Clickbait-Kommentare in diversen Variationen führen auf einen falschen Profilviewer.

Eine solche Kombination sahen wir bisher auch noch nie: Clickbait-Kommentar auf Facebook mit augenscheinlich sensationeller Thematik, der aber zu einem angeblichen Profilviewer führt.

Jene Kommentare haben gemeinsamen, dass die URL immer mit mehreren X und O beginnt. So sehen sie beispielsweise aus:

Dubiose Kommentare

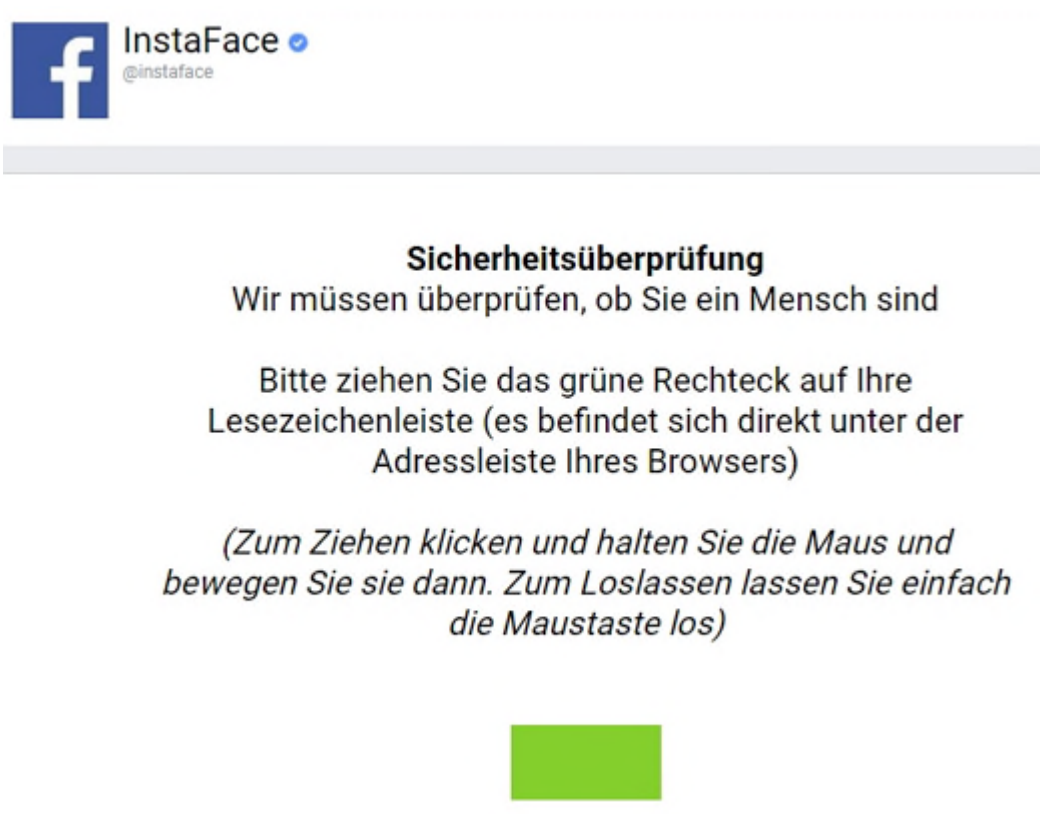
Die Intention hinter der scheinbar willkürlichen X und O-Kombination in den URLs: Die tatsächliche Adresse ist dadurch nicht sichtbar, ein automatischer Block jener Adressen durch Facebook wird dadurch zusätzlich erschwert.

Der Clickbait führt zu einem falschen Profilviewer

Klickt man nun neugierig auf die Links, landet man auf einer Seite namens „InstaFace“, welche rein optisch wie Facebook aussieht – da enden aber auch schon die Gemeinsamkeiten! Angeblich sei ein technischer Fehler bei Facebook entdeckt worden, wodurch es nun möglich sei, die Besucher des eigenen Profils einsehen zu können.

Das ist nicht Facebook!

Klickt man hier auf „WEITER“, dann muss man ein grünes Rechteck in seine „Lesenzeichenleiste“ des Browser ziehen:



Doch Achtung!

Ab diesem Moment haben die Betrüger vollen Zugriff auf das Facebook-Konto! Dahinter versteckt sich ein sogenanntes „JAVASCRIPT“ und bei diesen Daten und Inhalten handelt es sich fast um alle Funktionen, die auch in der Facebook API-Dokumentation enthalten sind.

Was bedeutet dies nun für das Opfer?

Hat man das Script einmal aktiviert, dann haben der oder die Betrüger vollen Zugriff auf:

- **alle privaten Daten** des Nutzers, die in seinem Profil vorhanden sind. Dazu zählen u.a. das Geburtsdatum, die Telefonnummer, Arbeitsplatz, Orte, Familienmitglieder usw.
- **auf alle Statusbeiträge** die der Nutzer jemals geschrieben hat,
- auf alle **Bilder und Videos,**
- auf alle **gelikten Seiten und Gruppen.**
- Zudem kann der oder die Betrüger auch auf alle **Facebook-Seiten** und **Facebook-Gruppen** zugreifen, bei denen der Nutzer Admin-Rechte besitzt.
- Sprich: Eine Übernahme des kompletten Profils sowie Seiten und Gruppen ist daher möglich!

Aber nicht nur das!

Der oder die Betrüger haben auch noch **Zugriff auf den Messenger des Opfers,** und man kann dadurch alle Nachrichten lesen bzw. könnten die Betrüger auch in seinem Namen nun Nachrichten versenden.

Hat man auch noch bei **Instagram** ein Konto und dieses mit seinem Facebookprofil verknüpft, dann bekommen die Betrüger auch Zugriff auf dieses.

Hat man also den Betrügern den Zugriff gestattet, dann können diese dieselben Handlungen durchführen, wie das Opfer selbst!

Hier findet man alle Rechercheberichte zum Thema „Profilviewer auf Facebook“ vor.