Hacker-Spionage (Stoppen) II

Der Schritt-für-Schritt-Sicherheitscheck

HACKER FINDEN.DE Powered by Audat

Disclaimer

Haftungsausschluss
Die dargestellten Inhalte werden mit größtmöglicher Sorgfalt zusammengestellt. Dennoch müssen wir die Haftung für die Vollständigkeit, Richtigkeit und Aktualität der eigenen Informationen, die auf der Website zur Nutzung bereitgehalten werden, ausschließen, es sei denn, wir handeln vorsätzlich oder grobfahrlässig. Der Haftungsausschluss gilt auch für Linksammlungen, die zurzeit Bestehen oder in Zukunft bestehen werden.

Rechtlicher Hinweis
Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen. Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

Die Inhalte unserer Website sind urheberrechtlich geschützt. Soweit Sie die Inhalte für Ihre eigenen beruflichen oder persönlichen Zwecke benötigen, räumen wir Ihnen das Recht ein, die bereitgestellten Texte ganz oder teilweise zu speichern und zu drucken.

Die Speicherung und Vervielfältigung von Bildmaterial oder Grafiken aus unserer Website ist nicht gestattet.

Wenn Sie weitere Fragen oder Anmerkungen haben, kontaktieren Sie uns per Mail: support@ownext.com

Securitycheck Cybersicherheit

Ihr Wissen über Cybersicherheit hat sich bereits um ein Vielfaches erweitert. In diesem Kapitel finden Sie zahlreiche fortgeschrittene Tipps, um sich gegen Online-Überwachung und hartnäckige Hacker zu wehren.

Berücksichtigen Sie Ihr persönliches Risikoniveau

Es ist wichtig zu überlegen, welche Risiken auf Sie zutreffen. Sind Sie eine Frau und nutzen das Internet? Wahrscheinlich mussten Sie sich schon einmal vor Belästigungen durch Männer schützen. Sind Sie Journalist? Dann ist es möglich, dass die Regierung versucht, Sie im Auge zu behalten. Besitzen Sie einen Computer und ein Bankkonto? Sie verstehen schon: Jeder kann zur Zielscheibe werden, aber für bestimmte Zielpersonen ist das Risiko größer!

Ergreifen Sie geeignete Maßnahmen, die Ihrem persönlichen Risikoniveau entsprechen. Dieser Leitfaden enthält viele Ratschläge, die jeder befolgen sollte, denn viele Gefahren gelten für, nun ja, jeden. Aber für eine aktive Feministin mit einem Twitter-Account ist es noch wichtiger, die eigene Adresse und Telefonnummer vor den meisten Menschen geheim zu halten.

Jede Situation ist anders und erfordert daher einen anderen Ansatz. Wenn Sie den Verdacht haben, dass Ihr gewalttätiger Ehepartner Ihre E-Mails und Whatsapp-Nachrichten liest, können Sie die Chatfunktion eines Videospiels, wie z. B. Words With Friends, nutzen, um einen Freund über Ihre Situation zu informieren. Es ist unwahrscheinlich, dass Ihr Ehepartner auch diese Unterhaltungen mitverfolgt.

Spear Phishing

Erkennen Sie Spear Phishing

Beginnen wir mit dem schwierigsten Ratschlag, denn Spear-Phishing ist bekanntermaßen schwer zu erkennen. Spear-Phishing ist eine Form des Phishings, bei der die Person, die Sie hereinlegen will, Ihnen eine Nachricht schickt, die speziell auf Sie zugeschnitten ist. Ein Hacker könnte z. B. Informationen aus Ihren Social-Media-Profilen sammeln, um die Spear-Phishing-Nachricht mit glaubwürdigen Informationen zu versehen.

Nehmen wir an, Ihr Flug mit Delta Airlines hat sich um eine Stunde verspätet und Sie posten darüber auf Facebook. Ein Hacker könnte diese Informationen nutzen, um Ihnen eine E-Mail mit einem "Entschädigungsangebot" von Delta zu schicken. Alles, was Sie tun müssen, ist, sich einzuloggen (wodurch der Hacker Ihr Passwort erhält) und ein Formular auszufüllen. Die ganze Zeit über verfolgt der Hacker, was Sie tippen.

