

girls who
code

Girls Who Code At Home

साइबर जासूस

गतिविधि अवलोकन

क्या आप जानते हैं कि पहला स्मार्टफोन 1992 में बनाया गया था? भले ही हम साइमन फोन को "स्मार्टफोन" कहते थे, लेकिन आज हम जो फोन इस्तेमाल करते हैं उसकी तुलना में इस फोन के फंक्शन और लुक बहुत ही बुनियादी था। दायीं ओर साइमन फोन की एक आईफोन 4एस से तुलना करने वाली एक फोटो देखें!



तस्वीर स्रोत: [समय](#)

साइमन फोन में एक टचस्क्रीन था जिसे केवल नोट्स, एक एड्रेस बुक, कैलेंडर, घड़ी को शामिल करने और कॉल लेने के लिए इस्तेमाल किया जा सकता था। आप इस फोन का डेमो देखने के लिए यह [वीडियो](#) देख सकते हैं। [वाईफाई](#) या [5G](#) के माध्यम से इंटरनेट से जुड़े लगभग सभी प्रकार के इलेक्ट्रॉनिक उपकरणों के साथ पहले स्मार्टफोन के बाद से प्रौद्योगिकी का तेजी से विकास हुआ है। हमारे सभी यंत्रों से जुड़ी सुविधा के साथ व्यापक संभावित सुरक्षा जोखिम आता है।

आप सोच रहे होंगे कि यह महत्वपूर्ण क्यों है? अगर आप ऑनलाइन चीजें खरीदते हैं, कॉलेज का आवेदन भरते या किसी नए ऐप के लिए साइन अप करते हैं, तो आप संवेदनशील सूचना प्रदान करते हैं जैसे क्रेडिट कार्ड का नंबर, आपका नाम, जन्मतिथि और कभी-कभी आपका सामाजिक सुरक्षा नंबर। 2019 में 15 में से लगभग 1 लोग [पहचान की धोखाधड़ी](#) के शिकार हो गए थे। खुद की रक्षा करने का पहला चरण यह है कि कुछ तरह के हमलों के बारे में शिक्षित हों जो आपको खतरे में डाल सकते हैं। साइबर सुरक्षा विशेषज्ञ किसी भी कंप्यूटर (यानी इंटरनेट से जुड़ा हुआ कोई इलेक्ट्रॉनिक उपकरण) में सुरक्षा उपायों को लागू करने और संभावित खतरों को पहचानने के लिए जिम्मेदार हैं। [साइबर सुरक्षा](#) एक तेज़ी से बढ़ता उद्योग है जो सभी अमेरिकी तकनीक नौकरियों का लगभग 32-45% है जिस में **\$83,000** का औसत मूल वेतन होता है। इस अनप्लग्ड गतिविधि में आप साइबर हमले की पहचान करने के लिए कहानी में दिखाए गए संकेतों का पालन करते हुए साइबर सुरक्षा विशेषज्ञ, या साइबर जासूस की भूमिका निभाएंगी।

सीखने के लक्ष्य

इस गतिविधि को पूरा कर लेने पर आप निम्नलिखित कर सकेंगे...

- ❑ विभिन्न प्रकार के सामान्य वायरसों और साइबर हमलों की पहचान।

सामग्रियां

→ कोई अतिरिक्त सामग्री नहीं चाहिए

पूर्व ज्ञान

→ कोई पूर्व ज्ञान नहीं चाहिए!

वुमन इन टेक स्पोटलाइट: जया बालू



तस्वीर स्रोत:
[बुद्धिमान CISO](#)

2017 में, जया बालू को [शीर्ष 100 CISO](#) (चीफ़ इन्फ़ॉर्मेशन सिक््योरिटी ऑफ़िसर) में एक नियुक्त किया गया था। वे [क्रिप्टोग्राफी](#) में विशेषज्ञ हैं, और संचार को सुरक्षित करने की तकनीक का अध्ययन करती हैं। जया की 9 वर्ष की आयु से ही कंप्यूटर में रुचि थी! [टफ्ट्स \(Tufts\) यूनिवर्सिटी](#) से ग्रेजुएट होने के बाद जया ने बैंकर्स ट्रस्ट (Bankers Trust) के लिए इंटरनेट सिक््योरिटी ट्रेनर के रूप में कार्य किया। अपने अनुभव के जरिए उन्होंने यह जाना कि अमेरिकी सरकार साइबर सुरक्षा को एक हथियार के रूप में देखती है, जिससे यह कारण स्पष्ट हो गया कि क्यों अमेरिकी सरकार ने अपनी टेक्नॉलजी को जनता से छिपा कर रखा था। हालांकि, जया के विचार इससे अलग थे, उनका मानना था कि साइबर सुरक्षा को सभी की जीवन रक्षा के लिए सार्वजनिक रूप से उपलब्ध होना चाहिए।

टेक्नॉलजी के विकास और अधिक “स्मार्ट” यंत्रों के आविष्कार के साथ, साइबर सुरक्षा पहले से कहीं अधिक महत्वपूर्ण हो गई है। अब चूंकि सारे डिवाइस एक ही सिस्टम के तहत जुड़े हुए हैं, अतः बहुत से लोग साइबर हमलों के प्रति असुरक्षित हो सकते हैं। जया अब सभी के लिए मुफ्त एंटीवायरस सॉफ्टवेयर लाने हेतु [अवास्ट \(Avast\)](#) के लिए कार्य करती हैं। अवास्ट (Avast) के साथ अपने कार्य के एक भाग के रूप में, वे खतरों का पता लगाने और कंप्यूटरों को सुरक्षित बनाने के लिए [क्वांटम कम्प्यूटिंग](#) और [आर्टिफिशियल इंटेलिजेंस](#) को लागू करने पर कार्य करती हैं। उनका मानना है कि साइबर सुरक्षा एक *मौलिक अधिकार* है जिसे मुक्त रूप से उपलब्ध होना चाहिए।

