Dangerous liaisons

The security issues of dating apps

Tatyana Shishkova,
Senior Malware Analyst,
Kaspersky
@sh1shk0va

kaspersky

3 billion

Swipes on Tinder in a single day in March 2020*

*According to the Tinder report "Future of dating is fluid"

But how safe are dating apps?

Potential risks of dating apps

- Revealing user's real name, work, school information, location
  - Stalking
  - Doxing (publicizing previously private personal information)
- Stealing account credentials
- App-related scams

What safety gaps in the apps can lead to this?

In 2017, we studied 9 popular dating apps and found several security risks:

- **6** made it possible to find user's location
- **4** made it possible to find user's real name and social media accounts
- **4** made it possible to intercept data sent from the app

Has the situation improved in 2021?

Apps

We selected dating applications with a large global user base, as well as those ranked highly by respected publications, such as CNET, PC Mag, and Tom's Guide.

The following apps were studied:

Registration

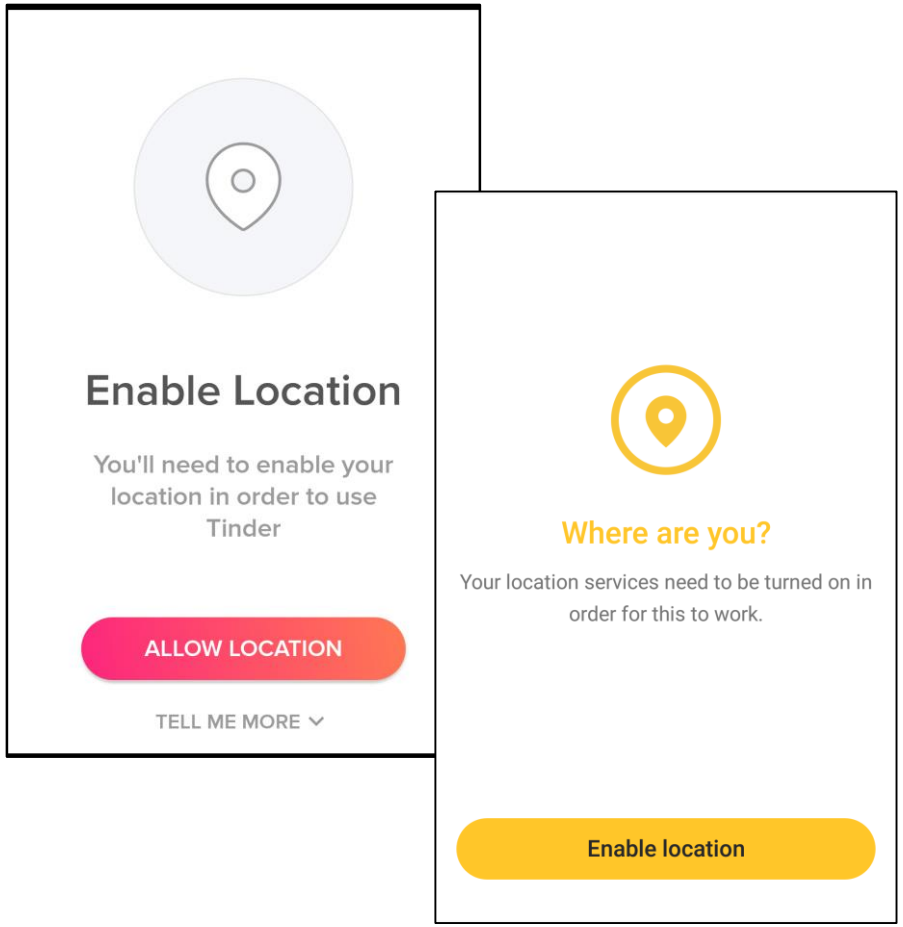
- All apps, except Pure, allow users to register via a Facebook account
- Most of apps require a phone number for verification (in some apps, the user should provide the phone number if their Facebook account is suspicious)
- In Tinder, OkCupid, Bumble and Happn, the user may connect other accounts (Instagram, Spotify) to their profile