Zum Glück werden die meisten Menschen nie mit Spear-Phishing zu tun haben. Spear-Phishing betrifft in der Regel Personen, bei denen ein hohes Risiko besteht, dass sie angegriffen werden, wie Politiker, Rechtsanwälte und Journalisten. Trotzdem lohnt es sich, wachsam zu sein. Wenn Sie einer Nachricht nicht trauen, googeln Sie nach dem Unternehmen oder der Organisation, von dem/der die Nachricht angeblich stammt, und rufen Sie dort an, um sich zu erkundigen, ob die Nachricht, die Sie erhalten haben, echt ist oder nicht.

Backups

Verschlüsseln Sie Ihre Festplatten und Backups

Sie können MacBooks und iMacs mit nur einem Mausklick verschlüsseln, indem Sie FileVault aktivieren. Das ist denkbar einfach und stellt sicher, dass niemand, der Ihren Laptop findet oder stiehlt, Zugriff auf Ihre privaten Dateien hat.

Warten Sie nicht: Schalten Sie diese Funktion sofort ein.

Bei Windows sieht die Sache ganz anders aus. Microsoft hat seinen Verschlüsselungsdienst Bitlocker ausschließlich für die Pro-Versionen von Windows reserviert. Das ist zufälligerweise die Version, die Verbraucher fast nie benutzen.

Zum Glück gibt es einige gute Alternativen, die man in Betracht ziehen kann. Veracrypt ist die sicherste und zuverlässigste Option. Stellen Sie sicher, dass Sie Ihre Dateien sichern, bevor Sie Ihre Festplatte verschlüsseln. Der Verschlüsselungsprozess kann Stunden dauern und in manchen Fällen auch schief gehen. Mit einer Sicherungskopie können Sie die Sicherheit Ihrer Dateien gewährleisten.

Cryptomator-SymbolApropos: Sie können auch Backups verschlüsseln. Verschlüsseln Sie zum Beispiel Ihre externe Festplatte oder Ihren USB-Stick mit Veracrypt. Eine weitere gute App ist Cryptomator, die Ihre Dateien sofort verschlüsselt und in die Cloud hochlädt. Seien Sie jedoch besonders vorsichtig mit Ihrem Passwort. Wenn Sie Ihr Passwort verlieren, haben Sie keinen Zugriff mehr auf Ihre Dateien.

Sicheres Passwort

Erstellen Sie ein sehr sicheres Passwort mit der Diceware-Methode

Die Diceware-Methode wird von Experten verwendet, um extrem sichere Passwörter zu erstellen. Diceware verwendet einen zufälligen Würfelwurf und eine lange Liste von Wörtern, um Passwörter zu erzeugen. Hier ist eine Liste (txt) mit englischen Wörtern, die Sie verwenden können.

Zuerst würfelt man. Machen Sie dies fünfmal hintereinander und notieren Sie den Wert jedes Wurfs. Am Ende erhältst du eine fünfstellige Zahlenreihe, die einem Wort aus der Liste entspricht. Wenn du zum Beispiel 3-6-4-5-5 würfelst, ist das Wort, dem es entspricht, Gesetz.

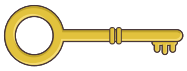
Wiederholen Sie diesen Vorgang sieben Mal, um sicherzugehen, dass er absolut sicher ist. Sie erhalten dann eine Reihe von sieben völlig zufälligen englischen Wörtern, z. B. limbo karma cosy ember pool swipe wow.

Die Diceware-Methode ist derzeit die beste Methode, um ein sicheres Passwort zu erstellen, das Sie sich merken können.

Zwei-Faktor-Authentifizierung mit einem Sicherheitsschlüssel

Experten empfehlen die Verwendung eines physischen USB-Schlüssels - auch bekannt als Sicherheitsschlüssel - für die Zwei-Faktor-Authentifizierung. Verbinden Sie Ihren Sicherheitsschlüssel mit Diensten wie Google, Facebook, Twitter und Dropbox und wenn Sie sich das nächste Mal anmelden möchten, werden Sie aufgefordert, Ihren USB-Schlüssel zu verwenden.

