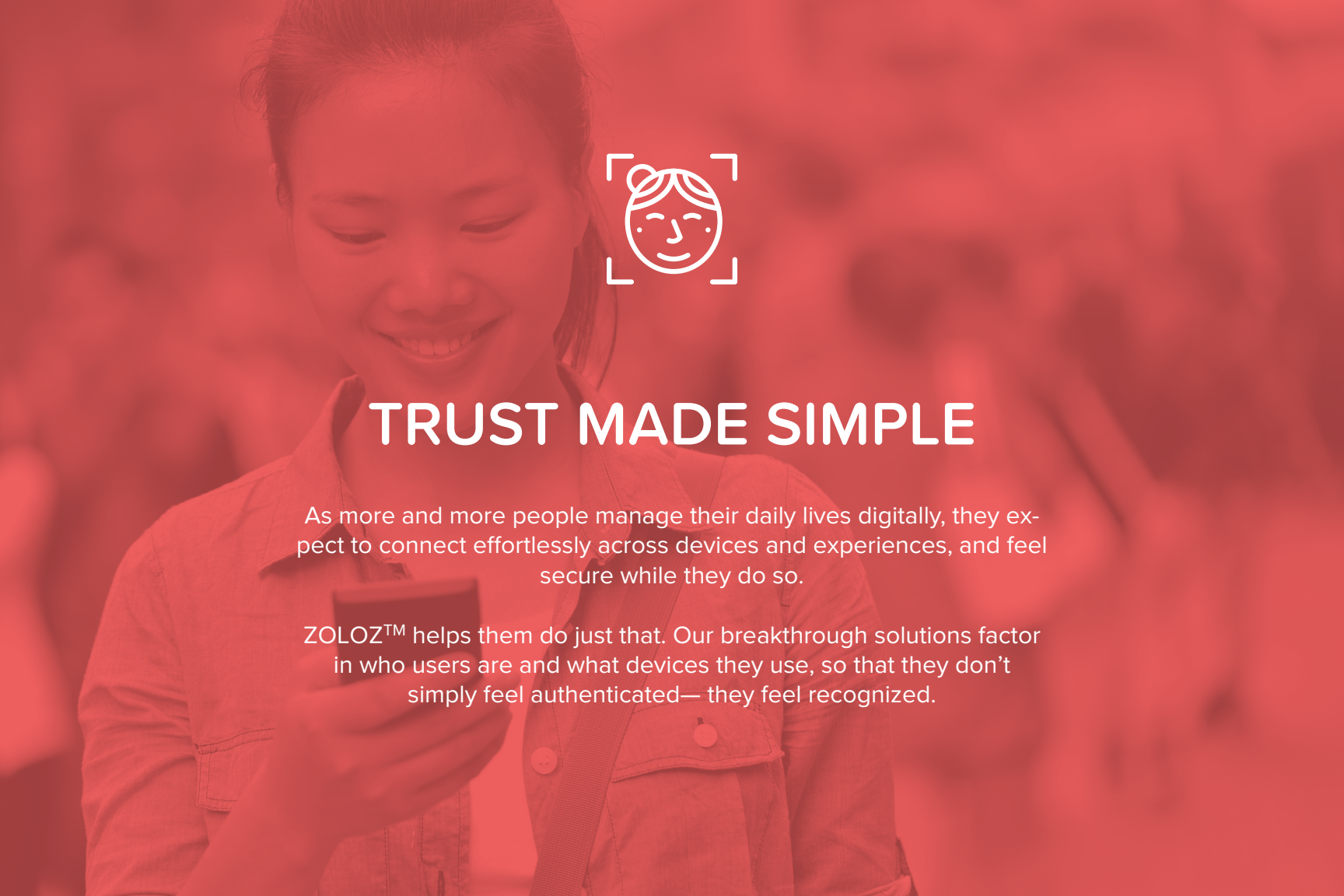
DETECTING HUMANITY IN DIGITAL IDENTITY:

THE FUTURE OF BIOMETRIC FRAUD PREVENTION

sales@zoloz.com / +1-913-608-9257

1740 Main Street, Ste. 100, Kansas City, MO 64108



TRUST MADE SIMPLE

As more and more people manage their daily lives digitally, they expect to connect effortlessly across devices and experiences, and feel secure while they do so.

ZOLOZ™ helps them do just that. Our breakthrough solutions factor in who users are and what devices they use, so that they don't simply feel authenticated— they feel recognized.

01 IDENTIFIERS EVERYWHERE

Faces found on Facebook. Voices caught on video. Fingerprints left on coffee cups. Biometric identifiers fill our world – and with time and know-how, hackers can collect them.

In this era of high-profile breaches, many fear the theft of their biometric data, which is permanent, unlike a password or PIN. ZOLOZ technology uses financial grade security and infrastructure to protect those templates — and now we're amplifying our efforts to stop fraudsters by strengthening "liveness."

WHAT IS A SPOOF ATTACK?

