता और सुरक्षा उपायों की समीक्षा करें।

सोशल मीडिया

इंटरनेट जानकारी, शिक्षा और मनोरंजन का मूल्यवान स्रोत हो सकता है। बहरहाल, आपके द्वारा ऑनलाइन—विशेष रूप से सोशल मीडिया पर प्रकाशित की जाने वाली व्यक्तिगत जानकारी की मात्रा को सीमित करने के लिए सतर्क रहें और सावधानियाँ बरतें।

लोकप्रिय सोशल मीडिया साइट्स व्यक्तियों को व्यक्तिगत प्रोफ़ाइल बनाने और अन्यों के साथ ऑनलाइन बातचीत करने की सुविधा देती हैं। व्यावसायिक नेटवर्किंग साइट्स पर लोग अपने प्रोफ़ाइल्स में अधिक विवरण जोड़ सकते हैं और काम के इतिहास और अन्य पृष्ठभूमि जानकारी शामिल कर सकते हैं। जहाँ इन टूल्स से आपको दूसरों के साथ संवाद करने और अपनी पेशेवर पृष्ठभूमि विज्ञापित करने में सहायता मिलती है, वहीं व्यक्तिगत जानकारी को ऑनलाइन प्रकाशित करने से संभावित जोखिम भी होते हैं।

व्यक्तिगत जानकारी पोस्ट करते समय सावधानी बरतें। दुर्भावनापूर्ण तत्व हैक करते हुए या पहचान चुराते हुए फ़ोटोज़, जन्मदिन, पूरे नाम, घर के पते और ईमेल विवरण से लोकेशन डेटा का प्रयोग कर सकते हैं। इसके अतिरिक्त, रोज़गार, परिवार के सदस्यों, शौकों या वाहन के विवरण से संबंधित जानकारी अपराधियों और उग्र पक्षों के लिए कीमती होती है। आपके परिवार के लोग और मित्र भी अनजाने में आपके बारे में तब जानकारी साझा कर सकते हैं अगर वे अपने स्वयं के प्रोफ़ाइल की जानकारी को सुरक्षित करने के लिए उचित उपाय नहीं करते हैं। याद रखें, इंटरनेट पर कोई "डिलीट" बटन नहीं है। सावधानी से साझा करें, क्योंकि अगर आप किसी पोस्ट या पिक्चर को अपने प्रोफ़ाइल से डिलीट कर देते हैं, तब भी संभावना है कि किसी ने इसे देख लिया है।

कुछ सोशल मीडिया नेटवर्किंग साइट्स आपके द्वारा पोस्ट किए गए डेटा का स्वामित्व रखती हैं और आपका विवरण थर्ड पार्टीज़ को बेच देंगी। इन साइट्स पर अपनी गोपनीयता और लोकेशन टैगिंग सेटिंग्स की नियमित रूप से समीक्षा करें, अन्यथा आप अपने व्यक्तिगत प्रोफ़ाइल के कुछ हिस्से या इसे पूरी तरह से आपके लिए अनजान विशाल व्यक्तियों द्वारा देखे जाने का जोखिम उठाते हैं।[9, 10]

8 संघीय संचार आयोग। 2019. अपने स्मार्ट उपकरण की रक्षा करें। 20 सितंबर, 2023 को देखा गया। fcc.gov/consumers/guides/protect-your-mobile-device.

9 यूनाइटेड किंगडम की सरकार। राष्ट्रीय साइबर सुरक्षा केंद्र। 2019. सोशल मीडिया: इसे सुरक्षित ढंग से कैसे इस्तेमाल करें। 20 सितंबर, 2023 को देखा गया। ncsc.gov.uk/guidance/social- media-how-to-use-it-safely.