Sicherheitschlüsse



Stecken Sie den USB-Schlüssel in Ihren Computer und verbinden Sie ihn mit Ihrem Smartphone, um Ihren Anmeldeversuch zu authentifizieren. Der Online-Dienst prüft, ob der USB-Schlüssel mit Ihrem Konto verknüpft ist, und der USB-Schlüssel erkennt, ob Sie sich bei der richtigen App oder Website anmelden. Dies schützt Sie vor Phishing-Versuchen und gefälschten Websites, da der Anmeldeversuch nur dann erfolgreich sein kann, wenn sowohl Ihr Schlüssel als auch der Online-Dienst gültig sind.

Es wird empfohlen, zwei Sicherheitsschlüssel zu kaufen: einen, den Sie immer bei sich tragen, und einen weiteren, den Sie als Backup sicher aufbewahren. Verknüpfen Sie beide USB-Schlüssel mit den Diensten, für die Sie die Zwei-Faktor-Authentifizierung aktivieren möchten.

Und **vergessen Sie nicht**, die anderen Formen der Zwei-Faktor-Authentifizierung zu deaktivieren, die Sie möglicherweise für diese Dienste aktiviert haben, wie z. B. Anmeldecodes per SMS.

Der schwedische Hersteller Yubico bietet gute Verschlüsselungscodes an. Am besten entscheiden Sie sich für den blauen Sicherheitsschlüssel, der mit allen wichtigen Online-Diensten funktioniert. Sie können zwei davon für 49 USD kaufen. Yubikey 5 mit nfc (45 USD) funktioniert mit Android-Telefonen, aber die Funktionalität auf iPhones ist begrenzt. Es gibt auch eine Version, die USB-C-Anschlüsse verwendet und 55 USD kostet.

Tipps

Deaktivieren Sie die automatische Vervollständigung und schalten Sie die automatische Sperre ein

Einige Passwortmanager bieten die Möglichkeit, Ihre Passwörter auf Websites automatisch auszufüllen. Dies ist nicht sicher. Ein Hacker könnte Ihren Passwortmanager mit einer gefälschten Seite täuschen. Deshalb sollten Sie diese Option ausschalten, z. B. bei LastPass.

Es ist auch sinnvoll, dass sich Ihr Passwortmanager automatisch sperrt, wenn Sie ihn eine bestimmte Zeit lang nicht benutzt haben. So wird verhindert, dass Ihr digitaler Tresor mit Ihren Passwörtern länger als nötig offen liegt.

Das Smartphone als Spionagegerät
Smartphones sind ideale Geräte zum Spionieren. Geheimdienste können Ihr Telefon abhören und seinen Standort abfragen, oder Hacker können eindringen und Ihr Mikrofon und Ihre Kamera einschalten. Seien Sie sich dessen bewusst.

Android und iOS zeichnen standardmäßig auf, wo Sie sich aufgehalten haben, und diese sensiblen Informationen könnten an Dritte weitergegeben werden. Sowohl bei Android als auch bei iOS können Sie diese Funktion deaktivieren, so dass Ihr Telefon nicht ständig Ihren Standort aufzeichnet. Das hindert einen Hacker oder einen Geheimdienst jedoch nicht daran, Ihren Standort mit Hilfe Ihres Smartphones zu verfolgen.

Eine extreme Maßnahme besteht darin, Ihr Telefon auszuschalten und es in einer Faradayschen Hülle aufzubewahren (die Sie selbst herstellen können) oder es in eine Mikrowelle zu legen (die Sie niemals einschalten sollten, wenn sich Ihr Telefon darin befindet). Nur so können Sie absolut sicher sein, dass niemand Ihren Standort aufspüren kann.

Sicherheit

Verbessern Sie die Sicherheit Ihres Smartphones weiter

Es gibt hochsichere Android-Versionen, die Sie auf Ihrem Telefon installieren können, wie z. B. CopperheadOS und GrapheneOS. Diese Android-Versionen haben zusätzliche Sicherheitsmaßnahmen eingebaut und versuchen, die Schwachstellen im System zu minimieren.