Location

	Need Location permission	Allow to manually specify location in free version	Allow to manually specify location in paid version
Tinder	+		+
OkCupid		+	
Badoo		+	
Bumble	+		+
Mamba		+	
Pure		+	
Feeld		+	
Happn	+		
Her	+		+

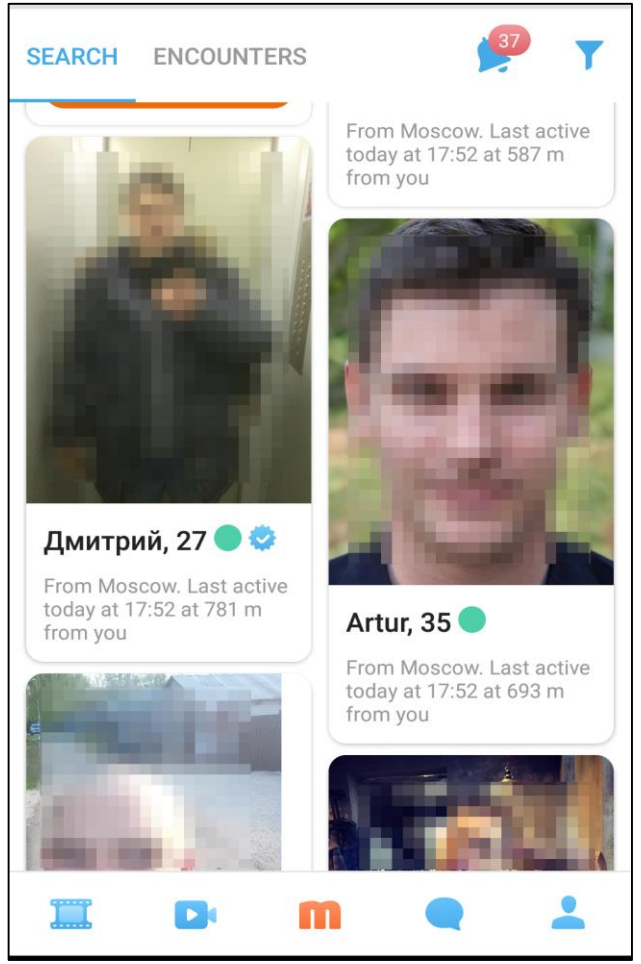
Location

- 4/9 apps will not work without Location permission
- All apps, except Happn, allow users to specify their location manually in either the free or paid version



Revealing user's location

If the app shows distance between users, it is possible to calculate the user's approximate location by moving around the victim