साइबर सुरक्षा के महत्व के बारे में, और कनेक्टेड 5G यंत्रों के जरिए सिस्टम को कैसे आसानी से हैक किया जा सकता है इस बारे में और जानने के लिए यह [वीडियो](#) देखें। जया के बारे में अधिक जानना चाहते हैं? हमारे रोजमर्रा के जीवन को साइबरसुरक्षा कैसे प्रभावित करती है इस बारे में उनकी 2017 की [TED talk](#) देखें और सिंगुलैरिटी यूनिवर्सिटी पर उनकी [प्रोफाइल](#) का अन्वेषण करें।

झलक

एक कंप्यूटर वैज्ञानिक होना, कोडिंग में बेहतरीन होने की तुलना में अधिक है। इस बात के बारे में सोचने में थोड़ा समय बिताएं कि कैसे जया और उनका काम उन शक्तियों से संबंधित है जो महान कंप्यूटर वैज्ञानिक की रचना का केंद्र रहा है - बहादुरी, लचीलेपन, रचनात्मकता और उद्देश्य के निर्माण के दौरान ध्यान केंद्रित करते हैं।

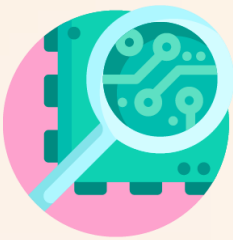


प्रयोजन

जया मानती हैं कि साइबर सुरक्षा सॉफ्टवेयर को सशुल्क सेवा की बजाय निःशुल्क उपलब्ध होना चाहिए। यह बात, अमेरिकी सरकार द्वारा इस ज्ञान को देखे जाने के तरीके से बिल्कुल विपरीत है। साइबर सुरक्षा सॉफ्टवेयर को निःशुल्क बांटने के लाभ क्या हैं? सॉफ्टवेयर को निःशुल्क बांटने के कुछ संभावित जोखिम क्या हैं?

परिवार के किसी सदस्य या मित्र के साथ अपनी प्रतिक्रियाएँ साझा करें। चर्चा में शामिल होने हेतु दूसरों को जया के बारे में अधिक पढ़ने के लिए प्रोत्साहित करें!

चरण 1: साइबर सुरक्षा क्या है? (2-3 मिनट)



एक हैकर की कल्पना करें। वे कैसे दिखते हैं? वे क्या करते हैं? कुछ फिल्में देखने के बाद आप बहुत से कंप्यूटरों के सामने खड़े काला हूडी पहने एक आदमी की कल्पना कर सकते हैं। क्या आप जानते हैं कि लगभग 20% हैकर महिलाएं हैं? **हैकर** वह व्यक्ति होता है जो अपने कंप्यूटर प्रोग्रामिंग के ज्ञान का उपयोग कंप्यूटर सिस्टम की संभावित कमज़ोरियों को उजागर करने में करता है। हो सकता है कि आप सोचें कि हैकर बुरा व्यक्ति होता है, पर कई हैकर असल में कंप्यूटरों की रक्षा करने का और साइबर अपराधियों के विरुद्ध सुरक्षा उपायों को और मजबूत बनाने का कार्य करते हैं। इस प्रथा को **साइबर सुरक्षा कहा जाता है।**

साइबर सुरक्षा साधारण तौर पर कंप्यूटर (कोई भी इलेक्ट्रॉनिक यंत्र जो डेटा को स्टोर और प्रोसेस कर सकता है), सर्वर, नेटवर्क, और डेटा को साइबर हमलों से बचाने की प्रथा है। लगभग सभी प्रकार की इलेक्ट्रॉनिक डिवाइसों के **वाईफाई** या **5G** के माध्यम से इंटरनेट से जुड़े होने के कारण साइबर हमलों से हमारी जानकारी की रक्षा करना अब पहले से भी अधिक जरूरी है। आप प्रसिद्ध व्यक्तियों की निजता के लीक होने, सरकारों की संवेदनशील जानकारी के जारी होने से हुए कुछ मशहूर हमलों से लेकर टीवी पर क्राइम शोज़ से परिचित होंगे, या आप व्यक्तिगत रूप से ऐसे किसी व्यक्ति को जानते होंगे जिस पर साइबर हमला हुआ है।

2019 में 15 में से लगभग 1 लोग **पहचान की धोखाधड़ी के शिकार** हो गए थे। खुद की रक्षा करने का पहला चरण यह है कि कुछ तरह के हमलों के बारे में शिक्षित होना है जो आप और आपके व्यक्तिगत डेटा को खतरे में डाल सकते हैं। इस गतिविधि में हम आपको कुछ आम हमलों के उदाहरण दिखाएंगे और इन संभावित खतरों से खुद की रक्षा करने की कुछ कार्रवाई योग्य चरण समझाएंगे!

चरण 2: गतिविधि के निर्देशों की समीक्षा करें (2 मिनट)

इस गतिविधि में आप साइबर हमलों में विशेषज्ञता वाले एक जासूस, या **साइबर जासूस** की भूमिका निभाएंगे। इसमें अपनी साहसिक गतिविधि चुनें गतिविधि में आप तय करेंगे कि साइबर हमले का जवाब देने के लिए आप क्या कदम उठाएंगे।



कहानी के पहले दृश्य में आपको घटना की जानकारी और परिस्थिति से संबंधित कुछ सुराग मिलेंगे। कहानी के प्रत्येक दृश्य के अंत में आपको आगे क्या करना है इसके दो विकल्प दिए जाएंगे। विकल्प को चुनने के बाद, आप अपने विकल्प से संबद्ध निर्देशों का पालन करेंगे। निर्देश आपके प्रत्येक विकल्प के आधार पर भिन्न होंगे और कहानी के समग्र परिणाम को प्रभावित करेंगे। यदि आपको जो परिणाम मिला वह पसंद नहीं है, तो वापस जाएं और कहानी को फिर से दोहराएं!

