

OUCH!

Der monatliche Security Awareness Newsletter für Sie

Frühjahrsputz

Übersicht

Die meisten von uns freuen sich so sehr auf den Frühling! Die Natur beginnt wieder zu erwachen, Blumen beginnen zu blühen, und für viele besteht der Wunsch nach einem Frühjahrsputz. Es mag zwar leicht sein, die Notwendigkeit zu erkennen, zu putzen und aufzuräumen, aber die Notwendigkeit, auch digital aufzuräumen, ist nicht so offensichtlich. Hier ein paar Tipps, um Ihr digitales Leben in Ordnung zu bringen und neue digitale Gewohnheiten zu schaffen:



DATENSICHERUNG: Wir haben diesen Schritt als ersten aufgeführt, weil er auf lange Sicht einer der wichtigsten ist und ein Schritt, den Sie machen sollten, bevor Sie zu den anderen übergehen. Ganz gleich wie sicher Sie sind, irgendwann werden Sie höchstwahrscheinlich Datensicherungen benötigen, um Ihre wichtigen Informationen wiederherstellen zu können. Gründe dafür können unter anderem der Ausfall einer Festplatte, der Verlust eines Geräts und die Infektion mit Malware, wie z.B. Ransomware, sein. Die Erstellung und Planung automatischer Datensicherungen stellt sicher, dass Sie Ihre wichtigsten Informationen wiederherstellen können.



LÖSCHEN: Löschen Sie alle nicht verwendeten Programme oder Anwendungen auf Ihren mobilen Geräten und Computern. Einige Anwendungen belegen große Mengen an Speicherplatz, können neue Schwachstellen einführen und sogar die Geschwindigkeit Ihrer Geräte verlangsamen. Je weniger Apps Sie haben, desto sicherer sind Ihre Systeme und Ihre Informationen. Viele Geräte zeigen Ihnen an, wie lange es her ist, dass Sie eine App benutzt haben. Wenn es mehr als ein paar Monate her ist, besteht die Wahrscheinlichkeit, dass Sie die App nicht mehr brauchen!



AKTUALISIEREN: Aktualisieren Sie alle Geräte und Anwendungen die Sie besitzen und aktivieren Sie die automatische Aktualisierung, wann immer möglich. Auf diese Weise bleiben Ihre Geräte und Apps immer auf dem neuesten Stand, was nicht nur dafür sorgt, dass sie schneller laufen, sondern es für Dritte viel schwieriger macht sich in sie zu hacken.



PASSWÖRTER: Überprüfen Sie Ihre Passwörter. Wenn Sie dieselben Passwörter für mehrere Konten verwenden, ändern Sie sie so, dass jedes Konto ein eindeutiges Passwort hat. Sie können sich all diese Passwörter nicht merken? Erwägen Sie die Verwendung eines Passwortmanagers. Schließlich sollten Sie, wann immer möglich, die Zwei-Faktor-Authentifizierung (2FA) aktivieren, insbesondere für E-Mail- und Finanzkonten.



FINANZKONTEN: Stellen Sie sicher, dass Ihre Bankkonten, Kreditkartenkonten und Rentenkonten so konfiguriert sind, dass Sie bei jeder Transaktion benachrichtigt werden, insbesondere bei großen Einkäufen oder Geldüberweisungen. Je früher Sie betrügerische Aktivitäten erkennen, desto schneller können Sie sie unterbinden. Je nachdem, in welchem Land Sie leben, kann eine Kreditsperre eine der wirksamsten Möglichkeiten sein, Ihre Identität zu schützen.



BROWSER: Überprüfen Sie alle in Ihrem Browser installierten Add-ons oder Plugins. Überprüfen Sie die Berechtigungseinstellungen. Benötigen die Plugins wirklich Zugang zu Ihrem Standort, Ihren Passwörtern oder Kontaktlisten? Wenn Sie bestimmte Plugins nicht mehr verwenden oder Bedenken bezüglich des Datenschutzes haben, löschen Sie diese.



SOZIALE MEDIEN: Schauen Sie sich Ihre Online-Präsenz an und nutzen Sie sie. Überprüfen Sie Ihre Datenschutzeinstellungen und löschen Sie alle Fotos und Videos, auf die nicht mehr zugegriffen wird oder die nicht mehr benötigt werden. Sie können sich auch selbst in einer Suchmaschine suchen und sehen, welche Informationen es über Sie gibt. Denken Sie daran, dass es in Ordnung ist, die Menge der Informationen, die Sie austauschen zu begrenzen und sogar zu beschränken, mit wem Sie diese Informationen teilen möchten.



ARBEITSPLATZ: Räumen Sie Ihre Schreibtischschublade aus, löschen Sie alte Festplatten und USB-Geräte und vernichten Sie Haftnotizen mit zu vielen Informationen. Erwägen Sie die Investition in einen Aktenvernichter, wenn Sie keinen haben.



E-MAIL: Führen Sie eine Bereinigung Ihrer E-Mails durch. Löschen Sie was Sie nicht benötigen und organisieren Sie Ihre Arbeit. Achten Sie besonders auf alle sensiblen Dokumente, z.B. solche mit Ihrem Geburtsdatum oder Ihrer Sozialversicherungsnummer, und löschen Sie diese aus Ihrem E-Mail Postfach!

Auch wenn dies eine gewaltige Aufgabe zu sein scheint, können Sie sicher sein, dass Ihre Geräte und Informationen weitaus besser geschützt sind. Falls Ihnen der Aufwand zu groß ist sollten Sie sich überlegen, ob Sie nur einige wenige Punkte auswählen oder versuchen, einen Punkt pro Tag oder Woche abzuhaken. Jeder noch so kleine Schritt ist ein wichtiger Schritt zu Ihrem Schutz.

Gastredakteur

Katie Nickels (@LiketheCoins) ist Principal Intelligence Analyst bei Red Canary sowie SANS Ausbilderin für FOR578: Cyber Threat Intelligence. Sie arbeitet seit über einem Jahrzehnt in den Bereichen Netzwerksicherheit, Incident Response und Cyber Threat Intelligence.



Weiterführende Informationen

Haben Sie Backups?:

<http://www.sans.org/u/ZVr>

Einfache Passwörter erzeugen:

<http://www.sans.org/u/ZVw>

Suchen Sie sich selbst online:

<http://www.sans.org/u/ZVB>

Entsorgung Ihres Mobilgeräts:

<http://www.sans.org/u/ZVG>

OUCH! wird von SANS Security Awareness veröffentlicht und unter der [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/) zur Verfügung gestellt. Sie dürfen diesen Newsletter weitergeben oder verbreiten, solange Sie ihn nicht verkaufen oder ändern. Redaktionelle Leitung: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley