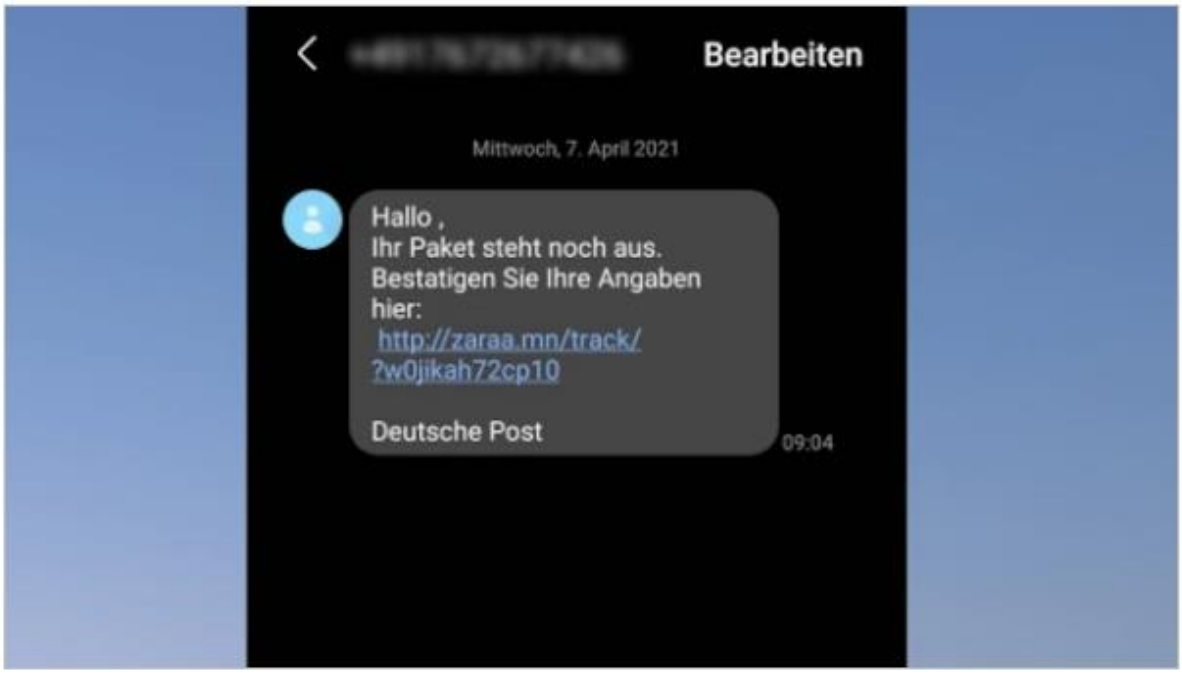
SPAM-WELLE NACH DATENLEAK – SO STOPPEN SIE UNERWÜNSCHTE SMS

Da kann Facebook noch 1.000 Mal behaupten, dass die kursierenden Daten aus einem älteren Leak stammen und die Lücke längst geschossen ist: Fakt ist, dass in den letzten Tagen über 500 Millionen Datensätze von Facebook-Nutzern von Cyberkriminellen im Internet angeboten wurden. Die Daten umfassen neben Namen auch Handynummern, Orte, sowie teilweise Geburtsdaten und Mail-Adressen. Wie sich zeigt, erhalten betroffene Nutzer aus Deutschland derzeit vermehrt SMS-Spam-Nachrichten.



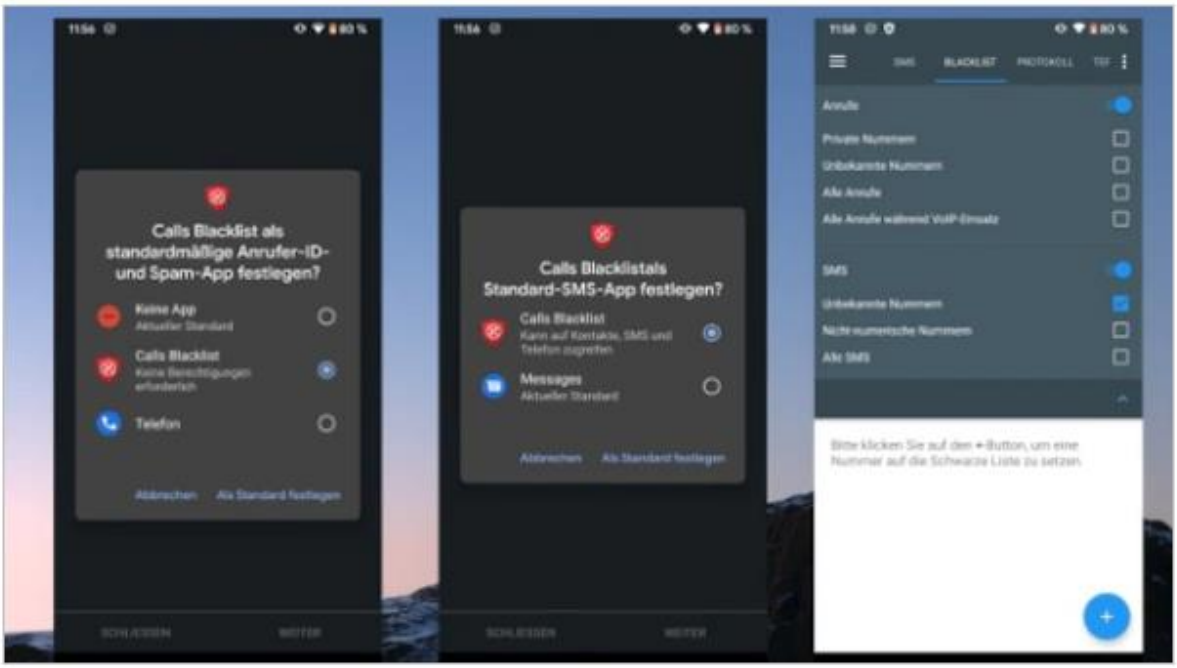
Sie können ganz leicht prüfen, ob auch Ihre Daten abgegriffen wurden. Die Web-App Have I Been Pwned können Sie nutzen, um nach Mail-Adresse und neuerdings auch nach ihrer Handynummer zu suchen. Wie sich zeigt, sind in den Datensätzen deutlich mehr Handynummern enthalten. Geben Sie Ihre mobile Telefonnummer im internationalen Format ein, das bedeutet, Sie stellen "+49" für eine deutsche Nummer voran, dafür lassen Sie die "0" am Anfang Ihrer Telefonnummer weg. Die Nummer 01234567 wird dann zu "+491234567".