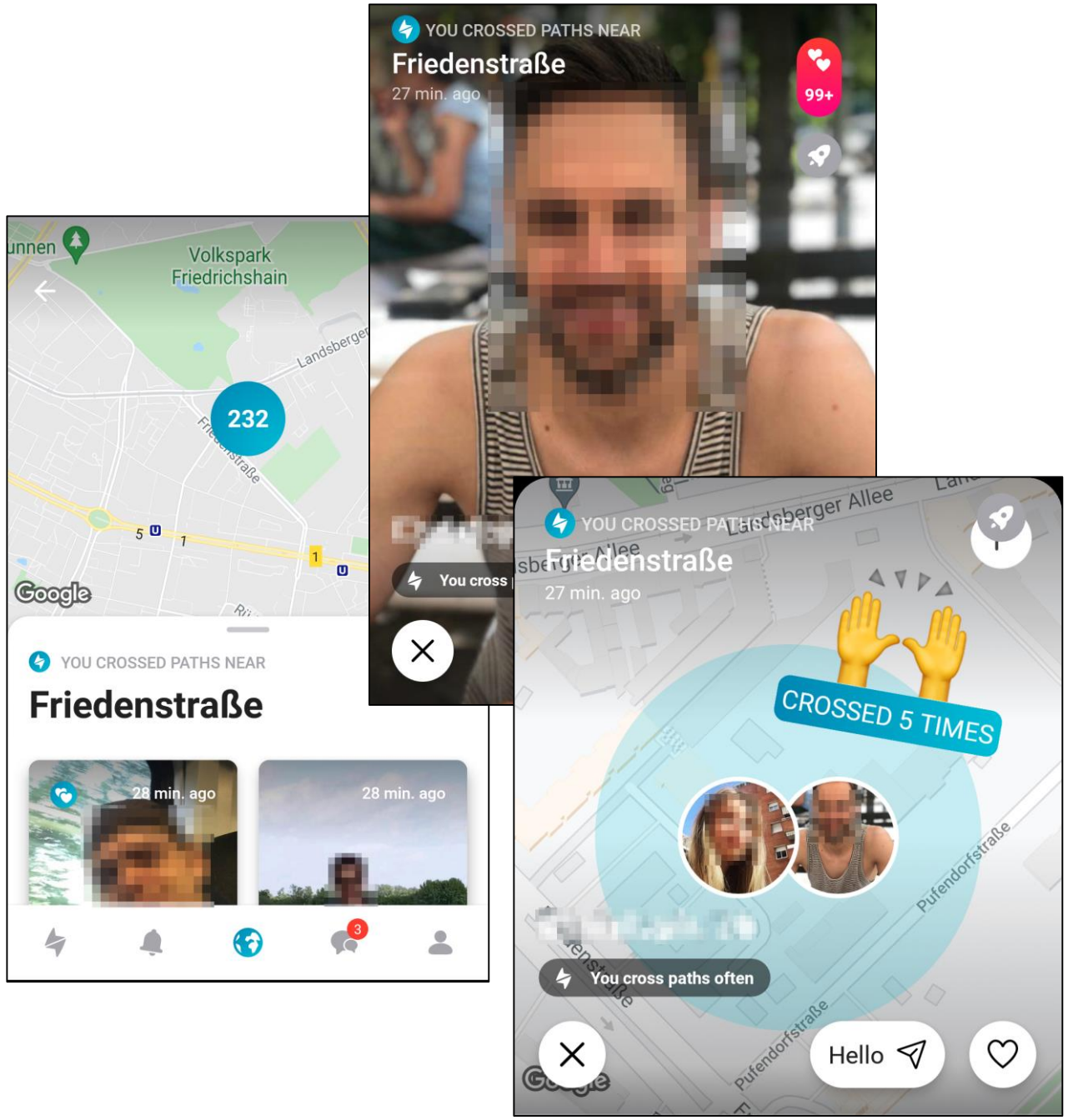
Revealing user's location

- Too much effort for attackers if done manually
- Most of the apps allow to use fake GPS services to mock location
- The less accurate an app is, the more measurements you need to make
- Will not work if the user specified location manually

Revealing user's location

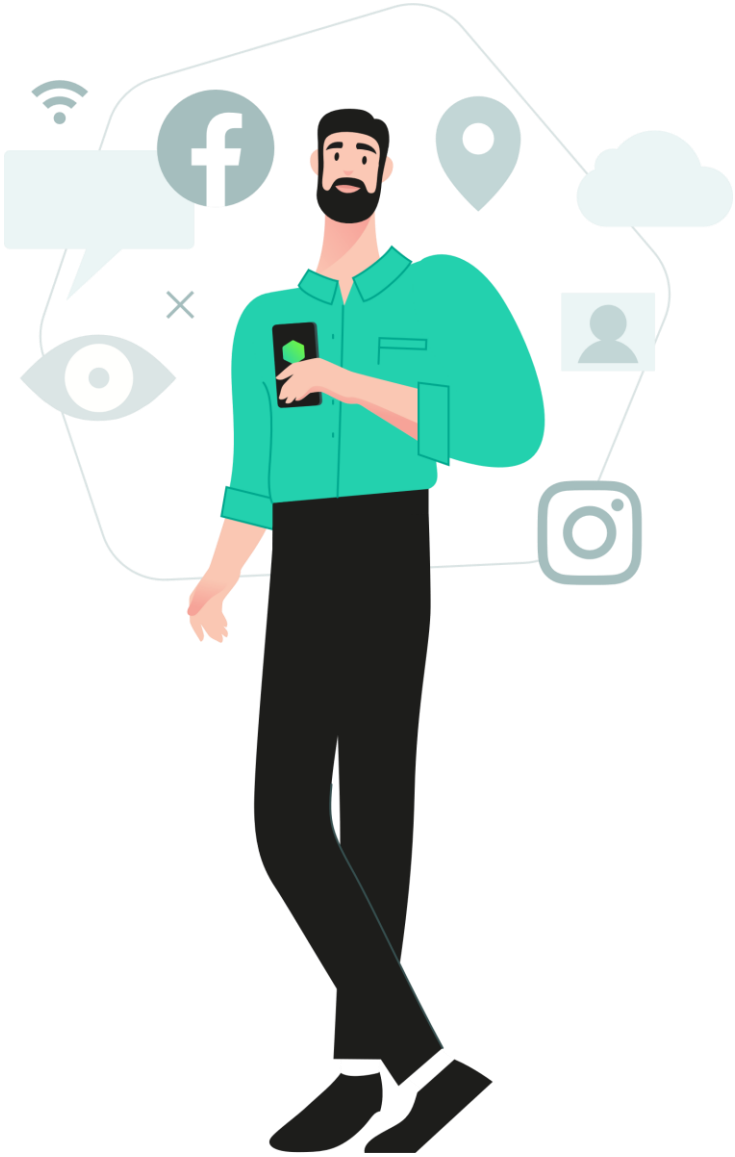
The Happn app has additional features: it shows, how many times and where you crossed paths with other users

