सुरक्षा जागरूकता संबंधी गाइड - घर पर सुरक्षित तरीके से काम करना

संक्षेप में

कोरोना वायरस की वजह से कई संगठनों को अपने कर्मचारियों से घर से काम करने को कहना पड़ रहा है। इसमें मुश्किलें सामने आ सकती हैं क्योंकि कई संगठनों के पास ऐसी नीतियाँ, टेक्नोलॉजी और ट्रेनिंग नहीं होती जिनकी मदद से वे कर्मचारियों से घर से काम कराने पर उन्हें साइबर ख़तरों से सुरक्षित रख सकें। साथ ही, कई कर्मचारी घर से काम करने को लेकर असहज महसूस कर सकते हैं या हो सकता है कि वे इस बारे में कुछ जानते ही न हों। इस गाइड का उद्देश्य है कि आप उन लोगों को सुरक्षित रखने के लिए जल्द से जल्द और ज़्यादा से ज़्यादा प्रशिक्षित कर सकें। इस गाइड को इस्तेमाल करने के संबंध में अगर आपके पास कोई सवाल हो, तो हमसे इस पते पर संपर्क करें: support@sans.org

चूँकि आपके कर्मचारी शायद बहुत ज़्यादा बदलावों और तनाव से गुज़र रहे होंगे, और आपके संगठन के पास शायद समय और संसाधनों की भी कमी होगी, इसलिए यह गाइड ट्रेनिंग को जितना हो सके उतना सरल बनाने की कोशिश करती है। हमारा सुझाव है कि आप सबसे गंभीर ख़तरों पर ही ध्यान दें, जिनका प्रभाव सबसे ज़्यादा होगा। ऐसे ख़तरों के बारे में हमने आगे बताया है। इन्हें शुरुआती कदम मानकर चलें। अगर ऐसे कुछ और विषय या ख़तरे हैं, जिन्हें आप जोड़ना चाहते हैं, तो ज़रूर जोड़ें। बस इतना ध्यान रखें कि जितने ज़्यादा तौर-तरीके, प्रक्रियाएँ या टेक्नोलॉजी आपके कर्मचारियों के लिए ज़रूरी होंगी, उतनी कम संभावना कर्मचारियों द्वारा उन सब को लागू कर पाने की होगी।

इस गाइड का इस्तेमाल कैसे करें

हमारा सुझाव है कि आप सबसे पहले इस गाइड में दी गई सामग्री को पढ़ें और दी गई अलग-अलग सामग्री के लिंक देखें ताकि आपको पता चल सके कि क्या-क्या उपलब्ध है। आप देखेंगे कि हमने हर ख़तरे के लिए अलग-अलग तरह की सामग्री दी है, जिसका इस्तेमाल आप अपने संगठन को प्रशिक्षित करने और जागरूक बनाने के लिए कर सकते हैं। इनकी मदद से आप वे तरीके चुन पाएँगे जो आपके हिसाब से आपकी ज़रूरतों और संस्कृति के लिए सबसे प्रभावी रूप से काम करेंगे। आप क्या हासिल करने की कोशिश कर रहे हैं, इसे बेहतर तरीके से समझने के लिए, इस दस्तावेज़ को पढ़ने के बाद इस किट में आई फ़ैक्टशीट और कम्युनिकेशन टेम्पलेट, दोनों को पढ़ें। एक बार दस्तावेज़ों को पढ़ लेने के बाद, ऐसे दो मुख्य समूह हैं जिनके साथ आपको बातचीत करनी होगी।

1. **सुरक्षा टीम**: आप किन मुख्य ख़तरों से निपटने की कोशिश कर रहे हैं, उन्हें बेहतर समझने के लिए अपनी सुरक्षा टीम से बातचीत करें। हमने इस गाइड में ऐसे कुछ ख़तरों की पहचान की है जो हमारे हिसाब से घर से काम करने वाले कर्मचारियों के लिए सबसे आम ख़तरे हैं, पर हो सकता है कि आपके ख़तरे इनसे अलग हों। एक आम ग़लती जो सुरक्षा टीमें करती हैं, वो है सभी ख़तरों से निपटने की कोशिश करना और इस प्रक्रिया में वे लोगों को बहुत सारी नीतियाँ और