Viele Nutzer in Deutschland bemerken den Facebook-Leak derzeit über ein vermehrtes Aufkommen von SMS-Spam. Die Methode ist nicht neu, die Versender scheinen sich aber aus den geleakten Handynummern von Facebook zu bedienen. Dabei handelt es sich derzeit oft um gefakte Paketbenachrichtigungen. Nutzer werden in den Nachrichten aufgefordert, auf einen Link zu tippen, um zu sehen, wo sich eine angebliche Paketlieferung befindet. Statt des Paketstatus werden Nutzer aber auf Malware-Seiten umgeleitet.

Die Nachrichten, die wir bisher gesehen haben, sind nicht besonders gut gemacht. Erstens sieht man im Absender die Nummer im Klartext und nicht etwa Hinweise auf Paketdienstleister wie DHL oder DPD, außerdem sind die Links oft auf den ersten Blick verdächtig, weil sie auf unübliche Domains verweisen. Doch manchmal kann man sich beim schnellen Drüberlesen auch täuschen lassen und erkennt Schreibfehler in Domains nicht. Wenn Sie so eine SMS kriegen, sollten Sie auf keinen Fall den enthaltenen Link antippen und schon gar nicht Bezahldaten oder Passwörter auf danach geöffneten Webseiten eintippen.

Android-Nutzer haben einen eingebauten Spamschutz in der Messages-App integriert und dieser ist auch aktiviert. Sie können das in den Einstellungen der App prüfen. Tippen Sie dort den Punkt "Spamschutz" an. Es gibt dann nur einen Ein-Ausschalter bei der Option "Spamschutz aktivieren". Doch diese Funktion allein schützt Sie nicht perfekt vor unerwünschten Nachrichten.

Sollten Sie schon Paket-Spam oder ähnliches per SMS erhalten haben, halten Sie die Nachricht kurz gedrückt und wählen Sie "Blockieren" sowie "Spam melden" aus. Damit können Sie Spam-SMS von der verwendeten Nummer stoppen. Da Angreifer aber meistens ziemlich schnell die Absendernummern wechseln, kann es sein, dass Sie dieses Prozedere öfter durchspielen müssen.



Für Android gibt es auch spezielle Apps, die das ganze Theme noch komfortabler angehen. Calls Blacklist zum Beispiel kann sich als SMS-App einklinken und dann zum Beispiel alle SMS-Nachrichten von Absendern blockieren, die nicht in Ihren Kontakten stehen. Das klingt gut, Sie sollten aber vorsichtig sein, weil viele Firmen auch SMS als Benachrichtigungswerkzeug einsetzen.

Was genau passiert, wenn man einen der Spam-Links antippt, kann man pauschal nicht sagen. Die Palette an Möglichkeiten ist umfangreich: Möglich ist zum Beispiel, dass Sie in einer Abofalle landen, dass Passwörter abgezweigt werden oder man versucht Ihnen eine verseuchte App unterzuschieben, die Sie ausspioniert.

Sollten Sie wirklich derart ausgetrickst worden sein, dass Sie ein Abo abgeschlossen haben, sollten Sie versuchen das Abo zu kündigen, falls sich der Anbieter herausfinden lässt. Zudem sollten Sie verwendete Zahlungsmittel wie Kreditkarten sperren lassen und Anzeige erstatten.

Grundsätzlich ist in so einem Fall nicht mehr gewährleistet, dass Ihr Gerät noch sicher ist. Bedenkliche Anzeichen dafür sind unerwünschte Apps auf Ihrem Gerät sowie aufdringliche Werbeanzeigen, die sich nur schwer abklemmen lassen. Was man in so einem Fall tun sollte? Falls vorhanden, ein Backup des Handys zurückspielen. Hat man das nicht parat, hilft natürlich ein Reset, wobei beim Zurückstellen auf Werkseinstellungen auch Inhalte verloren gehen.