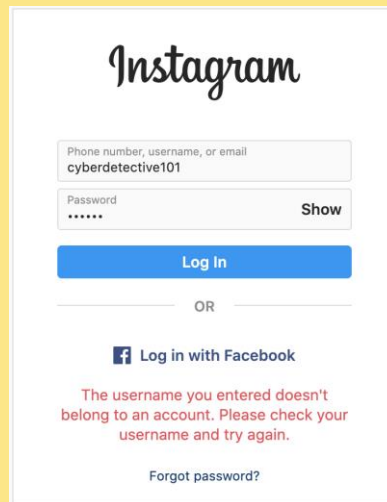
अब जबकि आपको इस गतिविधि के निर्देशों का सारांश मिल गया है, अब अपना जासूसी हैट पहनें और आभासी मैग्निफाइंग ग्लास थामें और काम शुरू करें!

माता-पिता/शिक्षक के लिए सुझाव

इस गतिविधि को अधिक सक्रिय बनाना चाहते हैं? हमारा सुझाव है कि दृश्यों से एक मिनी स्कैवेंजर हंट बनाया जाए और अपने साइबर जासूस के लिए निर्देश अपडेट करें!

चरण 3: इंस्टाग्राम संकट के बारे में पढ़ें (10-15 मिनट)

किसी भी सामान्य सुबह की तरह, आप जागते हैं, अपना फोन चालू करते हैं, और तत्काल इंस्टाग्राम खोलते हैं। जब आप अपनी आँखें मलते हुए नींद उड़ा रहे होते हैं, आपको अपने स्क्रीन पर कुछ अलग दिखाई देता है। कुछ और बार आँखें मलने के बाद, आपको निम्नलिखित संदेश नज़र आता है:



आपने जो यूज़रनेम दर्ज किया है, लगता है कि वह किसी खाते से संबंधित नहीं है। कृपया अपने यूज़रनेम की जाँच करें और दोबारा प्रयास करें।

आप सोचते हैं, “हूँ, अजीब बात है, शायद मैंने गलत पासवर्ड टाइप किया हो?” आप फिर से लॉग इन करने का प्रयास करते हैं और वहीं त्रुटि संदेश मिलता है। आप सोचते हैं, “इसका क्या मतलब हो सकता है? मुझे अपना यूज़रनेम और पासवर्ड पता है!!”

अब आप क्या करेंगे?

- A. हटाओ इसे, फोन रख देंगे और स्कूल के लिए तैयार होने लगेंगे। आप बाद में फिर से लॉग इन करने की कोशिश करेंगे। पेज [6 पर जाएं](#)।
- B. परेशान होना त्रुटि संदेश को गूगल करके पता लगाने कि कोशिश करेंगे कि आगे क्या करना चाहिए। पेज [7 पर जाएं](#)।

पेज 6

आप अपने रोज की दिनचर्या के लिए तैयार होने लगते हैं लेकिन आपको मन ही मन लगता है कि कहीं कुछ गड़बड़ है। आप फिलहाल के लिए इसे नज़रअंदाज करते हैं, स्कूल के लिए तैयार होना जरूरी है। आप नाश्ता करते हैं, परिवार को अलविदा कहते हैं और बस स्टॉप की ओर बढ़ते हैं ताकि आप स्कूल पहुँच सकें।

बस में बैठे-बैठे आप समय काटने के लिए इंस्टाग्राम में लॉग इन करने की फिर से कोशिश करते हैं। आप लॉगिन क्रेडेंशियल भरते हैं, और खास ध्यान रखते हैं कि आपके यूज़रनेम या पासवर्ड में कोई गलती न हो। आपको अब भी वही त्रुटि मिलती है, अब क्या करें?

- A. आप त्रुटि संदेश को गूगल करके समझने की कोशिश करते हैं कि इसका क्या मतलब है। पेज [7 पर जाएं](#)।
- B. आप मान लेते हैं कि इंस्टाग्राम में कुछ गड़बड़ है और संदेश को फिर से नज़रअंदाज कर देते हैं। आप अपनी ईमेल की जाँच करने लगते हैं। पेज [9 पर जाएं](#)।

पेज 7

आप त्रुटि संदेश को गूगल सर्च में कॉपी और पेस्ट करते हैं और आपको एक [Quora प्रश्न](#) दिखाई देता है।

प्रश्न: मैं इंस्टाग्राम में लॉग इन करने की कोशिश कर रहा हूँ लेकिन साइट का कहना है कि मेरा यूजरनेम किसी खाते से संबंधित नहीं है। क्या किसी को पता है कि इसे कैसे फिक्स करते हैं?