ज़रूरतें बताकर परेशान कर देती हैं। इस ग़लती से बचना ज़रूरी है। जिन ख़तरों से आप निपटने वाले हैं, उन्हें जितना हो सके उतना कम रखने की कोशिश करें। एक बार उन ख़तरों की पहचान कर लेने और उनकी प्राथमिकता तय कर लेने के बाद, उन तौर-तरीकों की पुष्टि करें जिनके ज़रिए उन ख़तरों से निपटा जाएगा। जैसा कि पहले बताया गया है, अगर आपके संगठन के पास इसके लिए समय और संसाधन नहीं हैं, तो नीचे हमने जो बातें बताई हैं, उनका फ़ायदा उठाएँ।

2. **कम्युनिकेशन**: एक बार अपने सबसे बड़े मानवीय ख़तरों की और उनसे निपटने के मुख्य तौर-तरीकों की पहचान कर लेने के बाद, उन तौर-तरीकों के बारे में अपने कर्मचारियों को प्रशिक्षित और जागरूक करने के लिए अपनी कम्युनिकेशन टीम के साथ मिलकर काम करें। सबसे असरदार सुरक्षा जागरूकता कार्यक्रमों में कम्युनिकेशन टीम का सहयोग बहुत मज़बूत होता है। अगर संभव हो, तो कम्युनिकेशन टीम के किसी व्यक्ति को अपनी सुरक्षा टीम में रखें। अपने कर्मचारियों से बातचीत करते समय, उनकी दिलचस्पी बनाए रखने के लिए आप इस बात पर ज़ोर दे सकते हैं कि इस ट्रेनिंग से न केवल वे अपने दफ़्तर में सुरक्षित रहेंगे बल्कि उन्हें अपने घर को भी साइबर हमलों से सुरक्षित बनाने में मदद मिलेगी। इससे वे और उनका परिवार भी सुरक्षित रहेगा।

इन दोनों समूहों के साथ काम करने का मतलब है कि आप अपने कर्मचारियों के लिए आसानी से सुरक्षा मुहैया कराने की कोशिश कर रहे हैं और उन्हें प्रेरित कर रहे हैं।तौर-तरीकों में बदलाव लाने के लिए ये दो बुनियादी बातें हैं। इस कार्यक्रम को शुरू करने के लिए आपको जिन लोगों की सलाह और सुझावों की ज़रूरत होगी, ऐसे महत्वपूर्ण लोगों का एक सलाहकार बोर्ड बना लेना अच्छा रहेगा। अपनी सुरक्षा और कम्युनिकेशन टीम के अलावा आप जिन विभागों के साथ मिलकर काम करने के बारे में सोच सकते हैं, उनमें मानव संसाधन और कानूनी विभाग शामिल हैं।

MGT433 डिजिटल डाउनलोड पैकेज

SANS Institute दो दिनों का ट्रेनिंग कोर्स MGT433: एक काफ़ी प्रभावी सुरक्षा जागरूकता कार्यक्रम को बनाने, उसका मूल्यांकन और रखरखाव करने का तरीका मुहैया कराता है। यह गहन ट्रेनिंग एक काफ़ी प्रभावी सुरक्षा जागरूकता कार्यक्रम बनाने के लिए पूरी जानकारी, ज़रूरी कौशल, रूपरेखा और संसाधन मुहैया कराती है, जिसकी मदद से आप अपने लोगों के लिए ख़तरे का मूल्यांकन कर सकते हैं और उससे असरदार तरीके से निपट सकते हैं। इस गाइड के साथ हम पाठ्यक्रम के डिजिटल डाउनलोड पैकेज का मुफ़्त एक्सेस दे रहे हैं, जिसमें टेम्पलेट और योजना के संसाधन दिए गए हैं। हालाँकि शायद यह इस पहल की आवश्यकताओं के दायरे से बाहर की बात है, पर ये सामग्रियाँ ऐसे मामलों में बहुत काम की हो सकती हैं, जिनमें संगठनों का आकार बहुत बड़ा हो या लागू करने की प्रक्रिया जटिल हो।