- Easy to find those around you
- Using a mock location app, it is possible to find people who live/work in a specific location



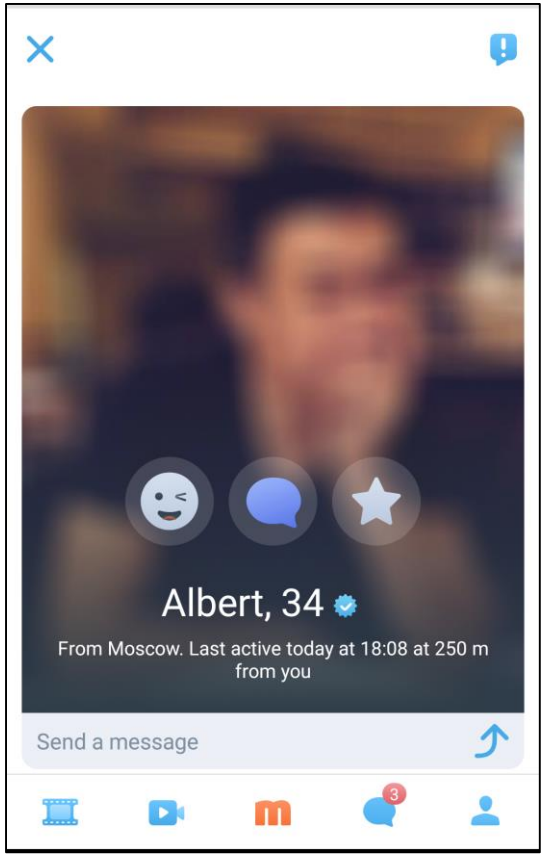
Revealing user's real name

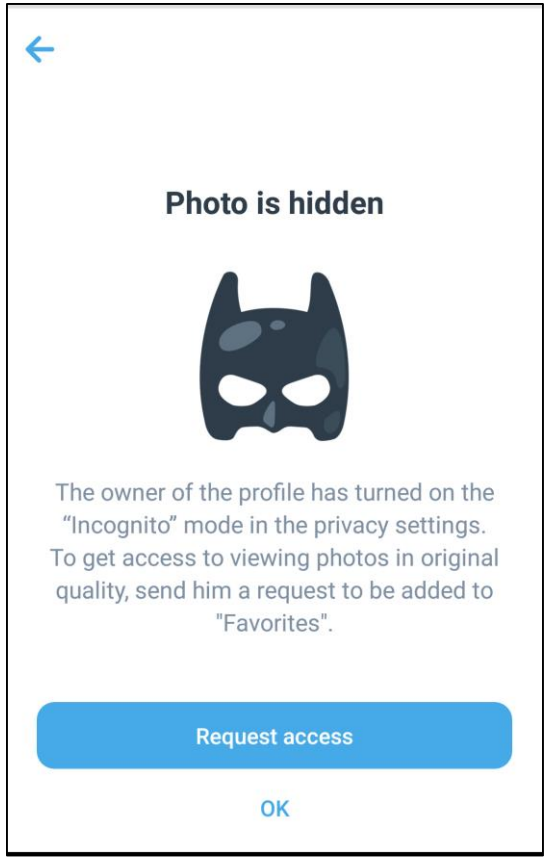
- No app asks for last name, but the first name is often taken from Facebook
- Profile pictures are often taken from Facebook by default
- Some apps ask to fill in information about school, work, etc.
- OkCupid asks a lot of personal questions
- Linking Instagram account makes it easier to identify the user
- Could lead to doxing



