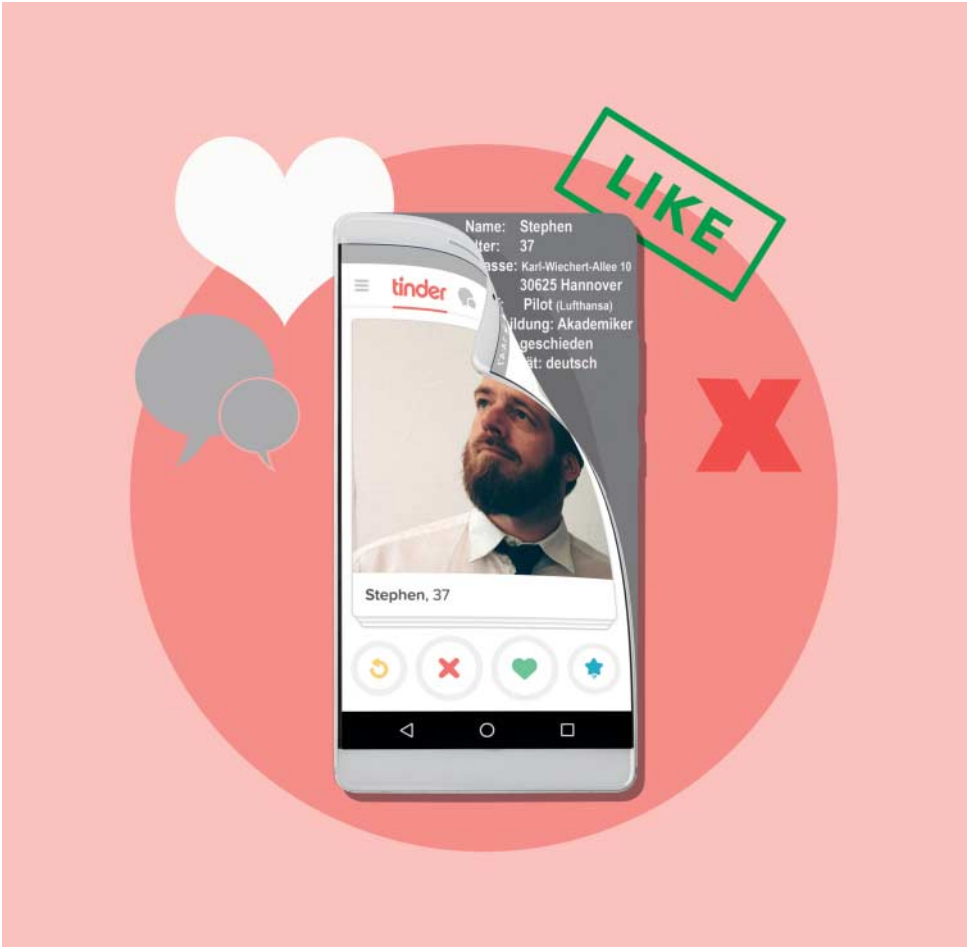


Tindersicherung

Anonymität in der Dating-App Tinder bewahren

Tinder ist die derzeit wohl populärste Flirt- und Dating-App. Sie verspricht völlig anonymes Kennenlernen – doch in der Praxis funktioniert das nicht immer perfekt.

Von Stefan Porteck

Kennlern- und Dating-Apps haben mittlerweile kein Schmuddel-Image mehr. Trotzdem wünschen sich Anwender vor allem Anonymität. Andernfalls kann es schnell passieren, dass es plötzlich Whatsapp-Nachrichten von verschmähten Partnern hagelt.

In der Vergangenheit war Tinder selbst mit teilweise massiven Datenschutz-Pannen negativ aufgefallen. Oft machen aber auch die Nutzer so viel falsch, dass ein Minimum an Social Engineering ausreicht, um im Nullkommanix herauszubekommen, mit wem man es zu tun hat. Letzteres betrifft auch andere bekannte Flirt-Apps. Gründe genug für uns, der Tinder-App auf die Finger zu schauen und zu prüfen, ob die Datenschutz-Probleme mittlerweile gelöst wurden. Zusätzlich haben wir beleuchtet, welche Fehler die Nutzer vermeiden sollten, um nicht versehentlich ihre wahre Identität auf einem Silbertablett zu servieren.