कर्मचारियों के सवालों के जवाब देना

अपने कर्मचारियों से बातचीत करने और उन्हें प्रशिक्षित करने के अलावा, हम आपको ऐसी किसी टेक्नोलॉजी या फ़ोरम का इस्तेमाल करने का सुझाव देते हैं जहाँ आप लोगों के सवालों के जवाब दे सकें, और साथ के साथ दे सकें तो और भी बेहतर। इसमें ये चीज़ें शामिल हो सकती हैं - ख़ास तौर पर इस काम के लिए बनाए गए ईमेल अड्रेस, Skype या Slack चैट चैनल, या किसी तरह का ऑनलाइन फ़ोरम बनाना, जैसे कि Yammer से। हमारा दूसरा सुझाव है, एक सुरक्षा वेबकास्ट होस्ट करना। आप इसे हफ़्ते में कई बार प्रसारित कर सकते हैं जिससे लोग अपने मनमुताबिक समय चुन सकें और लाइव इवेंट में शामिल हो सकें। वे इसमें अपने सवाल भी पूछ सकते हैं। आपका उद्देश्य है जितना हो सके उतना ज़्यादा लोगों तक सुरक्षा पहुँचा पाना और लोगों के सवालों के जवाब दे पाना। अपने कर्मचारियों से बातचीत करने और सुरक्षा जैसे विषय को लोगों के लिए आसान बनाने का यह एक सुनहरा मौका है, इसका पूरा फ़ायदा उठाने की कोशिश करें। ध्यान रखें कि इसे असरदार बनाने के लिए आपको सुरक्षा चैनल को सँभालने और सवालों के जवाब देने के लिए एक व्यक्ति नियुक्त करना होगा।

ख़तरे और प्रशिक्षण सामग्री

कहीं दूर से काम करने वाले कर्मचारियों के लिए हमने तीन मुख्य ख़तरों की पहचान की है, जिनसे आपको निपटना होगा। कहानी इनसे शुरू होती है और इस बात की पूरी संभावना है कि यही आपके लिए सबसे ज़्यादा काम के साबित होंगे। नीचे दिए गए हर ख़तरे के साथ कई संसाधनों के लिंक दिए गए हैं, जिनकी मदद से उस विषय का प्रशिक्षण दिया जा सकता है और उसके बारे में बातचीत की जा सकती है। हम कई तरह से बातचीत करने वाली सामग्री मुहैया कराते हैं ताकि आप इसमें से वह सामग्री चुन सकें जो आपकी संस्कृति के अनुसार सबसे ज़्यादा प्रभावी हो। साथ ही, लगभग सारी सामग्री कई भाषाओं में उपलब्ध है। अगर यह सामग्री आपके लिए बहुत ज़्यादा है और आपके पास समय बहुत कम है, तो हमारा सुझाव है कि नीचे दी गई दो विषय-सामग्री पढ़ें और उसे अमल में लाएँ।

1. घर से सुरक्षित तरीके से काम करने के बारे में ज़रूरी जानकारी (आपकी डिप्लॉयमेंट किट में शामिल है)।
2. घर को साइबर हमले से सुरक्षित बनाना - वीडियो (अंग्रेज़ी) यहाँ अन्य भाषाओं में भी उपलब्ध है।

सोशल इंजीनियरिंग

जिन सबसे बड़े ख़तरों का सामना कहीं दूर से काम करने वाले कर्मचारियों को करना पड़ेगा उनमें से एक हैं सोशल इंजीनियरिंग हमले, ख़ास तौर से आजकल के बहुत तेज़ी से बदलते हुए और हड़बड़ी की स्थिति वाले परिवेश में। सोशल इंजीनियरिंग एक मनोवैज्ञानिक हमला होता है जिसमें हमलावर अपने शिकार को धोखा देकर या बेवकूफ़ बनाकर उससे