उत्तर: फिर से जाँच करें कि आप सही वर्तनी का उपयोग कर रहे हैं। विराम चिह्न, कैपिटलाइज़ेशन, वर्तनी, प्रतीक। सबकुछ। जरूरत पड़े तो कॉपी और पेस्ट करें।

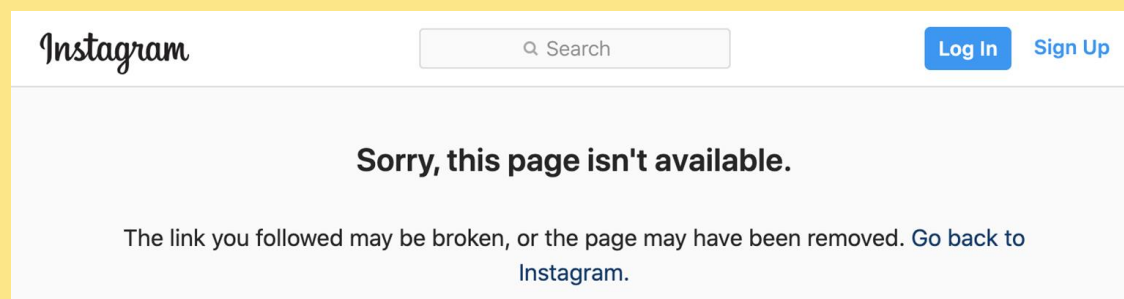
अब भी काम नहीं बन रहा है?

इसकी बजाय फेसबुक या ईमेल से लॉगिन करने की कोशिश करें।

अब भी काम नहीं बन रहा है?

हो सकता है आपका खाता अक्षम या बैन कर दिया गया हो (यानी आपने इंस्टाग्राम की नीति का उल्लंघन किया हो सकता है)। यह देखने के लिए क्या ऐसा हुआ है, किसी कंप्यूटर के वेब ब्राउज़र पर जाएं और "http://www.instagram.com/[your profile here]" टाइप करके देखें कि क्या आपका खाता पॉप अप होता है। यदि ऐसा नहीं होता है, तो आपको डिलीट कर दिया हो सकता है। नया खाता बनाएं, या इंस्टाग्राम टीम से संपर्क करें। यदि ऐसा होता है, तो पहले दो विकल्पों को फिर से आजमाएं। अब भी काम नहीं बना? इंस्टाग्राम टीम को ईमेल करें।

ऊपर Quora उत्तरों में मिले निर्देशों का पालन करें। आपको पहले अपने क्रेडेंशियल्स से लॉग करने की कोशिश करनी चाहिए, और फिर से जाँचना चाहिए कि आपके यूजरनेम और पासवर्ड की वर्तनी सही है। कोई फायदा नहीं। अब भी काम नहीं बन रहा है। फिर, आप फेसबुक से लॉगिन करने की कोशिश करते हैं, *बेकार है!* आपको थोड़ा बुरा लगता है, पता नहीं क्या हो रहा है। आप सबसे अंतिम चरण आजमाते हैं। आप अपने फोन पर सफ़ारी खोलते हैं और "<http://www.instagram.com/cyberdetective101>" टाइप करते हैं।



“क्षमा करें, यह पेज उपलब्ध नहीं है”

कहानी को जारी रखने के लिए [पेज 8](#) पर जाएं।

पेज 8

अंतिम चरण, आप मन में उम्मीद कर रहे थे कि आपको अंतिम चरण पूरा नहीं करना पड़ेगा। आप **मदद** बटन खोजते हैं और विषयों को पढ़ते हैं। आप लोकप्रिय विषय के तहत **लॉगिन ट्रबलशूटिंग** को चुनते हैं। फिर आप “I can't locate my account or don't know my username on Instagram” को चुनते हैं और उत्तर पढ़ते हैं।

यदि आपको अपना यूजरनेम दर्ज करने के बाद आपका खाता नहीं मिल रहा है:

- सुनिश्चित करें कि आपने अपना यूजरनेम सही दर्ज किया है, खास तौर से अगर उसमें दोहराए गए वर्ण हैं।
- अपना यूजरनेम दर्ज करते समय @ प्रतीक शामिल मत करें।

यदि आपको लगता है कि आपके खाते के किसी और के हाथ में लग जाने से आपका यूजरनेम बदल गया है:

- जाँच करें कि क्या आपको इंस्टाग्राम से कोई ईमेल आया है जो कहता है कि आपके खाते की जानकारी बदली गई है।
- किसी मित्र से आपकी प्रोफाइल में जाने और आपके वर्तनाम यूजरनेम का स्क्रीनशॉट लेने के लिए कहें।

इस बारे में अधिक जानें कि यदि आपको **लगता है कि आपका खाता हैक हो गया है** तो क्या करना चाहिए।

आप ये सभी सुझाव आजमाते हैं और अंतिम वाक्य को देखते हैं। आप सोचते हैं, “क्या मेरा खाता हैक किया गया है?” अब आप क्या करेंगे?

- A. आप सोचते हैं, “किसी को मेरा खाता हैक करने में क्यों दिलचस्पी हो सकती है? मेरे तो ज्यादा फॉलोअर भी नहीं हैं और मेरा खाता निजी है!” आप इसे नज़रअंदाज कर देते हैं और दोपहर में फिर से जाँच करने का निश्चय करते हैं। [पेज 9 पर जाएं](#)।
- B. आप सोचते हैं, “हो सकता है किसी ने मेरा खाता हैक कर लिया है।” आप [लिंक](#) पर क्लिक करते हैं और अगले चरण का पालन करते हैं। पेज [10 पर जाएं](#)।

पेज 9

जब आप अपना ईमेल स्कैन करते हैं, आपकी नज़र एक ईमेल पर पड़ती है जो कहता है, “यदि आप अपना इंस्टाग्राम खाता वापस चाहते हैं तो हमसे संपर्क करें”। आप ईमेल पर क्लिक करके खोलते हैं और विवरण पढ़ते हैं।

हैलो @cyberdetective101,

हमने आपके खाते पर कब्जा कर लिया है और आपके फोटो, मित्र और जानकारी देख ली है। यदि आप आज रात तक [इस खाते](#) में \$2,000 भेजकर जवाब नहीं देते हैं, तो हम आपका खाता डिलीट कर देंगे और आपकी व्यक्तिगत जानकारी बेच देंगे।

इंस्टाग्राम से मदद के लिए संपर्क मत करें क्योंकि हमने आपकी सारी जानकारी सफलतापूर्वक बदल दी है और यदि आप अपने खाते को बहाल करने की कोशिश करते हैं तो हमें पता चल जाएगा और हम उसे तत्काल डिलीट कर देंगे।

आपको इस सब पर भरोसा नहीं हो रहा है! अब आप क्या करेंगे?