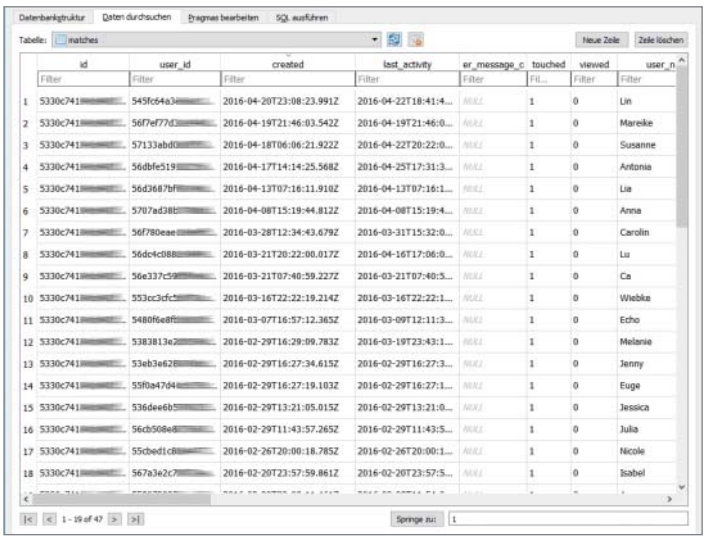
Das Konzept von Tinder ist simpel: Man meldet sich in der App über seinen Facebook-Account an und gibt dann lediglich das gesuchte Geschlecht und den gewünschten Umkreis an. Anschließend schlägt Tinder passende Personen zum Kennenlernen vor.

Wisch und weg

Hierfür präsentiert die App Karten mit Profilfotos, Vorname, Alter und der Entfernung voneinander. Mit einem Wisch schiebt man die Karte nach links oder rechts und entscheidet so über Gefallen oder Nicht-Gefallen. Die vorgeschlagene Person bemerkt davon zunächst nichts. Nur wenn sich zwei Nutzer gegenseitig

sympathisch finden, kommt ein sogenannter Match zustande. Erst dann können beide einander anschreiben.

Zunächst haben wir untersucht, welche Informationen die Tinder-App an andere Nutzer schickt. Unsere größte Sorge galt einem Fauxpas aus den Anfangstagen der App: Tinder hatte die Entfernung zwischen zwei Nutzern nicht auf dem Server errechnet, sondern lokal auf den Smartphones der Nutzer. Dafür verschickte die App bei jeder vorgeschlagenen Person in den Meta-Daten deren exakten Nutzerstandort. Wer den Netzwerkverkehr abhörte, konnte anhand der GPS-Koordinaten bis auf wenige Meter genau einsehen, wo sich eine vorgeschlagene Person zuletzt aufgehalten hatte. Beim Tindern vom heimischen Sofa gab man also ganz nebenbei seinen Wohnort preis – gruselig.



In seiner SQL-Datenbank speichert Tinder alle Nutzerinformationen, darunter das Alter und das Geschlecht. Hier finden sich aber auch Angaben, die die App gar nicht anzeigt.

Abgehört

Mithilfe eines SSL-Proxies belauschten wir als Man-in-the-middle den Netzwerkverkehr zwischen der Tinder-App und dem Server. Zur Entwarnung: Im Datenstrom tauchen nun keine Geo-Koordinaten der potenziellen Partner mehr auf. Einzig den eigenen Standort verschickt die App, damit der Server die Entfernung bestimmen kann. Dieser liefert bei jedem Vorschlag das Ergebnis in Form von `"distance_mi":166` als Kilometerangabe zurück.

Auch das bietet keinen hundertprozentigen Schutz vor Stalkern, doch immerhin müssten diese den Chatpartner in ein längeres Gespräch verwickeln und sich ins Auto oder die Bahn setzen, um mithilfe von Triangulation hinter den Aufenthaltsort des Tinder-Match zu kommen. Das ist mühsam und nur dann erfolgreich, wenn sich der oder die Ausgespähte währenddessen nicht vom Fleck bewegt.

Außer dem Vornamen zeigt Tinder auch das Alter der vorgeschlagenen Personen an. Ein zweiter Datensatz, der uns auffiel lautete:

```
"birth_date_info":"fuzzy birthdate
active, not displaying real birth_date"
"birth_date":"1980-09-23T00:00:00.000Z"
```

Eigentlich hätten wir erwartet, dass der Server auch das Alter ausrechnet und nicht Nutzerdaten wie das Geburtsdatum durch die Welt schickt. Stattdessen hat Tinder sich beim Alter dafür entschieden, das Ausrechnen den Clients zu überlassen. Immerhin stimmte bei unseren Stichproben der Hinweis, dass nicht das korrekte Geburtsdatum übertragen wird. Bei mehreren Tinder-Matches war der Geburtstag stets zufällig, lediglich das Geburtsjahr und der -Monat stimmten. Mit einem Namen nebst Geburtsdatum lässt sich schon einiger Unfug anstellen – so macht die App es Identitätsdieben wenigstens etwas schwerer.