10 साइबर सुरक्षा और अवसंरचना सुरक्षा एजेंसी, राष्ट्रीय साइबर गठबंधन। 2019. सोशल मीडिया साइबर सुरक्षा। 20 सितंबर, 2023 को देखा गया। cisa.gov/sites/default/files/ publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

सोशल मीडिया गोपनीयता और लोकेशन सेटिंग्स की समीक्षा करें

X जिसे पहले Twitter के रूप में जाना जाता था

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

Instagram

- **help.instagram.com/811572406418223**
- IOS: **help.instagram.com/171821142968851**
- Android: अपने एंड्रॉयड डिवाइस पर सेटिंग्स > ऐप्स > **Instagram** > अनुमतियाँ > लोकेशन पर जाएँ

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**

डॉक्सिंग

डॉक्सिंग का मतलब है—किसी ओपन स्रोत या छेड़छाड़ की गई सामग्री से—किसी व्यक्ति की व्यक्तिगत रूप से पहचाने जा सकने वाली जानकारी (PII)—या किसी संगठन की संवेदनशील जानकारी एकत्र करना और इसे सार्वजनिक क्षेत्र में छोड़ने या दुर्भावनापूर्ण उद्देश्यों के लिए इसका प्रयोग करना।[11, 12] अपराधी इस जानकारी का प्रयोग संभावित लक्ष्यों को ब्लैकमेल करने या उनमें डर बैठाने के लिए कर सकते हैं।

जब आप ऑनलाइन पोस्ट करते हैं, इस बारे में सतर्क रहना महत्वपूर्ण है कि आप क्या और कैसे पोस्ट कर रहे हैं। अगर आप उचित गोपनीयता सेटिंग्स का प्रयोग किए बिना बहुत अधिक जानकारी पोस्ट करते हैं, तो आप अपनी व्यक्तिगत सुरक्षा को जोखिम में डाल सकते हैं। लोग इस जानकारी का प्रयोग आपके संबंधों, राय, रुचि के स्थानों और अन्य विषयों की पिक्चर बनाने में कर सकते हैं जिसका लाभ वे भविष्य में उठा सकते हैं।

डेटा ब्रोकर्स भी इस व्यक्तिगत जानकारी को एकत्र कर सकते हैं और इसे अन्य कंपनियों को बेच सकते हैं। अपने डेटा के ब्रोकर्स तक जाने के जोखिम को कम करने के लिए:

- PII को साझा करने से **बचें।**
- सोशल मीडिया पर ऐसे लोगों को स्वीकार **न करें** जिन्हें आप वास्तविक जीवन में नहीं जानते।
- यह **सुनिश्चित करें** कि जिन ऐप्स का प्रयोग आप कर रहे हैं उनमें एंड-टू-एंड एनक्रिप्शन है।
- ऐप अनुमतियों को **सीमित करें।**
- अपने नाम के लिए **Google Alerts सेट करें।**
- मुख्य डेटा ब्रोकर और लोक खोज साइटों से ऑप्ट-आउट करने के लिए **समय निकालने** या किसी सेवा द्वारा आपके लिए यह करने के लिए सदस्यता लेने पर विचार करें।

लोकेशन-आधारित जानकारी, विशेष रूप से GPS-सक्षम सेल फोनों और मोबाइल डिवाइसेज़ से सोशल नेटवर्कों पर पोस्ट की जा सकती है। यह जानकारी सुरक्षित नहीं है और इसे ऐसे लोगों सहित किसी के भी द्वारा देखा जा सकता है जो आपको नुकसान पहुंचाना चाह सकते हैं। अपने द्वारा पोस्ट की जाने वाली चीज़ों का ट्रैक रखें और यह सुनिश्चित करने के लिए ज़िम्मेदारी से पोस्ट करें कि आप द्वारा सार्वजनिक की जाने वाली जानकारी से कोई व्यक्ति जोखिम में न पड़ जाए।

अगर आपको लगता है कि आपकी निजी जानकारी उजागर की जा रही है:

- **घटना की रिपोर्ट** स्थानीय कानून प्रवर्तन इकाई या किसी भी ऐसे प्लेटफॉर्म पर करें जहाँ आपकी निजी जानकारी जारी की गई हो।
- जो कुछ हुआ हो, उसे **दस्तावेज़** में दर्ज करें और जाँचकर्ताओं से साझा करने के लिए स्क्रीनशॉट लें।
- यह **निर्धारित करें** कि किस जानकारी का फायदा उठाया गया था, खतरे की गंभीरता क्या है और खतरे का बिंदु क्या है।
- वेबसाइटों या एप्लिकेशनों से जानकारी को हटाने के लिए **वेबसाइट प्रशासकों से सहयोग करें।**
- गोपनीयता की **सेटिंग्स** को सबसे निजी विकल्पों पर **कॉन्फिगर करें।**
- चोरी की पहचान के **संकेतों पर निगाह रखें,** वित्तीय लेखाओं की निगरानी करें, धोखाधड़ी के अलर्ट्स सेट करें और सभी ऑनलाइन खातों के लिए लॉग-इन और पासवर्ड की जानकारी को बदलें।

निजी जानकारी को उजागर करने संबंधी कानून क्षेत्राधिकार के अनुसार भिन्न होते हैं, इसलिए यह महत्वपूर्ण है कि जब आप कमी और रोकथाम करने के विकल्पों पर विचार करें, तब आप अपने क्षेत्र में इनके बारे में जानें। अगर अपनी शारीरिक सुरक्षा के बारे में चिंतित हों, तो अगले चरणों के लिए स्थानीय कानून प्रवर्तन इकाई से संपर्क करें।

पहचानें और फिशिंग की रिपोर्ट करें

अपराधी प्रायः आप द्वारा हानिकारक लिंकों, ईमेल्स या अटैचमेंट्स को खोले जाने के लिए फिशिंग के हथकंडों का उपयोग करते हैं जिनमें आपकी निजी जानकारी का अनुरोध किया जा सकता है या आपके डिवाइसेज़ इन्फेक्ट हो सकते हैं। ऐसे मैसेज प्रायः ऐसे दिखने के लिए तैयार किए जाते हैं कि मानों वे किसी विश्वसनीय व्यक्ति या संगठन से आए हों।

फिशिंग मैसेज ईमेल, टेक्स्ट, सोशल मीडिया पर डायरेक्ट मैसेज या फोन कॉल के रूप में आ सकते हैं। तात्कालिक या भावनात्मक भाषा, निजी जानकारी भेजने के अनुरोधों, अविश्वस्त छोटे URLs और गलत ईमेल पते और लिंकों से सावधान रहें।

अगर आपको यह संदेह होता है कि आपको किसी फिशिंग हमले का शिकार बनाया गया है, तो किसी भी लिंक या अटैचमेंट पर क्लिक न करें। इसकी बजाए, रिपोर्ट करें और इसके बाद मैसेज को मिटा दें।

11 U.S. होमलैंड सुरक्षा विभाग। 2024. भागीदारी और सहभागिता कार्यालय। निजी जानकारी उजागर करने के खतरे वाले व्यक्तियों के लिए संसाधन 09 फरवरी, 2024 को देखा गया। dhs.gov/ publication/resources-individuals-threat-doxing.

12 यूरोपीय परमाणु अनुसंधान परिषद। 2017. कंप्यूटर सुरक्षा: अगले स्तर में प्रवेश करें: Doxware. 12 दिसंबर, 2023 को देखा गया। home.cern/news/news/computing/computer- security-enter-next-level-doxware.

संसाधन

शारीरिक सुरक्षा

- CISA सुरक्षा और लचीलापन गाइड
- CISA सक्रिय शूटर के लिए तैयारी
- FBI धमकी और डराने संबंधी गाइड
- CISA बम की धमकियाँ
- CISA मामले को शांत करने संबंधी शृंखला

स्थिति के प्रति सतर्कता

- पीछा करने को रोकना, जागरूकता, और संसाधन केंद्र (SPARC)

ऑनलाइन सुरक्षा

- CISA अपने विश्व को सुरक्षित करें
- CISA गोपनीयता और मोबाइल उपकरण ऐप्स
- CISA इनसाइट्स: महत्वपूर्ण अवसंरचना पर डॉक्सिंग के प्रभावों को कम करना
- CISA सोशल मीडिया साइबर सुरक्षा