Die Top 8 der fiesesten Instagram-Abzocken

Seit seiner Einführung 2010 hat Instagram mehr als eine Milliarde Konten eröffnet. Fast 100 Millionen Fotos werden täglich ausgetauscht. Doch wo sich viele Menschen tummeln, mischen sich auch Kriminelle unter das Volk. Das Geschäft mit fiesen Instagram-Scams boomt – insbesondere seit Beginn der Pandemie. Sophos beschreibt die acht häufigsten Betrügereien und wie man sich davor schützt.

Instagrams Popularität mag an seiner Einzigartigkeit liegen. Kein anderes Social-Media-Netzwerk bietet diese visuelle Vielfalt an, denn anders als Twitter und Facebook ist diese Plattform explizit für das Teilen von Bildern und Videos entwickelt worden. Für viele Menschen ist Instagram heute fester Bestandteil ihres Lebens, und Unternehmen wie Influencer nutzen die Plattform als Einkommensquelle.

In den letzten Jahren wuchs mit dem Erfolg jedoch auch der groß angelegte Betrug: Im Januar 2021 hieß es, Instagram-Betrugsanzeigen haben sich seit Ausbruch der Pandemie Anfang 2020 um 50 Prozent gesteigert (Quelle: BBC).

Da die Abzocker immer geschickter und aggressiver werden, ist es umso wichtiger, den Schwindel rechtzeitig zu erkennen und zu wissen, was man tun kann, wenn man Betrügern auf den Leim gegangen ist.

Hier sind die Top 8 der häufigsten Instagram-Betrügereien:

1. Phishing-Betrug
Phishing-Betrüger versuchen Zugang zum fremden Instagram-Konto zu bekommen, indem sie einen manipulierten Link schicken – als Insta-Direktnachricht oder via E-Mail – um dem Opfer auf einer Fake-Instagram-Seite Username und Passwort zu entlocken. Haben sie Erfolg, liegen ihnen die persönlichen Informationen zu Füßen – mitsamt der Änderungsmöglichkeit des Passworts, um das Opfer aus seinem eigenen Account zu sperren.
Fake-Insta-“Warnungen“ sind in letzter Zeit weit verbreitet und sehen den originalen Instagram--Hinweisen täuschend ähnlich.

Tipp: Bei einer Direktnachricht von einem Konto mit 13.000 „Followern“ aber 0 Posts sollte der Nutzer hellhörig werden. Diese Nachrichten nicht öffnen, sondern gleich löschen.

2. Fake Influencer Sponsoren
Der Aufstieg der Influencer auf Instagram hat auch Kriminelle auf den Plan gerufen, die sich ihrerseits als etablierte Unternehmen ausgeben und Influencern getürkte Werbe-Deals anbieten. Die Betrüger erschleichen sich von ihren Opfern so die persönlichen Bank-Daten – wohin natürlich niemals ein Kampagnen-Honorar gezahlt werden wird...

3. Romance Scam (= Liebesbetrüger)
Nicht alle Instagram-Tricks sind schnell initiiert. Manche Gegner haben einen langen Atem, wenn es um ihren Schwindel geht. Romance Scammers lullen ihre Opfer in Online-Beziehungen ein, die sie nur vorspielen. Hier steckt mitunter jahrelange Vorarbeit drin. Ist der betrogene Partner einmal fest an der Angel, wird dieser um Geld gebeten für Visum, Flüge, Reisekosten etc. Romance Scammers sind nie um Ausreden verlegen und besonders penetrant, wenn es um ihre „Ziele“ geht.

Wie hält man sie sich vom Leib?

Niemals Geld an eine Person senden, die man noch nie gesehen hat (auch wenn dieses Geld das Begegnen ermöglichen soll). Selbst mit anwaltlicher oder gerichtlicher Unterstützung ist es fast unmöglich, die Beträge zurückzuholen.