- A. आप पैसे भेजो। अब सबकुछ ठीक हो जाना चाहिए, है ना? [page 11 पर जाएं](#)।
- B. आप वाकई में हैक हो गए! आप संदेश को नज़रअंदाज कर देते हैं और सीधे इंस्टाग्राम मदद पेज पर जाते हैं। पेज [10 पर जाएं](#)।

पेज 10

इंस्टाग्राम मदद पेज को पढ़ते समय, आपकी नज़र [मेरा खयाल है कि मेरा इंस्टाग्राम खाता हैक हो गया है](#) पर पड़ती है। आप लिंक पर क्लिक करते हैं और इंस्टाग्राम हेल्प इनफार्मेशन में दिए गए निर्देशों का पालन शुरू करते हैं।

आप इंस्टाग्राम के संदेश के लिए अपने ईमेल की जाँच करते हैं। आप अपने ईमेल को विस्तार से पढ़ते हैं और अपने ट्रैश फोल्डर की भी जाँच करते हैं। आपको इंस्टाग्राम से लगभग 2 दिन पहले आया एक ईमेल दिखता है जिसमें सूचना है कि आपका ईमेल पता बदल गया है। आप [अपने खाते को यहाँ सुरक्षित करें](#) लिंक पर क्लिक करके परिवर्तन को बदलने की कोशिश करते हैं।

आपके खाते की पुष्टि करने के लिए आपको अपनी पहचान का सत्यापन करना है, लेकिन आप किसी भी रीकवरी विकल्प को नहीं पहचानते हैं। आपके खाते पर ईमेल और फोन नंबर बदल गया है।

अब केवल एक तरीका बचा है जिसमें आपको खाते को रिपोर्ट करने के लिए चरणों का पालन करना है और भगवान का नाम लेना है। आप अपने अनुरोध के लिए इंस्टाग्राम के जवाब की प्रतीक्षा करते हैं।

[पेज 12](#) पर जाएं।

पेज 11

आप फटाफट अपने माता-पिता के क्रेडिट कार्ड की जानकारी निकालते हैं, और मन ही मन कहते हैं, “वाह, मुझे खुशी है कि मेरी माँ ने मुझे ऐप स्टोर पर मेरे खाते में अपने कार्ड की जानकारी सहजने दी!” कार्ड की जानकारी लेकर, आप ईमेल में दिए लिंक को क्लिक करते हैं, और पैसे भेजने के निर्देशों का अनुसरण करते हैं। आप चैन की सांस लेते हैं और अपने खाते के अपनी तरफ वापस किए जाने का इंतज़ार करते हैं। अंत में यह दुःस्वप्न लगभग खत्म हो गया है।

आप अपने फोन पर एक वेब ब्राउज़र खोलते हैं और आपको एक पॉप अप दिखता है जो कहता है।

आपका फोन हैक हो गया है!
डिवाइस पर होने वाली सभी हरकतें एक हैकर ट्रैक कर रहा है।

तत्काल कार्रवाई की जरूरत है!

आपको एक नया ईमेल मिलता है। आप उसे देखते हैं और वह आपके हैकर से आया एक और ईमेल है, जो कहता है:

हैलो @cyberdetective101,

आपका फोन हमारे नियंत्रण में है और हमारे पास आपकी सभी फोटो, संपर्क, और जानकारी है। यदि आप आज रात तक **इस खाते** में \$10,000 भेजकर जवाब नहीं देते हैं, तो हम आपकी व्यक्तिगत जानकारी और सब मित्रों के संपर्क बेच देंगे।

आपके सिस्टम हैक हो गए हैं और अब आपके पहचान की धोखेधड़ी का शिकार बनने का जोखिम है।

[पेज 12](#) पर जाएं।

चरण 4: निष्कर्ष (10-15 मिनट)

संपूर्ण कहानी के दौरान आपने जो मार्ग चुना उसके आधार पर आपको अनेकों साइबर हमलों द्वारा हैक किया जा सकता है।



हमला #1: कमज़ोर पासवर्ड (5-8 मिनट)

यदि किसी हैकर ने आपके खाते में प्रवेश कर लिया है, तो इसका सबसे संभावित कारण एक **कमज़ोर/अरक्षित पासवर्ड** है। पासवर्ड बनाते समय एक वैध खाता बनाने में सक्षम होने से पहले कुछ सरल आवश्यकताएं हो सकती हैं। कुछ प्रतिबंधों में शामिल हैं:

- कम से कम 6-8 वर्ण
- अपरकेस और लोअरकेस अक्षरों का मिश्रण
- कम से कम एक संख्या का उपयोग
- कम से कम एक विशेष वर्ण

भले ही आप न्यूनतम आवश्यकताओं को पूरा करने वाला पासवर्ड बना लें, किसी हैकर को उसे समझने में मात्र कुछ सेकंडों से लेकर एक दिन तक का समय ही लगेगा! अधिकांश खातों को हैक करना हैकरों के लिए बेहद सरल और सस्ता है। यह तुलना करने के लिए नीचे दिया गया चार्ट देखें कि पासवर्ड कैसे आपके ऑनलाइन खातों की अरक्षितता को प्रभावित कर सकते हैं।

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



Cybersecurity that's approachable.
Find out more at hivesystems.io

तस्वीर स्रोत: रेडिट

चरण 4: निष्कर्ष (जारी)

पासवर्डों के बारे में अभी-अभी जो सीखा उस पर चिंतन करने में एक पल बिताएं और यह देखने के लिए खुद प्रयोग करें कि क्या आप सुरक्षित पासवर्ड बना सकते हैं!

