Blick

Angriff auf Ihre Daten

So schützen Sie sich vor SMS-Betrügern

ZÜRICH - Betrüger missbrauchen die Namen grosser Schweizer Firmen, um ahnungslose User abzuzocken. Doch es gibt ein paar Möglichkeiten, um solche Nachrichten zu erkennen.

Betrüger geben sich als Schweizer Firmen aus. HERMANN BREDEHORST

Michael Bolzli

Ob Coop, Migros oder Sunrise: Immer wieder werden die Namen bekannter Schweizer Unternehmen von Betrügern missbraucht. Diese verschicken gefälschte Nachrichten – sogenannten Spam – per Mail oder SMS. Dadurch wollen Betrüger an Kontodaten oder Logins kommen.

Jüngster Fall ist die Post. Seit letzter Woche sind gefälschte SMS des gelben Riesen im Umlauf. Wer den Link in der Nachricht anklickt, lädt sich eine Schad-Software aufs Handy.

Doch so weit muss es nicht kommen. BLICK hat bei Dominik Schupp nachgefragt, wie man betrügerische Nachrichten erkennt. «Früher war es einfacher», gibt der Wirtschaftsinformatiker von der Hochschule Luzern zu. Denn damals waren Grammatik und Rechtschreibung häufig sehr fehlerhaft. Spam war schnell an schlechtem Deutsch auszumachen.

Nicht mehr voller Fehler

Das hat sich geändert: Ob per SMS oder E-Mail: Heute kommen betrügerische Nachrichten oft in gutem Deutsch daher. Erkennen kann man die Mails trotzdem. «Oft verfügen die Mails über eine generelle Anrede. Das ist verdächtig», sagt Schupp. Zudem sollte man unbedingt die Absender-Adresse überprüfen.

Grundsätzlich handeln viele Betrüger gleich. «Wenn man aufgefordert wird, auf einen Link zu klicken und die Nutzerdaten einzugeben, sollte man skeptisch werden», sagt Schupp. Und ergänzt: «Finanzinstitute verschicken nie solche Nachrichten.»

Spam-Experte Dominik Schupp NO CREDIT

In solchen Fällen empfiehlt er, den Link zu überprüfen. Dazu fährt man am Computer mit dem Mauszeiger über die Internet-Adresse. Nach kurzer Zeit taucht die ganze URL auf – also die Adresse der Website, die hinter dem Link steckt.

«Wichtig dabei ist der DNS-Name – also in der Regel der Name des Unternehmens – der sich vor der ersten Landesdomäne befindet» sagt der Informatiker. Bei einer Schweizer Adresse ist die Landesdomäne .ch. «Am einfachsten verwendet man nie einen Link, der per E-Mail zugeschickt wurde – sondern gibt die Adresse immer manuell ein», empfiehlt Schupp.

Doch nicht immer erkennt man gefälschte E-Mails oder SMS-Nachrichten sofort. Darum empfiehlt Schupp unbedingt eine Anti-Viren-Software. Die gibt es auch für Android-Smartphones. «Bei iPhones und iPads ist das zur Zeit nicht nötig», sagt der Wirtschaftsinformatiker. Denn dort kann man nur Software installieren, die aus dem iTunes-Store stammt – und nicht wie bei Handys mit dem Android-Betriebssystem Programme, die irgendjemand in seinem Hinterzimmer programmiert hat.

Mehrere Mail Adressen

Falls man eine betrügerische Nachricht öffnet, ist noch nicht alles verloren. «Heikel ist es erst, wenn man auf Phishing-Seiten die verlangten Informationen eingibt», sagt Schupp. Dennoch empfiehlt er, solche Nachrichten umgehend zu löschen.

Zudem rät er zu mehreren E-Mail-Adressen. «Eine für die Korrespondenz. Die andere für Online-Einkäufe und andere Dienstleistungen», sagt er. Zudem sollte die eigene E-Mail-Adresse zurückhaltend verbreitet werden.

Eine Zusammenfassung und weitere Tipps im Umgang mit Internet-Sicherheit hat die Hochschule Luzern auf dieser Webseite zusammengetragen.

Publiziert am 22.06.2016 | Aktualisiert am 22.06.2016