Ausgelesen

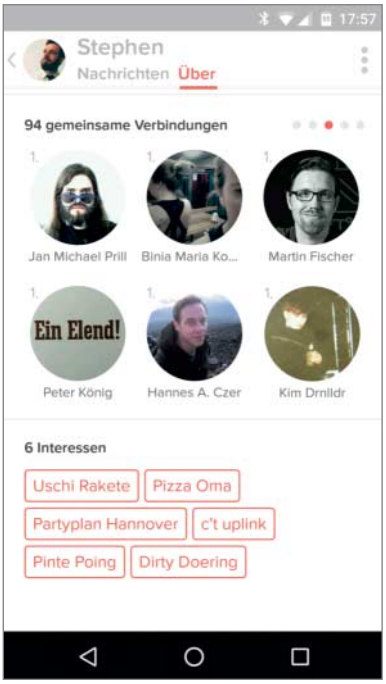
Um sicherzustellen, dass keine Daten verschlüsselt an unserem Proxy vorbeigeschleust werden, haben wir uns auch die interne Datenbank der App genauer angesehen. Sie liegt bei Android-Smartphones im Daten-Ordner der App unter /data/data/com.tinder/databases/tinder.db. Normalerweise kommen Nutzer an die Datenbank nicht ran. Um sie auf einen PC zu kopieren und dort mit einem SQLite-Viewer zu betrachten, mussten wir auf ein Telefon mit Root-Rechten zurückgreifen.

Spannend ist vor allem die Tabelle „Matches“. Hier speichert Tinder die Daten von Personen, zu denen man eine Verbindung aufgebaut hat. Größtenteils fanden wir hier genau die Informationen, die man auch in der App zu sehen bekommt – beispielsweise das Alter und das Geschlecht. Eine Ausnahme: Die Spalte „last_activity“ weist aus, wann der Chatpartner zuletzt mit Tinder online gewesen ist. Diesen „Zuletzt Online“-Status zeigt die offizielle App mittlerweile nicht mehr an. Damit wollen die Anbieter offenbar verhindern, dass Schnüffler ein Bewegungsprofil mitschneiden könnten. Konsequenterweise sollte Tinder dieses Datum dann auch nicht mehr im Netzwerkverkehr mitschicken.

Intern identifiziert Tinder jeden Nutzer anhand einer eindeutigen 24-stelligen hexadezimalen ID. Sie taucht in mehreren Tabellen der Datenbank auf; unter anderem in der Tabelle „photos“. Darin sind für jeden Match die URLs hinterlegt, über die die App die Profilbilder herunterlädt. Der Aufbau der Adressen beginnt stets mit dem Server-Namen, gefolgt von der Tinder-ID und schließlich der ID des jeweiligen Fotos. Eine vollständige URL hat also folgenden Aufbau: `http://images.gotinder.com/Tinder-ID/Foto-ID.jpg`

Erfreulicherweise birgt das kein Missbrauchspotenzial: Wir haben es im Browser und mit Tools wie wget nicht geschafft, auf den Tinder-Servern das gesamte Verzeichnis einer Tinder-ID zu durchsuchen. Ohne Kenntnis der eindeutigen und offenbar zufällig erzeugten Foto-ID hat man keinen Zugriff auf die Bilder. Löscht man die Verbindung mit einem anderen Tinder-Nutzer, kann er oder sie über die URLs noch auf die bestehenden Fotos zugreifen. Auf später hinzugefügte Bilder wird mangels ID kein Zugriff möglich sein.

Bei der Analyse der Nutzer- und Bild-Verwaltung stellten wir zudem fest, dass die Entwickler auch hier nachgebessert haben: In der Vergangenheit hatte Tinder statt eigener Nutzer-IDs einfach die Facebook-ID übernommen und für Profilfotos die Facebook-Foto-IDs genutzt. Über



In den gemeinsamen Verbindungen tauchen auch Freunde auf, die Tinder gar nicht benutzen. Sie und die gemeinsamen Interessen reichen meist aus, um einen Tinder-Nutzer auf Facebook zu finden.

diese IDs ließ sich das Facebook-Profil des jeweiligen Tinder-Nutzers aufrufen.