- ❑ निम्नलिखित पासवर्डों को 1-5 तक रैंक करें, जहाँ 1 का मतलब सबसे अधिक सुरक्षित और 5 का मतलब सबसे कम सुरक्षित पासवर्ड है। पासवर्डों को रैंक करने में आपकी मदद करने के लिए, हमने कुछ कॉलम शामिल किए हैं: वर्णों की संख्या और वर्ण में भिन्नता।
 - ❑ प्रत्येक पासवर्ड के लिए वर्णों की संख्या और वर्ण की भिन्नता कॉलम भरें।
 - ❑ पासवर्डों को 1-5 तक रैंक करें।
 - ❑ [इस वेबसाइट](#) का उपयोग करके अपने उत्तर जाँचें और प्रत्येक विकल्प टाइप करें। अपनी रैंकिंग की तुलना करने के लिए अंतिम कॉलम, हैकर को क्रैक करने में लगने वाला समय, भरें।

रैंक करें 1: सबसे सुरक्षित से लेकर 5: सबसे कम सुरक्षित तक	पासवर्ड	वर्णों की संख्या पासवर्ड में कितने वर्ण हैं?	वर्णों की भिन्नता क्या पासवर्ड में अपर और/या लोअर केस अक्षर शामिल हैं? संख्याएं? प्रतीक?	हैकर के द्वारा खोलने में लगने वाला समय इस वेबसाइट , किसी हैकर को पासवर्ड खोलने में कितना समय लगेगा?
उदाहरण पासवर्ड	ku8@}:'\$	8	लोअरकेस अक्षर, प्रतीक, संख्याएं	4 घंटे
	hcVESx			
	vWESp3Tt			
	Sg3Jpezyhv			
	पासवर्ड1			
	jG/8ab{s			

चरण 4: निष्कर्ष (जारी)

- ❑ अपने खुद के सुरक्षित पासवर्ड बनाने में **2 मिनट** लगाएं और उन्हें नीचे दी गई जगह में लिखें। आपके पासवर्डों को खोलने में हैकरों को *कम से कम 1 वर्ष* लगना चाहिए।
- ❑ पिछले चरणों में पासवर्ड कितने सुरक्षित थे यह जाँचने के लिए [इस वेबसाइट](#) तक नेविगेट करें।



क्या आप अपने परिणामों पर चकित हुए? आपके सभी खातों को सुरक्षित करने के लिए यहाँ कुछ दिशानिर्देश और सुझाव दिए गए हैं

- **कई खातों के लिए समान पासवर्ड का कभी उपयोग मत करें।** कुछ वेबसाइट दूसरों से अधिक सुरक्षित होती हैं, और यदि कोई हैकर एक खाते में प्रवेश पा लेता है, तो आप नहीं चाहेंगे कि उसके लिए आपके अन्य खातों में प्रवेश करना आसान हो जाए। आपके सभी पासवर्ड को याद रखना कठिन हो सकता है, इसलिए हम [BitWarden](#), [KeePassXC](#), या [LastPass](#) जैसे पासवर्ड मैनेजर का उपयोग करने का सुझाव देते हैं।
- **अपने पासवर्ड को कभी भी अपने ब्राउज़र में मत सहेजें।** हर बार जब आप किसी वेबसाइट में ऑनलाइन लॉग इन करते हैं, आपका ब्राउज़र आपको पूछेगा कि क्या आप अपना पासवर्ड सहेजना चाहते हैं। **कभी नहीं का चयन करें!** भले ही आपका पासवर्ड को याद रखना कठिन हो, ब्राउज़र में पासवर्ड को सहेजने से हैकरों के लिए आपकी जानकारी में प्रवेश करना आसान हो जाता है। अपने पेचीदा पासवर्ड को याद रखने में आपकी मदद करने के लिए पासवर्ड मैनेजर का उपयोग करें।
- **अपने पासवर्ड में विविध प्रकार के पासवर्ड का उपयोग करें।** सामान्य रूप से, पासवर्ड को विविध प्रकार के अपरकेस, लोअरकेस अक्षरों, संख्याओं, और विशेष वर्णों का उपयोग करना चाहिए और उन्हें कम से कम 11 अक्षरों का होना चाहिए। आपको सामान्य शब्दों जैसे, “पासवर्ड”, नामों, विशिष्ट तारीखों (जैसे जन्म तिथियाँ), या “111” या “1234” जैसी संख्याओं का उपयोग करने से बचना चाहिए।
- **2-फैक्टर ऑथेंटिकेशन (2FA) सेट अप करें।** अपने खातों को और सुरक्षित करने के लिए 2FA सेटिंग ऑन करें जो आपको अपने खातों में पासवर्ड और किसी भरोसेमंद डिवाइस, ईमेल, या सुरक्षा प्रश्नों के माध्यम से सत्यापन के द्वारा लॉग इन करने के लिए मजबूर करती है। यह अतिरिक्त चरण आपके खातों को सुरक्षित करने में बहुत उपयोगी है। इस [लेख](#) को पढ़कर देखें कि विविध प्रकार के खातों के लिए 2FA को कैसे ऑन करें जिनमें [इंस्टाग्राम](#), [अमेज़न](#), [फेसबुक](#), [गूगल](#), और [ट्विटर](#) शामिल हैं।
- **अपने पासवर्ड को अक्सर बदलें।** अपने पासवर्ड को हर तीन महीने में बदलना अच्छी आदत है।

हमला #2: फिशिंग (5-8 मिनट)



फिशिंग अक्सर एक ईमेल, टेक्स्ट संदेश, या पॉप-अप संदेश होता है जो किसी सुविख्यात स्रोत से आया प्रतीत होता है और प्रयोक्ताओं से एक लिंक पर क्लिक करने या संवेदनशील जानकारी प्रदान करने के लिए कहता है। ये ईमेल किसी बैंक, विश्वविद्यालय के क्रेडेंशियल्स, विभिन्न ऑनलाइन खातों आदि से प्रतीत हो सकते हैं। ये लिंक अक्सर प्रयोक्ताओं को असुरक्षित वेबसाइट पर ले जाते हैं जहाँ हमलावर आपके कंप्यूटर में प्रवेश पाने में और अन्य दुर्भावनापूर्ण गतिविधि जारी रखने में सक्षम हो सकते हैं।

कभी-कभी वेबसाइट सुविख्यात साइट को दोहराती हैं और जब आप उनकी साइट में लॉग इन करते हैं तो आपकी जानकारी चुरा लेती हैं।

हमारी कहानी में आपने कोई ऐसा मार्ग चुना हो सकता है जहाँ आपको कोई दुर्भावनापूर्ण ईमेल मिली थी। यह विशिष्ट ईमेल सामान्य फिशिंग ईमेल से अलग है और अधिक स्पष्ट निर्देशों और जानकारी से युक्त है। इस हमले को **स्प्रियर फिशिंग** कहते हैं क्योंकि इस ईमेल को विशिष्ट निर्देशों के साथ एक अकेले प्रयोक्ता को विशिष्ट रूप से भेजा गया था। ईमेल में लिंक को क्लिक करने पर, कंप्यूटर **मालवेयर**, या दुर्भावनापूर्ण सॉफ्टवेयर के संपर्क में आ गया जो कंप्यूटर को संक्रमित करता है।

यहाँ फिशिंग ईमेल का एक उदाहरण प्रस्तुत है:



तस्वीर स्रोत: नॉर्टन

यह विशिष्ट ईमेल भरोसेमंद दिख सकता है क्योंकि लोगो सही है और टेक्स्ट का स्टाइल इंस्टाग्राम के अन्य संचारों से मेल खाता है। 2-फैक्टर ऑथेंटिकेशन (2FA) सेट अप करते समय आपके द्वारा सफलतापूर्वक लॉगिन करने से पहले आपके कोड को एक अलग ईमेल में भेजा जाना चाहिए। आपको अंतिम वाक्य के बीच खाली स्थान का अभाव भी दिख सकता है। ये बहुत ही छोटे लेकिन विस्तृत संकेतक हैं कि यह ईमेल नकली है!

- ❑ **5-10 मिनट** लगाकर इस **वेबसाइट** पर फिशिंग ईमेल के कुछ उदाहरणों की समीक्षा करें और देखें कि क्या आप ऐसे मुख्य विवरणों की पहचान कर सकते हैं कि यह एक फिशिंग हमला है।



फिशिंग ईमेलों को पहचानना कठिन हो सकता है। यह निर्धारित करने के लिए कि क्या कोई ईमेल घोटाला है या नहीं, यहाँ कुछ दिशानिर्देश दिए गए हैं।

- **व्याकरण-संबंधी/वर्तनी की त्रुटियाँ:** क्या संदेश में व्याकरण-संबंधी त्रुटियाँ हैं? क्या कुछ शब्दों की वर्तनी गलत है या क्या फॉर्मेटिंग में हल्की सी गलती है?
- **लोगो/तस्वीर की त्रुटियाँ:** क्या तस्वीरें गलत हैं? क्या संभव है कि प्रेषक अनाधिकारिक लोगो का उपयोग कर रहा है? क्या रिजोल्यूशन, या तस्वीर की गुणवत्ता खराब है (क्या उसमें फ़ज़ी पिक्सेल हैं)?
- **URL त्रुटियाँ:** क्या कोई लिंक मूल/विश्वसनीय वेबसाइट से अलग है? शायद URL, .com की बजाय .org में समाप्त हो रहा है।



यदि आपने किसी फिशिंग ईमेल की पहचान की है, हाँ कुछ कदम हैं जिन्हें उठाकर आप खुद को संभावित दुर्भावनापूर्ण हमलों से सुरक्षित कर सकते हैं।

- **किसी भी लिंक पर क्लिक मत करें।** फिशिंग ईमेल ऐसे लिंकों पर क्लिक कर सकते हैं जो आपके कंप्यूटरों में मालवेयर इनस्टाल करते हैं। ईमेल में मौजूद किसी भी लिंक पर *कभी* क्लिक मत करें।
- **ईमेल को रिपोर्ट करें।** कई मामलों में आपको किसी नए ब्राउज़र में विश्वसनीय वेबसाइट को एक्सेस करना चाहिए और कंपनी को संदिग्ध ईमेल की सूचना दें ताकि वे अपनी वेबसाइटों को सुरक्षित कर सकें। आपको ईमेल की रिपोर्ट फेडरल ट्रेड कमीशन को भी [ftc.gov/complaint](https://www.ftc.gov/complaint) पर देनी चाहिए।
- **कभी कोई व्यक्तिगत जानकारी मत प्रदान करें।** फिशिंग ईमेलों का उद्देश्य प्रयोक्ताओं से अतिरिक्त जानकारी एकत्र करके उनके सिस्टमों को अधिक अरक्षित बनाना है। कई मामलों में हैकर के पास आपके ईमेल के अलावा और कोई जानकारी नहीं होती है।
- **अपना पासवर्ड बदलें।** हमले के बाद, अपने खातों को सुरक्षित करने के लिए अपने पासवर्ड बदलना एक अच्छी परिपाटी है।

चरण 5: अपने ऑनलाइन फुटप्रिंट को सुरक्षित करना (5-10 मिनट)



अब जबकि आपने कुछ आम साइबर हमलों की छोटी सी झलक देख ली है, आगे क्या है?

