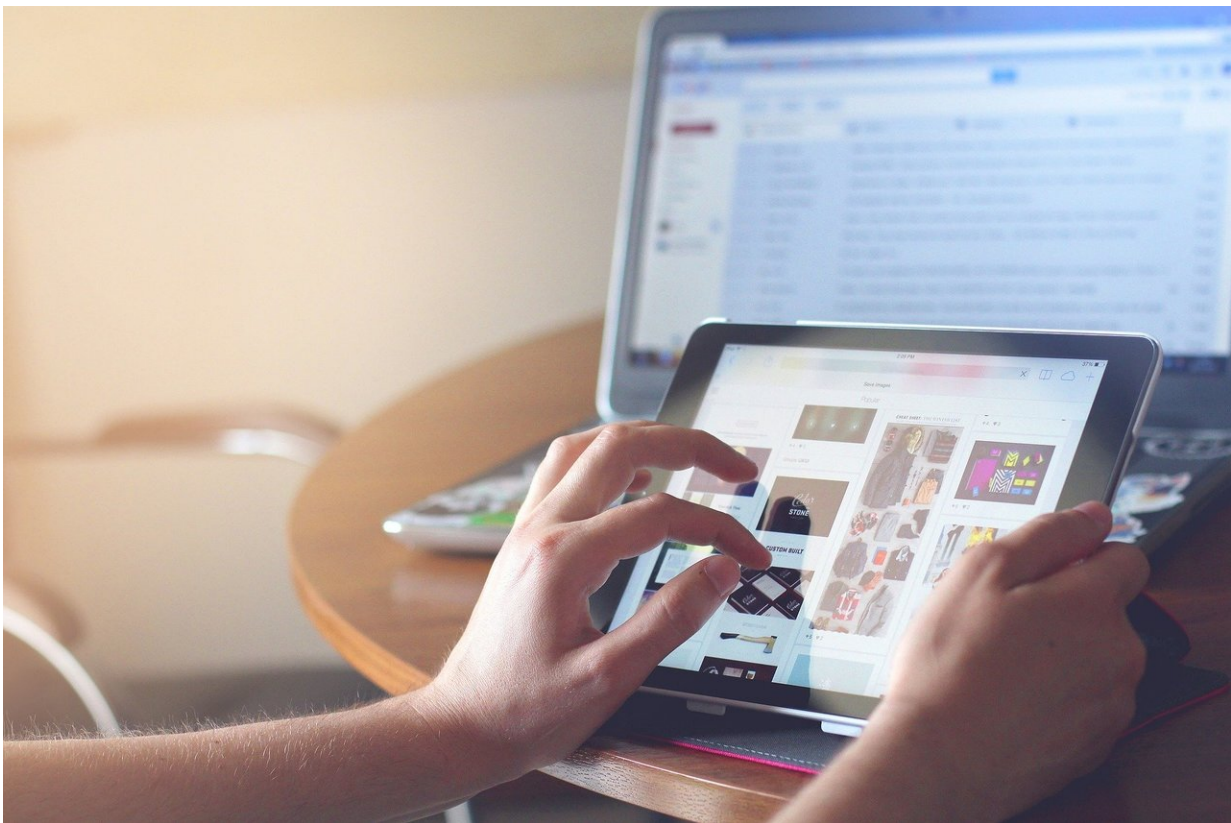


Dating apps: How to protect your personal data from hackers, advertisers

January 22 2020, by Dalvin Brown



Credit: CC0 Public Domain

Setting up a profile on most dating apps is simple.

You input your name, upload some photos, set your location and sexual

preferences and you're launched into a sea of mostly singles to chat with, meet and take things from there.

During the process, you're also giving up valuable, [personal information](#) to platforms that often monetize by selling that data to third parties you've never heard of. Not to mention, [data breaches](#) abound.

Grindr, OkCupid and Tinder, for example, were at the center of controversy last week when researchers accused the companies of disclosing highly personal information and breaking privacy laws. Each app denied many of the accusations.

But why should you care?

When you sign up for a dating or hookup app, "you're putting information out there that people can use against you. Whether it's hackers or predators, a cybercriminal can use that information to send you a phishing email, and you can fall for it," said Jo O'Reilly, a data privacy expert at ProPrivacy. "For women, you're putting information out there like addresses and phone numbers that can make you vulnerable to stalkers."

Most [dating apps](#) monetize by persuading users to sign up for premium memberships, according to Nazmul Islam, a junior forecasting analyst at eMarketer. However, dating app subscription growth is slowing, so the platforms are looking for other ways to diversify revenue streams.

"They've started offering sponsored surveys where they will give users access to premium features if they take a survey from a marketing partner," Islam said. "The user gets paid in virtual currency like temporary premium access, while the app is being paid actual dollars by advertisers for the content."

So your [personal details](#) like height, weight and sexual orientation may be up for sale. Some of these apps, like Grindr, also have information on STD status and your exact location.

The situation is particularly dire in countries where your sexual practices can get you in trouble with the law if the information gets into the wrong hands, O'Reilly said.

Advertisers use this treasure trove of consumer data to display marketing materials online that are tailor-made for you, like restaurants you'd enjoy or clothes you'd buy based on your assumed amount of disposable income and other metrics.

But it's also important to remember that online dating companies also have access to your private messages and any personal pictures and videos you share. And the companies will likely give that information up if subpoenaed, O'Reilly said.

And like many other tech sectors, dating apps are rife with data breaches.

In 2019, Heyyo reportedly left a server exposed on the internet, exposing nearly 72,000 users' data online. That same year, Coffee Meets Bagel sent an email to users informing them that an "unauthorized party" gained access to their information. Perhaps most infamous of all was the Ashley Madison infidelity scandal in 2015.

"These companies convince us to overshare. They convince us that the more information we put out there, the better the match we're going to get," O'Reilly said.

Still, there are things you can do to better protect yourself from having your personal data shared with advertisers or being exposed to bad actors

on the internet.

Dating app tips from an internet privacy expert:

1. Only sign up for apps that you have to pay for. Free apps are more likely to sell your data, O'Reilly said.
2. Use only your first name or a nickname as it makes you harder to identify if hackers access your account details.
3. Don't give away your home address, work address, [phone number](#) or email address in private messages, or when signing up.
4. Don't let other users persuade you to continue conversations via another app like WhatsApp or Messenger. They could be trying to scam you, O'Reilly said.
5. Turn off location settings, or use them sparingly.
6. Use as little personal and identifiable information on your profile as possible. That includes displaying your education, employer or other identifiable markers.

"Whatever data you give to an app, it's not just going to stay on an app," O'Reilly said. "The best approach is for consumers to assume that whatever data or private information they put onto an app will be sent to advertising companies."

(c)2020 U.S. Today

Distributed by Tribune Content Agency, LLC.

Citation: Dating apps: How to protect your personal data from hackers, advertisers (2020, January 22) retrieved 23 April 2024 from <https://techxplore.com/news/2020-01-dating-apps->

[personal-hackers-advertisers.html](#)

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.