Allgegenwärtiges Facebook

Obwohl weder die mitgeschnittenen Daten noch die Datenbankeinträge Rückschlüsse auf das Facebook-Profil aktueller oder ehemaliger Chatpartner erlauben, ist die Bindung an das soziale Netzwerk aus mehreren Gründen problematisch: Jeder Tinder-Nutzer hat zwangsläufig auch ein Facebook-Profil, über das er sich wahrscheinlich eindeutig identifizieren lässt. Alle Infos, die Tinder einblendet, stammen von Facebook – darunter das Alter, der Arbeitgeber und die Interessen. Da Facebook sich leicht durchsuchen lässt, ist es für viele Schnüffler die Startadresse. Auch wenn bei Tinder selbst keine gravierenden Datenschutzprobleme auftreten, enttarnen sich viele Nutzer über Facebook versehentlich.

In vielen Fällen schlägt Tinder Personen vor, mit denen man gemeinsame Freunde auf Facebook hat. Ein Blick in deren Freundesliste reicht dann meist schon aus, um zu wissen, mit wem man es zu tun hat. Weit häufiger als vermutet lassen sich die Flirtwilligen einfach über die bei Tinder angezeigten Vornamen identifizieren. Viele Nutzer finden Facebooks Datenschutzeinstellungen offenbar zu kompliziert oder vertrauen dem Netzwerk grundsätzlich nicht. Statt das eigene Profil ordentlich vor Einblicken Fremder zu schützen, vertrauen sie lieber darauf, unter einem Fantasienamen nicht gefunden zu werden.

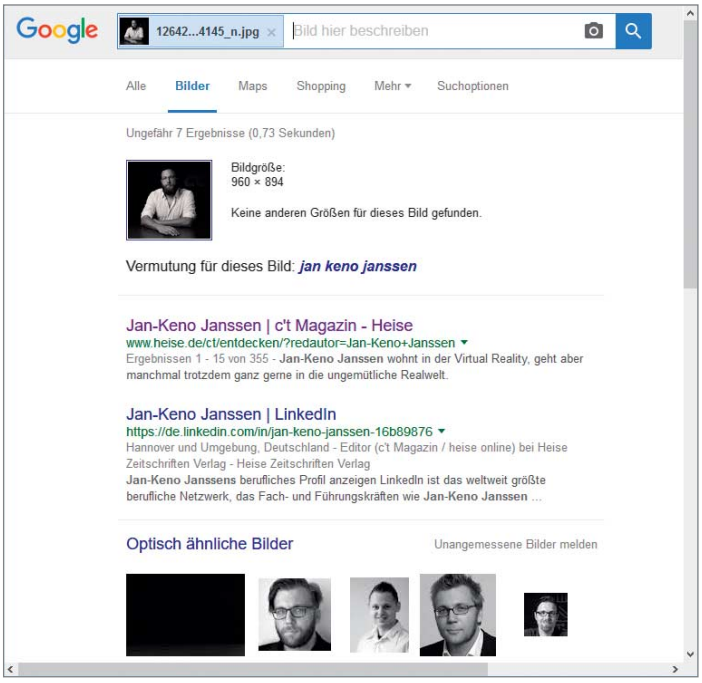
Dieser Fantasiename taucht dann auch im Tinder-Profil auf, weshalb diese vermeintliche Schutzmaßnahme Tinder-Nutzer dummerweise besonders schnell enttarnt: In der Suche von Facebook rangieren Personen, die man wahrscheinlich kennt – beispielsweise aufgrund gemeinsamer Freunde oder gleichem Wohnort – meist ganz oben in der Trefferliste. Mit einem Allerweltsnamen wie „Stefan“ geht man mit großer Wahrscheinlichkeit in der sehr langen Trefferliste unter oder wird mit etwas Glück von Facebook erst gar nicht angezeigt. Nennt man sich dagegen auf Facebook (und damit auch auf Tinder) „Rumpelstilzchen77“, ist das fast schon die Garantie, dass das eigene Facebook-Profil der erste Treffer sein wird.

Eine weitere Schwachstelle sind die gemeinsamen Interessen auf Tinder. Für sie greift die App auf Likes bei Facebook zurück. Auch darüber lassen sich Nutzer auffinden: Facebooks sogenannter Searchgraph erlaubt nicht nur die Suche nach Namen, sondern auch nach Nutzern mit gewünschten Attributen. Stellt man die Sprache von Facebook auf Englisch um, fördert der Suchbegriff „Men who like c't magazin and heise online“ männliche Nutzer zutage, die sowohl auf der Facebook-Seite von c't als auch auf der von heise online auf „Gefällt mir“ geklickt haben. Das Ganze ließe sich auch mit dem Alter, anderen Facebook-Likes, dem Wohnort oder bisherigem Arbeitgeber oder Ausbildungsstätten kombinieren – alles Informationen, die im eigenen Tinderprofil für jeden sichtbar sind.

