Checkliste: «Eigene Daten und guten Ruf im Internet schützen»

Wie können Sie Ihre Daten und Ihren Ruf im Internet schützen? Stéphane Koch*, Spezialist für Online-Reputation und Datenschutz, nennt einige einfache Tipps.

✓ Inhalte, die sich auf die eigene Person beziehen

Um den eigenen Ruf wirksam zu schützen, muss man unbedingt die Online-Inhalte kennen, die sich auf die eigene Person beziehen. «Googeln» Sie Ihren Namen deshalb regelmässig. In gewissen Fällen ist es möglich, über den Webmaster der Website oder die Suchmaschine, die die Website anzeigt, unerwünschte Inhalte löschen und aus dem Index der Suchmaschine entfernen zu lassen.

✓ Facebook und soziale Netzwerke

Geben Sie keine sensiblen Inhalte bekannt und seien Sie genau so vorsichtig wie im realen Leben. Informieren Sie sich, wie Sie Ihr Konto deaktivieren oder löschen können. Aktivieren Sie die Zwei-Faktor-Authentifizierung. Teilen Sie Ihre Freundeliste nicht öffentlich, ebenso wenig wie Ihre Interessen (gefällt mir). Kontrollieren Sie die Beiträge, in denen Sie markiert wurden. Akzeptieren Sie als Freunde nur Personen, die Sie auch wirklich kennen. Die Zahl der «gemeinsamen Freunde» ist kein zuverlässiges Kriterium.

✓ Seltsames Verhalten von Freunden

Betrüger können die Konten Ihrer Freunde hacken und von dort aus Links verschicken. Wenn ein Inhalt sich nicht mit dem deckt, was ein Bekannter normalerweise online stellt oder verschickt, klicken Sie nicht darauf und rufen Sie die Person an, um sie zu informieren. Auch über private Nachrichten können falsche Links verschickt werden, ebenso wie über WhatsApp. Sie sollten keine Links anklicken, die Ihnen über eine zweifelhafte Nachricht zugestellt wurden und Sie auf einen Inhalt oder eine Plattform führen (wie «Google Docs» oder wenn man sich über einen Webservice identifizieren muss, etwa «Verbinden Sie sich mit Facebook um dieses Video sehen zu können»).

✓ **Sicherheitskopie**

Sichern Sie die wichtigsten Daten regelmässig. Schützen Sie Ihre Speichergeräte mit einem sicheren Passwort und bewahren Sie die Sicherheitskopie an einem anderen Ort auf als das Original.

✓ **Daten löschen**

Wenn Sie ein Gerät entsorgen, in Reparatur geben oder verkaufen (Smartphone, Tablet, PC, USB-Stick, SD-Karten), löschen Sie zuvor sämtliche Daten. Achtung: Gewisse Daten bleiben auch nach dem Löschen erhalten. Es reicht nicht, sie einfach in den Papierkorb zu verschieben. Es muss eine sichere Datenlöschung vorgenommen werden.

✓ **Passwörter**

Sichern Sie Ihre Geräte und Online-Konten mit sicheren Passwörtern. Verwenden Sie für jedes Konto ein eigenes, spezifisches Passwort. Hier kann ein Passwortmanager helfen (nur wenn man gleichzeitig auch die Zwei-Faktoren-Authentifizierung verwendet). Tools wie Keepass, Dashlane, LastPass und 1Password funktionieren auch mit Smartphones (Android und Apple).

✓ **Über einen öffentlichen PC oder ein fremdes Gerät einloggen**

Verwenden Sie einen Einmal-Code und loggen Sie sich am Schluss manuell aus allen Online-Konten aus.

✓ **Remote-Management bei Diebstahl**

Wird Ihnen ein Gerät gestohlen, können Sie das Gerät über den Android Device Manager oder iCloud lokalisieren, es sperren und den Inhalt löschen. Es ist wichtig, die IMEI-Nummer Ihres Geräts zu kennen, damit Sie Ihrer Telefongesellschaft und Ihrem Versicherer im Falle eines Diebstahls angegeben werden kann. Diese Seriennummer findet man auf der Rechnung, auf der Verpackung sowie in den Einstellungen des Geräts selbst.