- **सुनिश्चित करें कि आपके पासवर्ड शक्तिशाली और सुरक्षित हैं।** अपने पासवर्डों पर नज़र रखने के लिए [BitWarden](#), [KeePassXC](#), या [LastPass](#) जैसे पासवर्ड मैनेजर का उपयोग करें और उन्हें कम से कम हर 3 महीने में बदलें।
- **एंटीवायरस/मालवेयर सॉफ्टवेयर डाउनलोड करें।** हो सकता है कि आपके कंप्यूटर पर पहले से मालवेयर है और आपको पता नहीं है! हमारे द्वारा सुझाए गए कुछ निःशुल्क एंटीवायरस/मालवेयर सॉफ्टवेयर में [Kaspersky](#), [Avast](#), [Malwarebytes](#) हैं। सुनिश्चित करें कि यह सॉफ्टवेयर स्वचालित रूप से चले ताकि आप मालवेयर के लिए अपने कंप्यूटर की अक्सर जाँच करते रह सकें।
- **नवीनतम सिस्टम अपडेट हमेशा डाउनलोड करें।** विंडोज़ और एप्पल जैसी कंपनियाँ हमेशा सुनिश्चित करने की कोशिश करती रहती हैं कि आपके द्वारा प्रयुक्त कंप्यूटर सुरक्षित रहें। जबकि आपके कंप्यूटर को अपडेट करने में समय लग सकता है, वह मूल्यवान है क्योंकि इन अपडेट में अक्सर आपकी जानकारी को सुरक्षित करने के लिए निवारणात्मक उपाय शामिल होते हैं।
- **व्यक्तिगत जानकारी कभी साझा मत करें।** व्यक्तिगत जानकारी साझा करते समय आपको सावधानी बरतनी चाहिए, जिसमें आपका नाम, जन्मदिन, स्थान, फोन नंबर आदि शामिल हो सकता है। यह जानकारी अधिक नहीं लग सकती है, लेकिन किसी हैकर को इस जानकारी का संयोजन मिलने से आपके सामाजिक सुरक्षा नंबर जैसी अधिक संवेदनशील जानकारी पाने में मदद मिल सकती है।
- **दूसरों को शिक्षित करें!** जबकि कई लोगों को विभिन्न साइबर सुरक्षा खतरों का पता हो सकता है, अधिकांश लोग अपने कंप्यूटरों को सुरक्षित करने के लिए बहुत थोड़ी सावधानी बरतते हैं। साइबर सुरक्षा के महत्व और कंप्यूटरों और खातों को कैसे सुरक्षित करना चाहिए इसके बारे में आपकी जानकारी को अपने मित्रों और परिवार के साथ साझा करें।

चरण 6: विस्तार (5-30 मिनट)

एक्सटेंशन 1: 2020 का साइबर सुरक्षा तथ्य (5-10 मिनट)

जब हम इस बारे में सोचते हैं कि इंटरनेट किस तरह से सारी दुनिया में लोगों को जोड़ता है, तब इस बात पर एक नज़र डालें कि 2020 में हैकर इस अरक्षितता का लाभ कैसे उठा रहे हैं। इस वर्ष विभिन्न हमलों के बारे में CSO का यह [लेख](#) पढ़ें! साथ ही ध्यान दें कि यह लेख मार्च 2020 में अंतिम बार प्रकाशित हुआ था और उसके बाद आंकड़े बदल गए हो सकते हैं!

एक्सटेंशन 2: इंस्टाग्राम हैकर की कहानी (5-10 मिनट)

हमने एक वास्तविक अनुभव के आधार पर इस गतिविधि में कहानी लिखी। आप उसकी मूल कहानी को [यहाँ](#) देख सकते हैं। दुर्भाग्य से, यह परिस्थिति कई सोशल मीडिया मंचों पर अक्सर उत्पन्न होती रहती है। आप इस Forbes [लेख](#) में भी एक ऐसे ही अनुभव के बारे में पढ़ सकते हैं।

एक्सटेंशन 3: अन्य साइबर हमलों के बारे में अधिक जानें (10-30 मिनट)

इस गतिविधि में हमने दो प्रकार के साइबर हमलों, कमज़ोर पासवर्डों और फिशिंग हमलों की समीक्षा की। लोगों और कंपनियों को प्रभावित करने वाले अन्य साइबर हमलों के बारे में अधिक जानने के लिए यहाँ कुछ संसाधन प्रस्तुत हैं।

- CDSE की [Scenario Based Student Guide](#)
- [Cybersecurity 101: Infocyte का Intro to the Top 10 Common Types of Cyber Security Attacks](#)

चरण 7: अपने Girls Who Code at Home परियोजना को साझा करें! (5 मिनट)



हम आपके काम को देखना पसंद करेंगे और हम जानते हैं कि दूसरे भी ऐसा करेंगे। [साइबर जासूस प्रमाणपत्र](#) में अपना नाम डालें, उसे प्रिंट करें, और एक सेल्फी लें! 📷

अपने फोटो को किसी भी सोशल मीडिया साइट पर अपलोड करें। [@girlswhocode](#) [#codefromhome](#) को टैग करना मत भूलें, और हो सकता है कि हम आपको हमारे खाते में प्रदर्शित कर देंगे!

और Girls Who Code at Home परियोजनाओं के लिए बनी रहें!