A spoof attack is an attempt to access a protected account using a fake biometric representation of the authorized user. Here are just a few spoofing methods:

Ocular or facial recognition: High-resolution photos and videos

Fingerprint recognition: Molded gelatin, transparencies, and etched circuit boards[1]

Voice recognition: Recordings and software-aided modulation

A spoof attack differs from an imposter attack, in which an attacker tries to gain access through normal procedures – for example, placing his own fingerprint on a scanner. (These are often called "zero-effort" attempts.)

02 LOOKING ALIVE

Liveness, sometimes called “spoof detection,” encompasses the techniques authenticators use to determine if false biometric input — a “spoof” – is being used to hack into an account. And as biometric authentication becomes widely adopted, spoofs make news (see the sidebar on page 6).

These events illustrate a well-known cyber-security trend: As technologies advance, so do the capabilities of criminals. Pocket-sized devices can capture HD and 4K video. Smartphone cameras and displays improve resolution with every release. Even high-quality photos from social media can now pose issues.

Multilayered spoof attacks increase the security challenge: In the physical layer, hackers present fake samples to the sensor itself; in the digital layer, they bypass sensors entirely, directly feeding digital misinformation to trick the authentication algorithms.

03 TALKING REAL

A more fundamental biometric challenge involves perception. While mobile phones may have a host of sensors — accelerometers, gyroscopes, fingerprint scanners, and more — each can only access one type of information. Without context, it is easy to misinterpret the information being collected.

For example, audio of someone talking can seem legitimate, as can a muted video of that person talking. But if the audio and video don't match, something's wrong.

Alone, sensors can't incorporate complex combinations of signals that humans would use to determine fakery, such as movement, environment, and physical characteristics. But advanced algorithms can detect those signs of life (or evidence of a spoof attack) by using a phone's native sensors to combine individual signals, creating a more complex picture.

04 POSING A CHALLENGE

One approach to determining liveness is “challenge response.” For instance, a facial scanner may ask for a user to blink – an action impossible for a static photo. Fraudsters, though, can toggle between a photo and a copy manipulated to make eyes appear closed, craftily simulating a blink.

Challenge-response techniques, in addition to being easy to predict and trick, can annoy and embarrass users. (Who wants to make faces on the train just to log in to a bank account?)

Consumers are not a captive audience. If posed with an unpalatable challenge, they may choose another solution or, worse yet, opt out of much-needed security measures.

Passive, non-challenge response that doesn’t require specific user actions is the goal: Give spoof detection the context it needs without exposing software (or user) vulnerabilities.

05 OUR APPROACH

PASSIVE LIVENESS: Our groundbreaking methods and algorithms collect and process user reactions and environmental cues during authentication, making normal interaction with the software enough to seamlessly distinguish a real person from a spoof.

LIVENESS DECISION ENGINE: A decision engine, much like the risk engines used by credit card companies, picks the most relevant algorithms from a verification event, aggregating the liveness data into a decision that's highly effective against photo- and video-based attacks.

06 FACING THE FUTURE

Without an effortless experience, people may avoid connecting their physical and digital identities, instead relying on familiar but frustrating and fallible password technology.

They and the companies that serve them can pay a price. Today, sophisticated attacks on individuals are unlikely but possible. And for business accounts, the risk for attackers can be worth it.

We know that fraud will evolve, biometric imitations will improve, and spoof attacks of new varieties and increasing scale will be attempted. And at ZOLOZ, we'll be prepared.

Our seamless, easy-to-use biometric solutions will always put the most advanced liveness detection to work for you and your customers, so you can both stay ahead of cyber criminals.

SPOOFS IN THE NEWS

Only a month after Samsung released the S8 smartphone, a still photo fooled its facial scanner,[2] and Europe's largest hacker association, the Chaos Computer Club, spoofed its iris scanner through the creative use of a contact lens.[3] In May of 2017, non-identical twins spoofed HSBC's voice ID system.[4,5]

REFERENCES

[1] The Register, Gummi bears defeat fingerprint sensors, Leyden, John, 16 May 2002, https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/

[2] The Verge, The Galaxy S8's facial scanner can, unsurprisingly, be tricked with a photo, Ashley Carman, 31 March 2017, https://www.theverge.com/2017/3/31/15136226/samsung-galaxy-s8-face-scan-security

[3] Mashable, These guys have already cracked the Galaxy S8's iris scanner, Raymond Wong, 23 May 2017, http://mashable.com/2017/05/23/samsung-galaxy-s8-iris-scanner-hacked/#LmBkUjEe8mqB

[4] The Telegraph, HSBC's voice recognition security breached by customer's brother, Laura Suter, 19 May 2017, http://www.telegraph.co.uk/personal-banking/current-accounts/hsbcs-voice-recognition-security-breached-customers-brother/

[5] BBC News, BBC fools HSBC voice recognition security system, Dan Simmons, 19 May 2017, http://www.bbc.com/news/technology-39965545

CONTACT US

sales@zoloz.com
+1-913-608-9257

1740 Main Street, Ste. 100
Kansas City, MO 64108
United States

ZOLOZ
1740 Main Street, Ste. 100
Kansas City, MO 64108
United States