4. Geschenke! Geschenke!
Influencer halten ihre Follower oft mit limitierten Werbegeschenken bei Laune, bei denen die Unternehmen den glücklichen Gewinnern Gratisprodukte oder Dienstleistungen versprechen. Oft sind diese luxuriös, ob Designer-Handtaschen oder Airpods. An sich eine schöne Idee. Nur, auch hier geben sich Kriminelle wieder als jemand aus, der sie nicht sind: von diesem „Fake-Influencer" bekommen Nutzer dann die Benachrichtigung, etwas gewonnen zu haben. Aber: es sollen doch Bitteschön die „Versandkosten" getragen werden. Auch hier werden persönliche Informationen eingesammelt, die sich für weitere kriminelle Zwecke einsetzen lassen.

5. Kredit-Betrug
Aufgepasst bei einer Direktnachricht, die einen Kredit mit fantastischen Raten anbietet. Um sich diesen zu sichern, müsse der Nutzer lediglich eine Kaution hinterlegen. Hier sagt schon der gesunde Menschenverstand, dass das Schwindelei ist.

6. Falschinvestitionen
Wer möchte nicht „schnell reich werden"? Bei diesem verlockenden Angebot sollte der Instagram-Nutzer lieber wegsehen, denn diese Investition wird sich ganz sicher nicht auszahlen. Die Betrüger posieren oft mit teuren Autos und ihrem gefälschten „Self-Made"-Status, um die Opfer zu einer Investition ins Leere zu überzeugen. Zu Beginn wirken die E-Mails oder der Webseiten-Login professionell und echt, so dass die Opfer sich sicher fühlen und weiteres Geld investieren. Oder noch schlimmer, auch Freunde und Familie zu Beteiligungen ermuntern.

7. Job-Betrug
Hinter einer interessanten Stellenanzeige kann auch ein Cyberkrimineller stecken. Er sucht nach persönlichen Informationen, die er via Bewerbung erhält, wie zum Beispiel Adresse, Telefonnummer, Einwanderungsinformationen etc. Hier handelt es sich um groß angelegten Identitätsdiebstahl, um sich Darlehen, Kreditkarten und mehr in fremdem Namen zu ergaunern.

8. Kreditkarten-Betrug
Kreditkartenbetrug startet oft harmlos mit einem Instagram-Post, der „Schnelles Geld" verspricht, zum Beispiel ein Gewinnspiel mit großer Belohnung. Klickt man auf den eingebetteten Link, erscheinen Abfragen für die Kreditkarte oder Bank-Daten.
Mit den gestohlenen Daten gelingen den Kriminellen dann mühelos Online-Einkäufe.

Was können Instagram-Nutzer gegen diese fiesen Acht tun?
Die beschriebenen Instagram-Betrugsmaschen sollten Nutzer achtsamer machen. Das heißt nicht, dass hinter jedem Post ein Krimineller wartet, aber es gibt sie und mit diesen Tipps lässt sich die eigene Sicherheit schon einmal deutlich verbessern:

- Ein gutes Passwort wählen
  Dieser Schritt erfordert nur wenig Mühe, hat aber einen enormen Effekt. Jedes Konto, jeder Login braucht ein EIGENES Passwort, keines darf für mehrere Kanäle verwendet werden. Denn wurde ein Account geknackt, können auch die anderen damit eingenommen werden. Ein Passwort-Manager unterstützt bei Vergabe und Verwaltung.

- Nicht zu viel preisgeben
  Persönliche Informationen sollten vorsichtig preisgegeben werden, auch bei vertrauten Instagram-Kontakten. Da es eine Bild-Plattform ist, müssen sich Nutzer auch bewusst

sein, was im Hintergrund alles auffällt. Hier haben wir Tipps speziell zu „Hintergrundwissen“ zusammengestellt.

- Bleiben Sie aufmerksam
  Ein Konto oder eine Nachricht erscheinen Ihnen nicht ganz koscher? Dann reagieren Sie nicht darauf. Ein Angebot klingt zu gut, um wahr zu sein? Dann ist es womöglich auch nicht wahr. Vertrauen Sie Ihrem gesunden Menschenverstand.

- Nutzen Sie ein privates Konto
  Solange nicht der Ehrgeiz besteht, Influencer zu werden und Instagram eher als eine Plattform betrachtet wird, um mit Freunden in Kontakt zu bleiben, auch ein privater Account. Nur die eigenen Follower (und die kann man sich ja aussuchen) sehen dann, was auf dem privaten Konto gepostet wird.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de