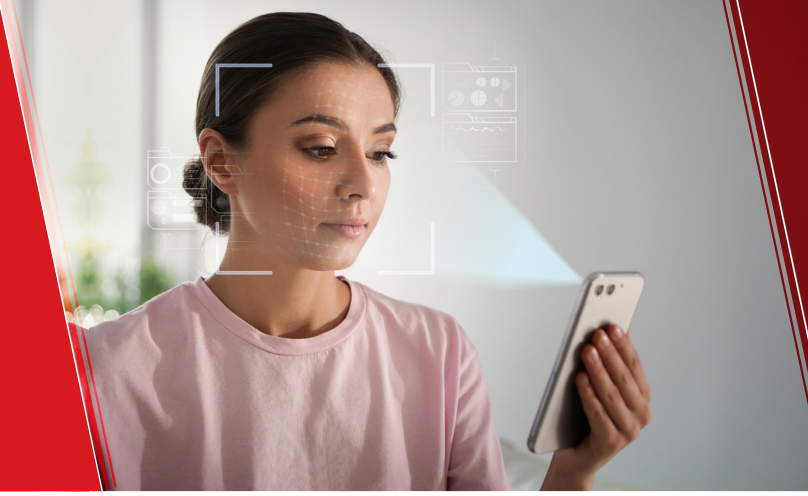
# LEAKED TODAY, EXPLOITED FOR LIFE

## How Social Media Biometric Patterns Affect Your Future



Today, different kinds of content are published in billions of social media posts, messaging networks, news outlets, and corporate and government portals. This content exposes a concerning number of biometric patterns. High-quality posts can contain face, voice, iris, palm, and fingerprint patterns that are susceptible for use in cyberattacks. Exposure of this kind applies to most social media users — even people who do not post themselves but are seen on social media. High-profile individuals are particularly at risk.

Some groups champion biometric authentication as a replacement for passwords because of its ease of use. People's biometric features can be used for identification and authentication. Unlike passwords, these features cannot be easily changed. We discuss the compromise of these features, how they can leave a lasting impact on our lives, and the key risks caused by biometric features already being unintentionally exposed on social media at scale.

## Key Findings

- Millions of biometric patterns with high-quality resolution were found exposed and searchable on major networks and platforms. The exposure rate is higher among public figures.
- Unintentional exposure can be very damaging. Many users are unaware that their posts expose their biometrics.
- Cybercriminals can abuse exposed biometric data to attack the reputation of C-level executives, political figures, and celebrities. They can also use such data to bypass authentication, produce deepfakes, or extort a victim.
- Malicious actors can also use such data to track people and their habits, commit digital identity theft, abuse social scoring systems, and trick law enforcement into believing that an individual was at a critical event.
- Biometric features cannot be changed like a password, so if stolen today, they can be weaponized for as long as 10 years from now.

## Security Suggestions

- Be aware of the major biometric data at risk: face, voice, fingerprint, palm, iris, and ear patterns.
- Minimize unintended exposure of high-quality media images that include sensitive biometric features.
- For authentication, prioritize the use of biometric patterns that are less exposed and use multifactor authentication (MFA) when possible.
- To address the problem at scale, significant policy changes should consider current and future circumstances, as well as address the use of current and previously exposed biometric data.

Read our full paper at
https://research.trendmicro.com/smbiometric.

TREND MICRO™ | research