✓ **Antivirus und Firewall**

Aktualisieren Sie Ihren Virenscanner regelmässig auf allen Geräten (Smartphone, Tablet und PC). Verschiedene kostenlose Antivirenprogramme wie Sophos oder Avast bieten einen Basisschutz. Die kostenpflichtigen Versionen von G Data, Kaspersky oder Bit Defender verfügen allerdings über eine bessere Virenerkennung und eine ganze Reihe von Sicherheitstools (wie Firewall, Schutz vor Ransomware und dem Zugang zur Webcam oder

Eindringen). Wenn Sie über öffentliche WLAN-Netze surfen, installieren Sie ein VPN und sichern Sie den Empfang Ihrer E-Mails.

✓ **Anwendungen**

Laden Sie Softwareprogramme und Applikationen nur von vertrauenswürdigen Websites herunter. Wenn Sie nicht sicher sind, verzichten Sie besser auf den Download. Achten Sie darauf, dass Ihr Browser und die anderen Applikationen immer auf dem neusten Stand ist.

✓ **Zusatzmodule für sicheres Surfen**

In den Einstellungen Ihres Browsers können Sie Ihren Browserschutz erhöhen und dafür sorgen, dass Firmen keine Daten über Ihre Internetaktivitäten sammeln und so dynamische Preise generieren bei Ihren Online-Einkäufen. Wichtig ist auch, die Aufzeichnung der Nutzeraktivitäten in Ihrem Browser auszuschalten. Dennoch ist es essentiell, dass Sie die Zuverlässigkeit der von Ihnen besuchten Websites prüfen und Online-Werbung unterbinden. Websites, die eine gesicherte Verbindung bieten (was man am «https» zu Beginn des Links erkennen kann), sind generell sicherer. Das Sicherheitsniveau der gängigsten Browser ist unterschiedlich hoch.

✓ **Werbung – im Internet ist nichts gratis**

Firmen wollen Geld verdienen, deshalb ist auch im Internet nichts gratis. Geben Sie nur die Informationen bekannt, die in den Pflichtfeldern wirklich gefordert werden, und hinterlassen Sie so wenig Spuren wie möglich.

✓ **Geografische Lokalisierung von Nutzern und Werbung**

Deaktivieren Sie den Ortungsdienst und die Funktion «Ad-Tracking» auf den einzelnen Geräten, wenn Sie den Dienst nicht benötigen.

✓ **Die richtigen Fragen stellen und die richtigen Antworten erhalten**

Sie brauchen kein Experte zu sein, um Ihr Privatleben im Internet zu schützen. Über die gängigen Browser finden Sie Informationen zum Datenschutz in den wichtigsten sozialen Netzwerken. Zudem können Sie sich ganz einfach darüber informieren, wie Sie den Browserverlauf löschen oder den Ortungsdienst auf dem Smartphone deaktivieren. Generell empfehlen wir Ihnen, sich auf zwei verschiedene Informationsquellen zu stützen und zu prüfen, ob deren Inhalte ähnlich sind.

✓ Rubrik «Datenschutz»

Besuchen Sie unsere Rubrik «Sicherheit & Datenschutz» mit zusätzlichen Informationen zu den Gefahren beim Datenschutz. Sie finden Ratschläge, wie Sie sich im Alltag schützen und den gesetzlichen Rahmen einhalten sowie viele weitere nützliche Tipps für Kinder und Jugendliche, für Eltern und für Lehrpersonen.

*** Stéphane Koch** ist Master of Advanced Studies in Bekämpfung von Wirtschaftskriminalität und Spezialist in Öffentlichkeitsarbeit. Ausserdem ist er Ausbildner, Berater und Lehrbeauftragter im Bereich Informations- und Kommunikationstechnologien.

Jugend und Medien ist die nationale Plattform zur Förderung von Medienkompetenzen. Kinder und Jugendliche sollen sicher und verantwortungsvoll mit digitalen Medien umzugehen wissen. Die Plattform bietet Eltern sowie Lehr- und Fachpersonen Informationen, Unterstützung und Tipps für eine sinnvolle Begleitung von Kindern und Jugendlichen. www.jugendundmedien.ch