कोई ग़लती करवा लेता है। भ्रम और बदलाव के दौर में यह काम और भी आसान हो जाता है। मुख्य बात है लोगों को सोशल इंजीनियरिंग के बारे में और सोशल इंजीनियरिंग हमले के सबसे आम संकेतों को पहचानने के बारे में प्रशिक्षित करना और यह बताना कि किसी ऐसे संकेत की पहचान करने पर क्या करना चाहिए। पक्का करें कि आप सिर्फ़ ईमेल फ़िशिंग हमलों पर ध्यान केंद्रित करने के बजाय दूसरे तरीकों पर भी पूरा ध्यान दे रहे हैं, जैसे कि फ़ोन कॉल, मैसेज, सोशल मीडिया या फ़र्ज़ी ख़बरें। इस विषय का प्रशिक्षण देने और इसे अच्छी तरह समझाने के लिए आपको जिस सामग्री की ज़रूरत होगी, वह सामग्री आपको हमारे सोशल इंजीनियरिंग के बारे में सामग्री फ़ोल्डर में मिलेगी। इसके अलावा, यहाँ दो SANS सुरक्षा जागरूकता वीडियो दिए गए हैं, जिन्हें आप सामग्री में जोड़ सकते हैं। ये वीडियो भी कई भाषाओं में उपलब्ध हैं।

- सोशल इंजीनियरिंग (अंग्रेज़ी) यहाँ अन्य भाषाओं में भी उपलब्ध है।
- फ़िशिंग (अंग्रेज़ी) यहाँ अन्य भाषाओं में भी उपलब्ध है।

मज़बूत पासवर्ड

जैसा कि वार्षिक Verizon DBIR में बताया गया है, दुनिया भर में होने वाले हैकिंग के मामलों के मुख्य कारणों में से एक है, कमज़ोर पासवर्ड। इस ख़तरे से निपटने में मदद के लिए चार मुख्य तौर-तरीके नीचे दिए गए हैं। इस विषय का प्रशिक्षण देने और इसे अच्छी तरह समझाने के लिए आपको जिस सामग्री की ज़रूरत होगी, वह सामग्री और इन चार बुनियादी तौर-तरीकों के बारे में जानकारी आपको हमारे पासवर्ड फ़ोल्डर में मिल जाएगी।

- पासफ़्रेज़ (ध्यान दें कि पासवर्ड की जटिलता और पासवर्ड की समय-सीमा ख़त्म होना, दोनों चीज़ें अब लागू नहीं होती हैं।
- हर खाते के लिए बिल्कुल अलग पासवर्ड
- पासवर्ड मैनेजर
- MFA (मल्टी-फ़ैक्टर ऑथेंटिकेशन) अक्सर टू-फ़ैक्टर ऑथेंटिकेशन या दो-चरणों की पुष्टि भी कहा जाता है

अपडेट किए गए सिस्टम

तीसरा ख़तरा नए वर्शन के इस्तेमाल से जुड़ा है। पक्का करें कि आपके कर्मचारी जो भी टेक्नोलॉजी इस्तेमाल करते हैं, उसके ऑपरेटिंग सिस्टम, ऐप्लिकेशन और मोबाइल ऐप के सबसे नए वर्शन का इस्तेमाल कर रहे हों। इसके लिए, निजी डिवाइस इस्तेमाल कर रहे लोगों को ऑटोमैटिक अपडेट की सुविधा चालू करने की ज़रूरत हो सकती है। इस विषय का प्रशिक्षण देने और इसे अच्छी तरह समझाने के लिए आपको जिस सामग्री की ज़रूरत होगी, वह सामग्री मैलवेयर या घर को साइबर हमले से सुरक्षित बनाना फ़ोल्डर में मिल जाएगी।

ध्यान देने योग्य अन्य विषय

- **वाई-फ़ाई**: अपने वाई-फ़ाई एक्सेस पॉइंट को सुरक्षित बनाना। इसके बारे में घर को साइबर हमले से सुरक्षित बनाना सामग्री में बताया गया है। साथ ही,घर को साइबर हमले से सुरक्षित बनाना - वीडियो (अंग्रेज़ी) भी देखें जो कि यहाँ अन्य भाषाओं में भी उपलब्ध है।.

- **VPN**: VPN क्या होता है और आपको इसका इस्तेमाल क्यों करना चाहिए। हम VPN संबंधी OUCH न्यूज़लेटर **पढ़ने का सुझाव देते हैं।.**

- **कहीं दूर से काम करना**: यह उन लोगों के लिए है जो कहीं दूर से काम कर रहे हैं पर घर से नहीं, जैसे कि किसी कैफ़े, एयरपोर्ट या होटल से। हमारा कहीं दूर से काम करना - वीडियो (अंग्रेज़ी) देखें जो कि यहाँ अन्य भाषाओं में भी उपलब्ध है।.

- **बच्चे / मेहमान**: इस बात पर ज़ोर देने के लिए कि परिवार वालों / मेहमानों को काम से जुड़े डिवाइस एक्सेस नहीं करने चाहिए, हमारा कहीं दूर से काम करना - ट्रेनिंग वीडियो (अंग्रेज़ी) देखें जो कि यहाँ अन्य भाषाओं में भी उपलब्ध है।.

- **पता लगाना / प्रतिक्रिया**: क्या आप चाहते हैं कि लोगों के घर से काम करने के दौरान अगर उन्हें लगता है कि कोई घटना हो गई है, तो वे उसकी सूचना दें? अगर ऐसा है, तो आपके मुताबिक उन्हें क्या सूचना देनी चाहिए और कब? इसके बारे में हमारी हैक किया गया सामग्री में बताया गया है।

OUCH न्यूज़लेटर

साथ ही, अपने कार्यक्रम के लिए सार्वजनिक तौर पर उपलब्ध OUCH न्यूज़लेटर की मदद लीजिए। हर एक न्यूज़लेटर का अनुवाद बीस से भी ज़्यादा भाषाओं में किया गया है। नीचे OUCH न्यूज़लेटर की एक सूची दी गई है। हमारे ख़याल से इनसे आपकी "घर पर सुरक्षित तरीके से काम करना" पहल में बहुत मदद मिलेगी। आप सारे न्यूज़लेटर, ऑनलाइन जाकर OUCH सुरक्षा जागरूकता न्यूज़लेटर आर्काइव में देख सकते हैं।.

संक्षिप्त विवरण

Four Steps to Staying Secure (सुरक्षित रहने के लिए चार कदम)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (घर को साइबर हमले से सुरक्षित बनाना)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

सोशल इंजीनियरिंग

SOCIAL ENGINEERING (सोशल इंजीनियरिंग)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (मैसेजिंग / स्मिशिंग)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (खास तौर पर किसी के लिए तैयार किए गए स्कैम)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (CEO फ्रॉड)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (फ़ोन कॉल से होने वाले हमले / धोखाधड़ी)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (फ़िशिंग रोकना)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (सोशल मीडिया के ज़रिए आपके साथ धोखाधड़ी करना)

https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

पासवर्ड

Making Passwords Simple (पासवर्ड आसान बनाना)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (अपने खातों को ज़्यादा सुरक्षित करना)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

थोड़े और

Yes, You Are a Target (हाँ, आप टारगेट हैं)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (स्मार्ट होम डिवाइस)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

फटाफट काम करने वाले उपाय

उपाय और युक्तियाँ जिन्हें आप आसानी से समझ में आने वाले फ़ॉर्मैट में शेयर कर सकते हैं।

- घर पर अपना वायरलेस नेटवर्क सुरक्षित बनाने के लिए आप जो सबसे असरदार कदम उठा सकते हैं, वे हैं - डिफ़ॉल्ट एडमिन पासवर्ड बदलना, WPA2 एन्क्रिप्शन चालू करना और अपने वायरलेस नेटवर्क के लिए एक मज़बूत पासवर्ड इस्तेमाल करना।
- आपके घर के नेटवर्क से जितने भी डिवाइस जुड़े हैं, उन सब पर नज़र रखें, जिनमें बेबी मॉनिटर, गेमिंग कंसोल, टीवी, उपकरण और यहाँ तक कि आपकी कार भी शामिल है। पक्का करें कि ये सारे डिवाइस एक मज़बूत पासवर्ड द्वारा सुरक्षित किए गए हों और/या इनके ऑपरेटिंग सिस्टम सबसे नए वर्शन पर चल रहे हों।
- घर पर अपने कंप्यूटर को सुरक्षित रखने के सबसे असरदार तरीकों में से एक यह भी है कि ऑपरेटिंग सिस्टम और आपके ऐप्लिकेशन, दोनों पैच किए हुए और अपडेटेड हों। जब भी संभव हो ऑटोमैटिक अपडेट की सुविधा चालू करें।
- अंत में, आपकी सूझ-बूझ ही आपकी सुरक्षा का सबसे कारगर हथियार है। अगर कोई ईमेल, ऑनलाइन मैसेज या

फ़ोन कॉल अजीब, संदिग्ध या कुछ ज़्यादा ही अच्छा लगे, तो वह हमला हो सकता है।

- पक्का करें कि आपके हर अकाउंट के लिए एक बिल्कुल अलग पासवर्ड हो। क्या आपको सभी पासवर्ड/पासफ़्रेज़ याद रखना मुश्किल लगता है? अपने सभी पासवर्ड सुरक्षित रूप से स्टोर करने के लिए एक पासवर्ड मैनेजर का इस्तेमाल करने पर विचार करें।
- किसी भी खाते को सुरक्षित रखने के लिए आप दो चरणों की पुष्टि का तरीका अपना सकते हैं, जो सबसे अच्छे तरीकों में से एक है। दो चरणों की पुष्टि का मतलब है कि आपको एक पासवर्ड और एक कोड जो कि आपके मोबाइल डिवाइस पर भेजा जाता है या उसके द्वारा जेनरेट किया जाता है, दोनों की ज़रूरत होती है। दो चरणों की पुष्टि की सुविधा देने वाली सेवाओं के उदाहरणों में Gmail, Dropbox और Twitter शामिल हैं।
- जब कोई हमलावर आपको बेवकूफ़ बनाकर आपसे किसी ख़तरनाक लिंक पर क्लिक करवाने या किसी ईमेल का अटैचमेंट खुलवाने की कोशिश करता है, तो उसे फ़िशिंग कहते हैं। ऐसे किसी भी ईमेल या ऑनलाइन मैसेज को लेकर सतर्क रहें जो हड़बड़ी पैदा करता हो, जिसमें स्पेलिंग की ग़लतियाँ हों या जो आपको "प्रिय ग्राहक" कहकर संबोधित करता हो।

आँकड़े

इस स्थिति में व्यवहार से जुड़े आँकड़े इकट्ठा करना मुश्किल है क्योंकि लोग घर पर किस तरह से व्यवहार करते हैं, इसका मूल्याँकन कर पाना और मुश्किल है। साथ ही, इनमें से कुछ व्यवहार काम से नहीं भी जुड़े हो सकते हैं (जैसे कि अपने वाई-फ़ाई डिवाइस की सुरक्षा करना)। हालाँकि आप माप सकते हैं कि जुड़ाव कितना है। हमने देखा है कि इनके जैसे निजी या भावनात्मक विषय बहुत दिलचस्पी वाले हो सकते हैं और दूसरे विषयों के मुकाबले कहीं ज़्यादा ध्यान आकर्षित कर सकते हैं। वैसे, इनके जैसे आँकड़े काम के हो सकते हैं।

- **इंटरैक्शन**: लोग कितनी बार सवाल पूछ रहे हैं, कोई आइडिया पोस्ट कर रहे हैं, या आपके द्वारा होस्ट किए जा रहे किसी फ़ोरम या सुरक्षा चैनल पर कितनी बार मदद के लिए अनुरोध कर रहे हैं?
- **सिम्युलेशन**: अलग-अलग तरह के सोशल इंजीनियरिंग हमलों वाली स्थितियों की नकल करें (सिम्युलेशन), जैसे कि फ़िशिंग, मैसेजिंग या फ़ोन कॉल के ज़रिए होने वाले हमले।

आँकड़ों की और ज़्यादा विस्तृत सूची के लिए MGT433 डिजिटल डाउनलोड पैकेज से इंटरैक्टिव "सुरक्षा जागरूकता आँकड़ों की मेट्रिक्स" डाउनलोड करें।.

लाइसेंस

कॉपीराइट © 2020, SANS Institute. सारे अधिकार SANS Institute के पास सुरक्षित हैं। उपयोगकर्ता के पास, SANS Institute की पहले से साफ़-साफ़ लिखित अनुमति के बिना, किसी भी उद्देश्य के लिए, किसी भी माध्यम से (प्रिंट, इलेक्ट्रॉनिक या कोई अन्य तरीका) इस सामग्री को कॉपी करने, फिर से बनाने, फिर से प्रकाशित करने, वितरित करने, दिखाने, बदलाव करने, या पूरी सामग्री या इसके किसी हिस्से के आधार पर इससे जुड़ी कोई सामग्री बनाने के अधिकार नहीं हैं। साथ ही, उपयोगकर्ता के पास, SANS Institute की पहले से साफ़-साफ़ लिखित अनुमति के बिना इन दस्तावेज़ों को किसी भी तरीके से और किसी भी आकार या रूप में बेचने, किराये पर या लीज़ पर देने, इनका व्यापार करने या इन्हें स्थानांतरित करने का अधिकार भी नहीं होगा।