Unauthorized use of photos and chats

- Only Mamba has a free possibility to blur the photo
- Several apps have it as a paid option
- Pure is the only app that can be used without providing the photo
- Pure is the only app that prevents the user from making screenshots of chats
- Screenshots of users' profile and chats could lead to blackmail and doxing





Encrypted protocols

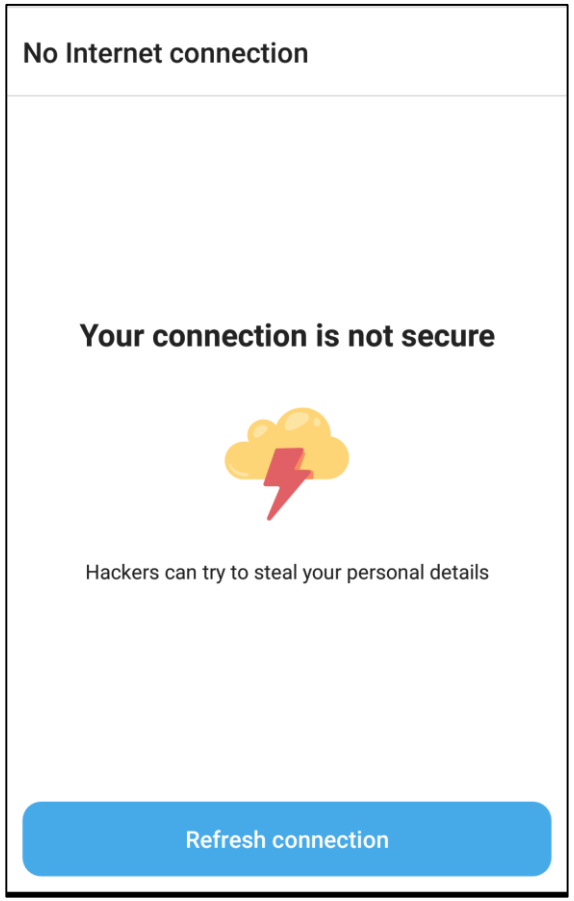
Much safer than 3 years ago:

- No HTTP
- Certificate pinning

(Almost) no ability to intercept traffic from another device

Encrypted protocols

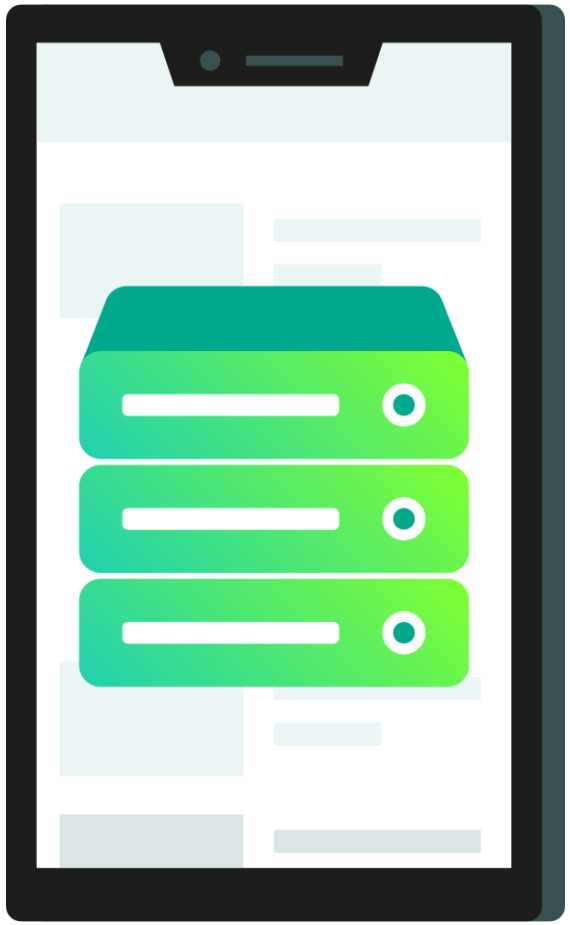
- When an invalid certificate is used, Mamba warns the user that traffic could be intercepted
- Other apps show that there is no Internet connection
- Data is not sent if the protocol is not secure



Data stored on the device

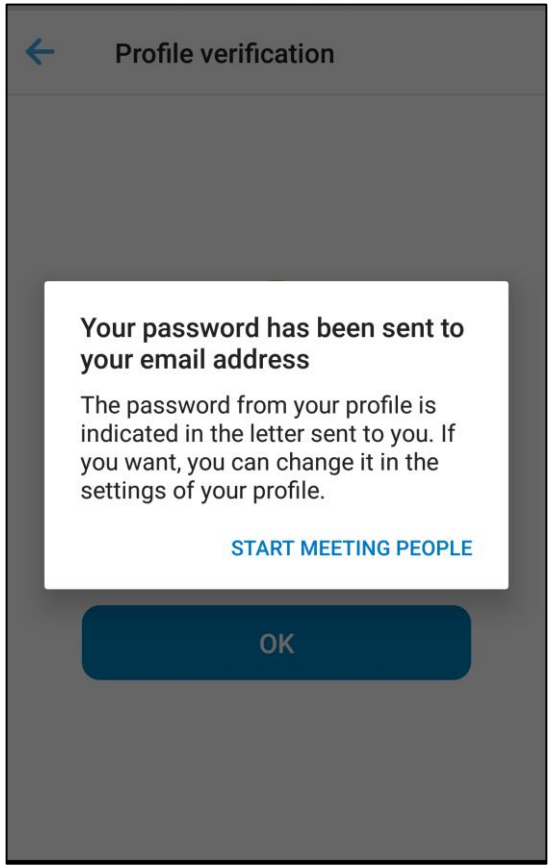
- Most of apps store messages and cached photos on the device
- Attacker with root access can obtain this data

Tricky but possible to read chats if the attacker has physical access to the device or the device is infected with some malware



Plain-text passwords

- Mamba and Badoo send password as plain text to the registered email address
- Without two-factor authentication, an attacker that gained access to the inbox or intercepted this email can get access to the user's profile



Vulnerability Disclosure & Bug Bounty

- Badoo and Bumble participate in the HackerOne bug bounty program
- Tinder, OkCupid and Mamba have their own programs

Launching a bug bounty or vulnerability disclosure program does not always result in better security, but is an important step for organizations

Summary

On the technical side, dating apps have gotten better in terms of security

There are still things that could be improved

The user still should think about privacy to stay safe

Many privacy features are available with subscription, not in free versions

Tips for users

Do not share too much personal information (last name, employer, photos with friends, political views, etc.)

Select your location manually, if possible

Delete or hide your profile if you no longer use dating apps

Do not tie other social media accounts to your profile

Use 2FA, if possible

It's important to regularly check if your privacy is secured.

To do that visit our page ->

Future of dating apps

Possible development vectors

- Possibility to hide photos & GPS location
- Disabling screenshots of profiles & messages
- Setting chats to be deleted automatically
- Informing users of the risks of sharing too much personal information

- Verified accounts
- Algorithms predicting a match based on users' personal information
- AI will protect users from fraud, and sensitive and abusive content

Thank you!

kaspersky