Für den Searchgraph gibt es mittlerweile sogar Meta-Suchmaschinen, die einem die Arbeit abnehmen. So lassen sich beispielsweise auf www.searchisback.com diverse Suchparameter einfach zusammenklicken. Danach leitet die Suchmaschine auf die Ergebnisseite bei Facebook weiter. Bereits mit der Facebook-Suche kommt man recht weit.

Gefahr lauert aber auch bei anderen sozialen Netzwerken: Seit einigen Monaten zeigt Tinder im Profil besuchte Schulen, Unis oder die bisherigen Arbeitgeber an. In Kombination mit dem Alter und dem Vornamen reichen diese Informationen oft schon aus, um damit Karriere-Netzwerke wie Xing oder Linkedin erfolgreich zu füttern.

Ein weiteres Risiko für die eigene Privatsphäre geht von den genutzten Fotos aus. Zwar dürften die meisten Nutzer da-



Googles Bildersuche zeigt zu einem hochgeladenen Bild weitere Fundstellen an. Wer bei vielen Diensten das gleiche Profilfoto nutzt, wird schnell identifiziert.

rauf achten, dass ihre Tinder-Profilfotos keine persönlichen Daten enthalten oder Rückschlüsse darauf erlauben. Doch viele Nutzer verknüpfen Tinder zusätzlich mit ihrem Instagram-Account. Das ist nur dann eine gute Idee, wenn dort weder im Profil noch auf irgendeinem der Bilder der eigene Klarname auftaucht. Wie schnell allerdings ein Bild durchrutschen kann, zeigen diverse Urlaubsfotos von Flugreisenden, auf denen die Bordkarte im Reisepass steckt …

Selbst sorgfältig gewählte Profilbilder können sich als Bumerang erweisen, wenn Neugierige davon einen Screenshot erstellen und diesen per Drag-and-Drop in die Bildersuche von Google ziehen. Die Suchmaschine spuckt dann bereitwillig aus, auf welchen Webseiten dieses Bild noch auftaucht. Häufig sind unter den Treffern die Webseite des Arbeitgebers oder eben wieder soziale Netzwerke.

Lösung: Datensparsamkeit

In unseren Tests klappte es leider nicht, auf der Facebook-Seite in der App-Einstellungen der Tinder-App einzelne Rechte wie den Zugriff auf die Freundesliste oder die Angaben zum Arbeitsplatz dauerhaft zu entziehen. Beim nächsten Start forderte die App die Rechte erneut an und ließ sich ohne Zustimmung nicht starten.

Wer keine peinlichen Überraschungen erleben möchte, sollte mit persönlichen Daten also bewusst sparsam umgehen. Dazu gehören Anpassungen der Privatsphäre-Einstellungen und der Profil-Einstellungen von Facebook, damit das eigene Profil nicht über externe Suchmaschinen gefunden werden kann und ausschließlich Freunde die eigenen Likes und Bilder sehen. Im Idealfall blendet man die eigene Freundesliste für alle aus. Informationen über frühere oder aktuelle Wohnsitze, besuchte Schulen oder den beruflichen Werdegang sollten ebenfalls erst gar nicht bei Facebook hinterlegt werden – das erspart nebenbei auch Anfragen von Freunde-Sammlern, mit denen man seit der Grundschule eh nichts mehr zu tun hat.

Die Profilbilder kann Tinder nur aus Facebook-Alben abgreifen. Deshalb sollten diese Fotos – wie auch die für andere Dating-Apps – bei keinem anderen Dienst als Profil- oder Erkennungsbild genutzt werden. Am besten nutzt man das als Profilbild ausgewählte Foto ausschließlich für Tinder. Damit Facebook-Stalker einen nicht wiedererkennen, sollten die Bilder zudem in einem privatem Album liegen, auf das man nur selbst Zugriff hat.

Wer diese Grundregeln beherzt, dürfte halbwegs sicher davor sein, dass der schon längst gelöschte Tinder-Match plötzlich am Sonntagnachmittag an der Tür klingelt, um sich auf einen Kaffee einzuladen. *(spo@ct.de)* c't