डिप्लॉयमेंट किट के लेखक

लैंस स्पिट्ज़नर के पास साइबर सुरक्षा का 20 साल का अनुभव है। उनके अनुभव में साइबर ख़तरों पर रिसर्च, सिक्योरिटी आर्किटेक्चर और सुरक्षा संबंधी जागरूकता और प्रशिक्षण जैसे क्षेत्र शामिल हैं। उन्होंने "हनीनेट प्रोजेक्ट" की स्थापना करके और हनीनेट बनाकर धोखाधड़ी और साइबर इंटेलिजेंस के क्षेत्रों की शुरुआत करने में मदद की। SANS प्रशिक्षक के तौर पर, उन्होंने MGT433:सुरक्षा जागरूकता और MGT521: सुरक्षा संस्कृति पाठ्यक्रम बनाए। साथ ही, लैंस ने सुरक्षा से जुड़ी तीन किताबें प्रकाशित की हैं, 25 से ज़्यादा देशों के साथ सलाहकार के तौर पर काम किया है और लोगों को होने वाले ख़तरों से निपटने के उद्देश्य से सुरक्षा जागरूकता और संस्कृति कार्यक्रम बनाने में 350 से ज़्यादा संगठनों की मदद की है। लैंस सामुदायिक सुरक्षा से जुड़े कई प्रोजेक्ट पर काम करते हैं, Twitter पर नियमित रूप से सक्रिय रहते हैं (@lspitzner) और अक्सर प्रेज़ेंटेशन देते रहते हैं। सूचना सुरक्षा (इन्फ़ॉर्मेशन सिक्योरिटी) के क्षेत्र में आने से पहले स्पिट्ज़नर सेना की रैपिड डिप्लॉयमेंट फ़ोर्स में एक आर्मर ऑफ़िसर के तौर पर काम कर चुके हैं और उन्होंने इलिनॉय विश्वविद्यालय से MBA किया है।

SANS Institute के बारे में

SANS Institute, 1989 में एक सहकारी अनुसंधान और शिक्षा संगठन के रूप में स्थापित किया गया था। SANS दुनिया भर में सरकारी और व्यावसायिक संस्थानों के पेशेवरों को साइबर सुरक्षा प्रशिक्षण और प्रमाणपत्र देने वाला सबसे भरोसेमंद और सबसे बड़ा संस्थान है। SANS के नामी प्रशिक्षक, ऑनलाइन और साइबर सुरक्षा प्रशिक्षण के 200 से ज़्यादा लाइव इवेंट में 60 से ज़्यादा अलग-अलग पाठ्यक्रम पढ़ाते हैं। GIAC, जो कि SANS Institute का एक सहयोगी है, 35 से ज़्यादा प्रैक्टिकल और टेक्निकल साइबर सुरक्षा प्रमाणपत्रों के ज़रिए किसी पेशेवर की योग्यताओं का सत्यापन करता है। क्षेत्रीय स्तर पर मान्यता प्राप्त स्वतंत्र सब्सिडियरी के रूप में काम करने वाला SANS Technology

Institute साइबर सुरक्षा में मास्टर्स डिग्री देता है। SANS, InfoSec (सूचना सुरक्षा) समुदाय को बहुत सारे संसाधन मुफ़्त में मुहैया करवाता है, जिसमें कंसेंसस प्रोजेक्ट, रिसर्च रिपोर्ट और न्यूज़लेटर शामिल हैं। यह इंटरनेट के पहले से चेतावनी देने वाले सिस्टम--इंटरनेट स्टॉर्म सेंटर का संचालन भी करता है। SANS के केंद्र में सुरक्षा से जुड़े बहुत सारे पेशेवर लोग हैं जो बड़ी कंपनियों से लेकर विश्वविद्यालयों तक, तरह-तरह के अंतरराष्ट्रीय संगठनों का प्रतिनिधित्व करते हैं और पूरे सूचना सुरक्षा समुदाय की मदद करने के लिए मिलकर काम करते हैं। (https://www.sans.org)