Wenn Sie Ihr eigenes Android-Handy noch sicherer machen wollen, sollten Sie diese Anleitung befolgen. Sie enthält eine Reihe nützlicher Tipps, darunter die notwendigen Schritte zur Deaktivierung von Javascript über Chrome > Einstellungen > Website-Einstellungen > Javascript. Viele Websites werden danach nicht mehr funktionieren, aber Ihr Gerät wird dadurch viel sicherer.

Für iPhones empfiehlt es sich, iMessage und FaceTime über Einstellungen > Nachrichten / FaceTime zu deaktivieren. Bei diesen beiden Diensten wurden in der Vergangenheit Sicherheitslücken festgestellt. Sie können auch AirDrop über Einstellungen > Allgemein > Airdrop deaktivieren und Javascript über Einstellungen > Safari > Erweitert deaktivieren. Die iVerify App bietet noch ein paar weitere Tipps.

Eine letzte allgemeine Regel: Verwenden Sie so oft wie möglich Ihren Browser und keine Apps. Andere Apps können Sicherheitslücken enthalten, während der Browser in der Regel eine der sichersten Apps auf Ihrem Smartphone ist .

Sicherheit

Erhöhen Sie die Sicherheit Ihres Windows-Computers weiter

Hardentools ist eine Anwendung, die von einer Gruppe von Hackern und Cybersicherheitsexperten entwickelt wurde. Sie deaktiviert anfällige Teile von Windows, so dass es für Hacker schwieriger wird, Ihren Computer zu übernehmen. Beachten Sie, dass die Anwendung auch Dinge deaktivieren kann, die Sie gerade verwenden, wie bestimmte Funktionen in Office oder Adobe Reader. Wenn ein Teil plötzlich nicht mehr funktioniert, können Sie es jederzeit über Hardentools wieder einschalten.

Natürlich auf eigene Gefahr.

Für MacOS gibt es kein solches Tool, aber Sie können diesem langen Handbuch oder Schritt-für-Schritt-Plan folgen. Aber seien Sie gewarnt. Wenn Sie nicht sicher sind, was Sie tun, laufen Sie Gefahr, Ihren Computer unbrauchbar zu machen.

Seien Sie vorsichtig bei der Sicherung von Chats in der Cloud
Viele Chat-Apps bieten die Möglichkeit, Ihre Chats in der Cloud, über Google Drive oder iCloud zu speichern. Seien Sie dabei vorsichtig.

Alle Nachrichten werden mit einer Ende-zu-Ende-Verschlüsselung verschlüsselt, sobald sie gesendet werden, aber sie verlieren ihre Verschlüsselung, sobald die Nachrichten Ihr Telefon erreichen, sonst könnten Sie sie nicht mehr lesen. Wenn Sie eine Sicherungskopie Ihrer Nachrichten erstellen möchten, werden diese unverschlüsselt in die Cloud hochgeladen. Ein Geheimdienst könnte Ihren Chatverlauf abfragen. Beachten Sie auch, dass Ihre Nachrichten von den Personen, mit denen Sie chatten, unverschlüsselt gesichert werden können.

Sicherheit

Sichere geheime Fragen

Antworten auf geheime Fragen sind oft (meist unbeabsichtigt) online verfügbar, wie der Name Ihres ersten Haustiers oder der Geburtsort Ihrer Mutter. Wenn ein Hacker Ihre geheimen Fragen richtig beantwortet, kann er Ihr Kennwort zurücksetzen und Zugang zu Ihren Online-Konten erhalten und Sie dabei aussperren. Es ist viel besser, geheime Fragen mit zufälligen Antworten zu beantworten und diese Antworten in einem Passwort-Manager zu speichern.

Beachten Sie, dass Ihre Antworten in manchen Fällen laut ausgesprochen werden müssen. Zum Beispiel, wenn Sie den Kundendienst anrufen. Anstelle einer komplizierten Zahlen- und Buchstabenfolge können Sie auch vier zufällige Wörter Fuchs-Sandwich-Fahrrad-Hochzeit als Antwort wählen.

