Augen auf bei diesen beliebten WhatsApp-Betrügereien

Augen auf bei diesen beliebten WhatsApp-Betrügereien

In Sicherheitswissen by Jochen on November 23, 2015 | Français, English, Deutsch zitiert vom blog.emsisoft.com
WhatsApp ist nicht ohne Grund so beliebt – kostenlos unbegrenzt Nachrichten über WLAN und mobile Datennetze austauschen, und das mit Menschen auf der ganzen Welt – da kann kein Anbieter mit seinen SMS-Paketen mithalten. Leider zieht diese Beliebtheit aber auch zahllose Betrüger an. Von angeblichen Fehlern über gefälschte Updates bis zu Abo-Fallen oder Phishing: WhatsApp-Nutzer geraten überall allzu leicht ins Fadenkreuz von Kriminellen. Erfahren Sie hier mehr über beliebte WhatsApp-Betrugsmaschen und wie Sie sich davor schützen.

Gefälschte WhatsApp-Versionen

Installieren Sie immer die echte WhatsApp-Version und laden Sie niemals WhatsApp über Links herunter, die man Ihnen zuschickt. Laden Sie die App nur aus dem jeweiligen offiziellen App-Store herunter (Google Play, Apple App-Store usw.). Sollten Sie Zweifel daran hegen, dass es sich bei der aktuell auf Ihrem Gerät verwendeten Version um eine echte handelt, so entfernen Sie die App und laden Sie sie erneut aus Ihrem jeweiligen App-Store herunter.

Gefälschte Voicemails

Bei dieser Masche handelt es sich einfach um gefälschte Voicemails — Sie brauchen lediglich auf den Link zu klicken, um in die Falle zu tappen!

Sie erhalten eine Nachricht mit dem Betreff “Incoming Voice Message”. Sie brauchen nur auf den darin enthaltenen Link zu klicken, und schon haben Hacker Zugriff auf Ihre persönlichen Daten und können sogar Ihr Gerät sperren!

WhatsApp Gold

Bei “WhatsApp Gold” handelt es sich um eine Betrugsmasche, die über soziale Medien den Weg zu Ihnen findet. Ihnen wird eine Premiumversion angeboten, bei der man angeblich die blauen Häkchen, die signalisieren, dass man eine Nachricht gelesen hat, deaktivieren kann, oder Fotos unkomprimiert verschicken kann.

Doch kaum klicken Sie auf den Link, sind Sie schon in einer Abo-Falle gelandet und dürfen beispielsweise monatlich 4,99 bis 14,97 € berappen. Eine neue Version mit dem Namen “WhatsApp Elegant Gold” macht bereits die Runde. Dabei werden Sie auf eine Webseite geleitet, auf der Sie nach Ihrer Telefonnummer gefragt werden, um eine neuere “verbesserte” WhatsApp-Version zu erhalten.

WhatsApp-Spionage

Es gibt eine ganze Menge Apps, mit denen Sie Leute über WhatsApp ausspionieren können. Traurige Realität ist, dass Sie bei einer Google-Suche nach “WhatsApp-Spionage” auf jede Menge Artikel stoßen, in denen Sie erfahren, wie Sie andere ausspionieren können, jedoch nicht, wie Sie sich selbst gegen dieses Eindringen in Ihre Privatsphäre schützen können.

Allerdings gibt es einen Haken: die meisten dieser sog. Spionage-Apps haben jede Menge Malware im Gepäck, die sie auf Ihrem Gerät abladen. Sollten Sie also die Benutzung einer dieser Apps in Erwägung ziehen, seien Sie gewarnt, dass Sie selbst ausspioniert werden!

Phishing mit WhatsApp bei Migros

Dabei werden Kunden mit der Aussicht auf den Gewinn eines Gutscheins über 500 Franken in die Falle gelockt.

Ähnliche Maschen finden sich mit Gutscheinen für McDonald's, IKEA, H&M, KFC und Zara sowie anderen großen Unternehmen. Diese Betrügereien sind in mehreren Sprachen und Länder aufgetreten und stellen somit ein internationales Problem dar. Dabei werden Ihre Daten abgegriffen, was viel schwerwiegender ist als die Hoffnung auf einen vermeintlichen Gewinn, den Sie nie erhalten.

Vorgetäuschte Fehler

Hier gaukeln die Cyberkriminellen den Nutzern vor, dass WhatsApp bei Ihnen nicht mehr funktioniert. Sie verschicken eine Nachricht, in der es heißt: „ACHTUNG: Bei Ihrem WhatsApp ist ein Problem aufgetreten. ‚x'-Nachrichten wurden blockiert [OK]". Wer nun in der Nachricht auf den mitgesendeten OK-Button klickt, wird auf die Seite „fun-clix.com" weitergeleitet. Dort reicht ein einfacher Klick aus, um ein teures Abo abzuschließen. Wer in die Falle geht, muss dann pro Woche rund 15 Euro bezahlen.

So erkennen Sie Betrugsversuche über WhatsApp

Betrügereien über WhatsApp nehmen zu, sollten Sie jedoch nicht von der Nutzung dieser nützlichen, tollen App abhalten. Denn schließlich können Sie damit weltweit kostenlos kommunizieren, und es wäre doch jammerschade, wenn

Sie darauf verzichten müssten. Behalten Sie einfach die folgenden Tipps im Hinterkopf, um nicht in die Falle zu tappen:

1. Vorsicht bei Nachrichten von WhatsApp

Stutzig werden sollten Sie, wenn Sie aus welchem Grund auch immer direkt von WhatsApp Nachrichten erhalten. Dies würde das Unternehmen nämlich niemals tun; daher handelt es sich bei solchen Nachrichten höchstwahrscheinlich um einen Betrugsversuch. Wie WhatsApp auf seiner eigenen Website schreibt, "[…], dass wir WhatsApp nicht verwenden, um Nachrichten an dich zu senden."

2. Augen auf bei Nachrichten mit der Bitte um persönliche Daten

Allgemein bitten WhatsApp (und andere legitimen Apps) Sie nicht einfach so nach persönlichen Daten. Sollten Sie Zweifel daran hegen, dass es sich um eine berechtigte Anfrage, können Sie jederzeit über die Website von WhatsApp eine Anfrage an den Kundendienst senden. Sollte Ihr Messenger-App keine Kontaktdaten für den Kundendienst anbieten, fragen Sie andere Nutzer, ob sie Ähnliches beobachtet haben.

3. Wahrscheinlich haben Sie nicht gewonnen

Es sei denn, Sie haben direkt an einem Ausschreiben teilgenommen, bei der man Sie nicht hinters Licht führen möchte. Die Verlockung ist groß, aber Sie haben wohl kaum 500 Franken gewonnen, ohne auch nur einen Finger gerührt zu haben. Nicht einmal durch Ausfüllen einer Umfrage. Denn wie heißt es so schön? "Wenn es zu schön klingt, um wahr zu sein, dann ist es das wahrscheinlich auch."

4. Teilen Sie niemals Ihre MAC-Adresse oder IMEI

Jedes Handy verfügt über eine sog. IMEI (International Mobile Equipment Number), die es eindeutig ausweist, sowie über eine sog. MAC-Adresse (Media Access Control), durch die es im Netzwerk eindeutig identifiziert werden kann. Jeder WhatsApp ist direkt mit einem Telefon durch diese spezielle Nummer verknüpft, wodurch diese sich wie ein Passwort zu Ihrem Konto verhält. Sofern

ein Hacker Ihre Telefonnumer und MAC oder IMEI in die Hände bekommt, kann er sich also leicht Zugriff auf Ihr Konto verschaffen.

Bedenken Sie: selbst die vorsichtigsten Nutzer können Betrügern in die Falle gehen, so bedacht sie auch vorgehen mögen. Holen Sie sich Anti-Malware-Software für Ihr mobiles Gerät und bringen Sie in Erfahrung, wie Ihre Messenger-App mit seinen Nutzern kommuniziert. Sie können selbstverständlich die neuesten, tollen Apps benutzen, sollten jedoch immer auf das Schlimmste vorbereitet sein; denn Vorsicht ist immer besser denn Nachsicht.

Weiteres zu früheren WhatsApp-Betrugsmaschen und dazu, wie Sie sich schützen können, finden Sie auch in einem älteren Artikel in unserem Blog.

Wir wünschen eine schöne (betrugsfreie) Zeit!