Soziale Medien und Netzwerke

Soziale Medien wie Facebook, Instagram oder Youtube boomen. Auf den ersten Blick geht von diesen fürs E-Banking keine unmittelbare Gefahr aus. Durch die grosse Verbreitung und deren oft sorglose Nutzung sind sie aber auch für Kriminelle interessant.

Schützen Sie sich, indem Sie...

- nur Informationen von sich veröffentlichen, welche Sie auch einem wildfremden Menschen auf der Strasse anvertrauen würden.
- den Zugriff auf Ihre veröffentlichten Informationen einschränken (Privatsphäre-Einstellungen).
- nur Personen als «Freunde» annehmen, welche Sie auch über andere Kanäle (z.B. persönlich) kennen.
- ein «gesundes Mass an Misstrauen» haben, wenn Sie Nachrichten von unbekannten Personen erhalten.
- keine Links aus unbekannten Quellen aufrufen und Dokumente, Bilder, Videos etc. zuerst prüfen, bevor Sie sie öffnen.
- unterschiedliche und starke Passwörter für verschiedene Dienste nutzen.
- aktuelle Software (Browser, Betriebssystem, Antivirus etc.) einsetzen.

Hacker lieben die Sozialen Medien

Durch die gezielte Platzierung von Links durch Kriminelle werden Soziale Medien oft als sogenannte «Virenschleuder» zur Verbreitung von Malware missbraucht.

Ebenfalls können über diese Netzwerke persönliche Informationen über Personen gewonnen werden, welche in einem nächsten Schritt für eine gezielte Attacke verwendet werden könnten.

Persönliche Informationen

In Sozialen Medien teilt man Fotos und persönliche Daten mit «Freunden». Diese Informationen können aber auch durch einen Angreifer missbraucht werden, z. B. für einen «Social Engineering» (https://www.ebas.ch/social-engineering/) -Angriff.

Überlegen Sie sich deshalb sorgfältig, welche Informationen Sie auf Ihrem Profil preisgeben: Veröffentlichen Sie nur die persönlichen Daten, die Sie auch einem wildfremden Menschen auf der Strasse anvertrauen würden.

Ein «gesundes» Mass an Misstrauen sollte bei der Nutzung dieser Netzwerke generell vorhanden sein. Man sollte nur Freundschaftsanfragen von Personen, die man auch persönlich oder über andere Kanäle kennt, annehmen.

Dateien wie Dokumente, Bilder, Videos etc. sollten immer zuerst mit einer Antiviren-Software geprüft werden. Und dies unabhängig davon, ob sie aus vertrauenswürdiger oder nichtvertrauenswürdiger Quelle stammen.

Beiträge und Interaktionen

Seien Sie sich bewusst, dass nicht nur Ihre veröffentlichten persönlichen Daten, sondern auch alle Ihre Beiträge

(Posts) sowie Interaktionen wie Likes, Shares usw. von den Dienstbetreibenden analysiert und zu einem (unter Umständen unvorteilhaften oder gar falschen) Benutzerprofil aggregiert und zum Beispiel zu Werbezwecken weiterverkauft werden. Diese generierten Profile verbreiten sich schnell über weitere soziale Netzwerke, bleiben über mehrere Jahre erhalten und lassen sich oft nur schwierig oder gar nicht mehr löschen.

Somit gilt in Sozialen Netzen: Nicht nur zurückhaltend, sondern stets auch gut überlegt kommunizieren!

Links

Der Aufruf eines Links zu einer schädlichen Webseite genügt, um Ihr Gerät mit Malware zu infizieren (Drive-By-Download (https://www.ebas.ch/drive-by-download/)). Daher sollte man sich vor dem Klick überlegen, ob man den Inhalt wirklich sehen will, und ob es sich um eine vertrauenswürdige Quelle handelt.

Unter www.getlinkinfo.com (http://www.getlinkinfo.com) können verkürzte Link-Adressen überprüft werden (siehe Weiterführende Informationen (#moreInfo)).

Ausserdem ist es unerlässlich, dass insbesondere Browser, Betriebssystem und Virenschutzprogramm sowie alle weitere Software auf dem aktuellsten Stand gehalten werden («Schritt 3 - Vorbeugen» (https://www.ebas.ch/3-vorbeugen-mit-software-updates/)).

Login und Passwort

Die Anforderungen an ein gutes Passwort (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) gelten auch für Soziale Medien und Netzwerke. Die Zugangsdaten müssen unbedingt vertraulich behandelt werden.

Zudem ist es wichtig, dass für die verschiedenen Dienstleistungen auch unterschiedliche Passwörter verwendet werden. **Verwenden Sie für Soziale Medien und Netzwerke auf keinen Fall dasselbe Passwort wie fürs E-Banking!**

Um Ihr soziales Konto besser zu schützen, sollten Sie zudem wo immer möglich die Zwei-Faktor-Authentisierung (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) des jeweiligen Dienstes verwenden.

Datenschutz

Im Zusammenhang mit Sozialen Medien und deren Verwendung wird auch der Schutz der persönlichen Information grossgeschrieben. Diesbezügliche Informationen und Verhaltens-Tipps erhalten Sie auf der Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz.html) .

Empfohlene Einstellungen

Soziale Medien bieten viele Konfigurationsmöglichkeiten. Unsere Checklisten sollen Sie bei der sicheren Konfiguration von Facebook (https://www.ebas.ch/facebook-einstellungen/) , X (Twitter) (https://www.ebas.ch/twitter-einstellungen/) , Instagram (https://www.ebas.ch/instagram-einstellungen/) und LinkedIn (https://www.ebas.ch/linkedin-einstellungen/) unterstützen.

Soziale Medien haben nur scheinbar nichts mit E-Banking-Sicherheit zu tun, denn Betrügern ist für die Informationsbeschaffung jede Quelle recht.

Mit wenigen effektiven Massnahmen erreichen Sie einen sorgenfreien Umgang mit den neuen Medien.

Merkblatt: *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2020/01/socialmediaSKP_de.pdf)*

Weiterführende Informationen für Interessierte

Einige Soziale Medien beschränken die Maximallänge der veröffentlichten Einträge. Twitter zum Beispiel erlaubt nur 280 Zeichen pro Nachricht. Um auch längere Links versenden zu können, bieten verschiedene Webseiten einen Service an, der Links verkürzt. Aus

«https://www.ebas.ch/de/ihrsicherheitsbeitrag/erweiterter-schutz/114-socialengineering»

wird zum Beispiel

«http://bit.ly/P4u765»

Anhand der verkürzten Adresse kann nicht mehr direkt festgestellt werden, wohin der Link wirklich führt. Dies kann durch Kriminelle ausgenutzt werden, indem Sie verkürzte Links verwenden, welche auf infizierte Webseiten verweisen.

Bevor ein verkürzter Link aufgerufen wird, sollte daher vorgängig die Original-Adresse überprüft werden. Unter www.getlinkinfo.com (https://www.getlinkinfo.com) können solche verkürzten Adressen zum Beispiel überprüft werden. Neben der Originaladresse erhält man zudem weitere Informationen zur Webseite.