Digitale Schwachstelle: Ihre Telefonnummer
Ihre Handynummer mag sicher erscheinen, aber in Wirklichkeit ist sie oft das schwächste Glied in Ihrer Online-Sicherheit. Die Nummer kann den Zugang zum Zurücksetzen eines Passworts und damit zum Verlust eines Ihrer Konten ermöglichen. Hacker sind sich dessen bewusst. Sie könnten versuchen, Ihre Telefonnummer zu kapern, indem sie Ihren Mobilfunkanbieter anrufen und sich als Sie ausgeben. Diese Angriffe werden als Sim-Swapping bezeichnet. Wenn ein Hacker die Kontrolle über Ihre Mobiltelefonnummer erlangt, erhält er auch Zugriff auf die mit dieser Nummer verbundenen Online-Konten.

Deshalb sollten Sie Ihren Mobilfunkanbieter bitten, ein Passwort festzulegen, bevor er Ihnen (oder jemandem, der sich für Sie ausgibt) bei Kundenanfragen hilft. Wenn Sie das nächste Mal dort anrufen, müssen Sie Ihr Passwort angeben, damit man Ihnen helfen kann. Wenn Sie wirklich vermeiden wollen, Opfer von Sim-Swapping zu werden, müssen Sie Ihre Telefonnummer aus allen Ihren Online-Konten entfernen. Sicherer ist es, sowohl einen Sicherheitsschlüssel als auch eine Authentifizierungs-App zu verwenden.

Sicherheit Daten

Achten Sie auf Standortdaten in Bildern

Wenn du mit deinem Smartphone ein Foto machst, speichert es alle möglichen zusätzlichen Informationen, wie das Datum, die Uhrzeit und den genauen Ort, an dem das Bild aufgenommen wurde. Diese Informationen werden auch als EXIF-Daten bezeichnet. Wenn Sie diese Bilder auf Facebook, Twitter, Instagram oder WhatsApp teilen, werden die EXIF-Daten automatisch entfernt. Wenn Sie jedoch ein Bild auf Ihre Website hochladen oder per E-Mail versenden, können andere Personen weiterhin auf diese Informationen zugreifen. Wenn Sie sicherstellen möchten, dass die EXIF-Daten entfernt werden, verwenden Sie die Website ImgClean.io, bevor Sie Ihre Bilder hochladen oder per E-Mail verschicken. ImgClean entfernt diese zusätzlichen Informationen aus den Bildern und lässt Sie eine saubere Version herunterladen, die Sie gefahrlos weitergeben können.

Sichere Anrufe

Wenn Sie jemanden anrufen möchten, ohne Gefahr zu laufen, dass Ihr Anruf abgehört wird und Ihr Gespräch mitgehört wird, sollten Sie Signal verwenden. Signal verschlüsselt die Anrufe mit einer Ende-zu-Ende-Verschlüsselung. Für viele Menschen mag diese Maßnahme übertrieben sein, aber für gefährdete Personen wie Journalisten und Anwälte kann sie von Zeit zu Zeit notwendig sein.

Anrufe über Signal (und WhatsApp) schützen Sie auch vor IMSI-Catchern. Diese Geräte imitieren Telefonmasten, um Ihre Anrufe und Nachrichten abzuhören. IMSI-Catcher werden meist von Geheimdiensten eingesetzt, können aber auch von Hackern hergestellt werden.

Sicherheit Internet

Verschlüsselter E-Mail-Versand mit ProtonMail

ProtonMail ist einer der benutzerfreundlichsten Dienste, wenn es um das Senden und Empfangen verschlüsselter E-Mails geht. Die Ende-zu-Ende-Verschlüsselung funktioniert allerdings nur, wenn sowohl der Absender als auch der Empfänger ProtonMail verwenden. Bei anderen E-Mail-Adressen, wie z.B. Gmail oder Outlook, fragt ProtonMail Sie, ob Sie die an sie gesendeten E-Mails mit einem Passwort schützen möchten. Der Empfänger braucht dann das Passwort, um die E-Mail zu öffnen. ProtonMail macht dies, um eine zusätzliche Sicherheitsebene zu schaffen. Ein Konto mit 500 MB ist kostenlos, aber wenn Sie mehr Speicherkapazität und zusätzliche Funktionen wünschen, müssen Sie zwischen 5 und 20 USD pro Monat bezahlen.

Der Tor-Internetbrowser schickt Ihren Internetverkehr durch zahlreiche Computer. Das schützt Ihre Privatsphäre, denn Websites können nicht herausfinden, woher Sie kommen, und Ihr Provider kann nicht sehen, was Sie im Internet tun. Das mag für manche Leute praktisch sein, aber für andere in Ländern wie dem Iran oder Russland kann es ein echter Lebensretter sein. Mit Tor kannst du auch gesperrte Webseiten besuchen, was in einem Land wie der Türkei besonders nützlich ist.

Tor bietet auch Zugang zum Dark Web, also zu dem Teil des Internets, den man mit einem normalen Internetbrowser nicht besuchen kann. Im Dark Web findest du vor allem Marktplätze für Drogen und Waffen, Webseiten mit Kinderpornografie und Nazi-Communities.

Der Nachteil der Anonymität von Tor ist, dass es auch für schändliche Zwecke genutzt werden kann.

Chatten und Router

OpenWrt auf Ihrem Router

Viele Hersteller stellen die Aktualisierung ihrer Router nach einer gewissen Zeit ein. Daher ist es ratsam, OpenWrt zu installieren. Die Software ist für alle Arten von Routern erhältlich und wird regelmäßig aktualisiert, um Sicherheitslücken zu schließen, ist aber auch schwierig zu installieren.

OpenWrt funktioniert nicht mit WiFi-Modems, die von Ihrem Internetanbieter bereitgestellt und verwaltet werden. Sie können jedoch einen eigenen Router kaufen und diesen mit dem Modem Ihres Internetanbieters verbinden. Stellen Sie Ihr WiFi-Modem auf den Bridge/DMZ-Modus ein, damit das Gerät die Internetverbindung nur weiterleitet.

Chatten mit OTR

OffThe Record (OTR) ist eine sichere Möglichkeit, mit anderen zu chatten, genau wie Signal. OTR wird mit einer E-Mail-Adresse und einer App auf Ihrem Desktop (Adium für MacOS und Pidgin für Windows und Linux) oder Smartphone (Conversations für Android und ChatSecure für iOS) verwendet. Mit diesen Apps können Sie mit anderen OTR-Benutzern chatten, aber die meisten Leute bevorzugen trotzdem Signal.

Betreiben Sie Ihr eigenes VPN

Wenn Sie technisch versiert sind, können Sie die Dinge selbst in die Hand nehmen und Ihr eigenes VPN betreiben.

Die einfachste Option ist Algo, das Sie auf Ihrem - vorzugsweise neuen - Server installieren. Sie verwalten dann Ihre eigene sichere Internetverbindung und können alle Ihre Geräte damit verbinden. Da Algo einfach zu konfigurieren ist, können Sie es auch für die Einrichtung eines temporären VPN verwenden.

IT-Hilfe von Experten erhalten

Schnell, einfach & diskret

Wurden Sie gehackt oder erpresst?
Haben Sie den Zugang zu Ihrem Konto verloren?
Müssen Sie sensible Bilder oder Videos entfernen?
Wurde Ihre ID missbraucht?
Wollen Sie eine Beweissicherung für Strafverfolgung?
Möchten Sie Cybermobbing stoppen?
Haben Sie ein Smartphone- oder Computerproblem?
Sind Sie Opfer von Online-Betrug?

Wir helfen Ihr Problem zu lösen

Bei Fragen oder IT-Notfällen einfach ein Online Videogespräch mit einem Experten buchen:
https://www.hacker-finden.de/kontakt/
oder schreiben Sie uns an hilfe@hacker-finden.de

Weitere e-Books: www.hacker-finden.de/ebooks
Weitere Informationen: www.hacker-finden.de

Es gibt Situationen, die sehr fortgeschritten sind und bei denen bestimmte Arten von Online-Schwachstellen oder Hacker-Angriffen die Schadensursache sein können. Wenn die Best-Practice-Schritte nicht zur Behebung führen oder Sie Informationen über den Täter herausfinden wollen, buchen Sie sich eine persönliche kostenlose Ersteinschätzung mit einen Experten:

JETZT STARTEN

HACKER FINDEN.DE Powered by Audat