

2024 - LIVENESS DETECTION SECURITY REPORT

Knowledge-Based Authenticators (KBA), such as passwords, PINs, emails, and codes sent to phones, attempt to prove that the person requesting access is the correct user, but they don't verify or reverify the user's identity. With PII breached and one-time-passwords consistently worked around, KBA remains ineffective at proving the correct user is actually physically present and opens doors for fraudsters.

Today, victims of social engineering attacks phishing, where fraudsters steal an individual's credentials, may only have slipped up once for their digital lives to be taken over by the attacker.

Biometric matching is now replacing legacy KBA in unsupervised authentication scenarios and is serving as a strong verifier of the correct user's unique biology. However, it is not enough to verify biometric data matches, as that data can be collected, stored, and then reused in most cases. To prevent such abuse, the new biometric data sample must be confirmed to be a first-generation capture from a living, 3D user just moments before it is matched to trusted enrolled data.

FaceTec's 2024 Liveness Security Status:

- Tripled the [Spoof Bounty program to \\$600,000](#), originally started in October 2019
- Now performing over [2,6000,000,000 3D Liveness Checks](#) annually with no fraud reported
- Passed NIST-accredited Bixelab PAD Testing in June 2023: [Level 2 with 0% FAR](#)
- Passed iBeta Level 1 & 2 PAD Certifications over four years ago
- Passed extensive 14 day Video Injection Penetration Tests by European biometrics lab
- Over 100 Channel Partners have tested and chosen to resell FaceTec's 3D Liveness AI




"Liveness Detection" provides confirmation that the user is a real, 3D, physical human. FaceTec is a pioneer in Liveness Detection (more specifically, 3D Liveness Detection) and, for the past nine years, has developed and deployed a user-friendly, yet exceptionally secure Liveness AI, delivering the most accurate 3D face matching for smartphones and web browsers available.

2D liveness detection isn't sufficiently accurate for remote user verification, and not all Liveness software can stop attackers, even low-skilled ones. In fact, [most cannot](#) and are merely a nuisance for fraudsters to work around. Relying only on outdated testing criteria, such as iBeta & ISO 30107-3, creates a false sense of security. Attack vectors have evolved so quickly that standards released in 2017 were rendered obsolete within just a few years. ISO 30107-3 and iBeta tests do not include new attack vectors such as digital deepfakes or video injection, two of the most scalable attack vectors.

To ensure real-world security in the face of emerging attack vectors, [FaceTec's \\$600,000 Spoof Bounty Program](#) has opened up the Liveness AI to global attackers 24/7, 365. Open access invites potential fraudsters to try to use their best tactics to bypass FaceTec's Liveness Detection. The ability to block these attacks provides up-to-the-minute proof that FaceTec's AI can defend against all known Level 1-5

Attacks. No other Liveness vendor in the world has AI capable of supporting such a program.

\$600,000 Spoof Bounty Program Details:

Threat	Description	Example	Bounty
Level 1	Hi-res paper & digital photos, hi-def videos exhibiting challenge/response and human-worn paper masks.		Browser, iOS, & Android: \$30,000 \$90,000 Total
Level 2	Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD\$300 in price.		Browser, iOS, & Android: \$30,000 \$90,000 Total
Level 3	Custom-made ultra-realistic 3D masks, sculptures, wax heads, etc. up to USD\$3,000 in creation costs.		Browser, iOS, & Android: \$40,000 \$120,000 Total
Level 4	Successfully decrypt & edit the contents of a 3D FaceScan to contain synthetic data not collected from the session, have the Server SDK process it and respond with Liveness Success.	<u>3D FaceScan Tampering</u>	Browser, iOS, & Android: \$60,000 \$180,000 Total
Level 5	Successfully take over the camera feed & inject previously captured frames that result in the Server SDK responding with Liveness Success.	<u>ManyCam</u> <u>Vcam</u> <u>vlc2Cam</u> <u>FakeWebcam</u>	Browser, iOS, & Android: \$40,000 \$120,000 Total

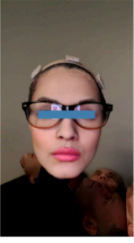



More info at www.SpoofBounty.com & dev.facetec.com/spoof-bounty-program

Bounties Payouts by Level & Attacks on the Bounty Program broken out by Level:

Attack Level	Browser	Android	iOS	Attacks	Bounties Paid	Attack Notes
Level 1	\$30,000	\$30,000	\$30,000	> 88,000	2*	PAD Paper & Digital Photos, Videos, 2D Masks
Level 2	\$30,000	\$30,000	\$30,000	> 2,000	-	3D Masks, Under \$300
Level 3	\$40,000	\$40,000	\$40,000	> 1,000	-	Hollywood Masks, <u>Madame Tussauds Wax</u> , etc.
Level 4	\$60,000	\$60,000	\$60,000	~ 5,000*	-	* ~5,000 est., but we cannot determine offline attempts to crack an already-encrypted 3D FaceScan
Level 5	\$40,000	\$40,000	\$40,000	> 14,000	-	<u>Virtual-Cam</u> & Video Injection attacks, set breakpoints and fail to pass Liveness

* Two Level 1 PAD bounties were claimed in mid-2020. These attacks both used high quality video with slight blurs applied. The bounties were paid and the vulnerability was patched. There are no known vulnerabilities at this time.

Rebuffed attacks with 2D & 3D artifacts:

<p>Type: 3D Liveness Request</p> <p>Liveness: Not Proven</p> <p>🕒 8/12/24 at 5:03:32am PST</p> <p>📱 FaceTec Android App</p> <p>📱 Android 9.7.29 (SM-G998B)</p> <p>📍 San Diego, CA</p> <p>💰 000.00.000.000 SV ADMIN</p> <p>✉ qatester@facetec.com</p> <p>🔗 fuEeAHSe0PHLpGKu5UfLHWYgXg9EEIsn SV1</p>		<p>Type: 3D Liveness Request</p> <p>Liveness: Not Proven</p> <p>🕒 8/29/24 at 8:22:31pm PST</p> <p>📱 FaceTec Browser App</p> <p>📱 Browser 9.7.29 (Windows NT 10.0)</p> <p>📍 San Diego, CA</p> <p>💰 000.00.000.000 SV ADMIN</p> <p>✉ qatester@facetec.com</p> <p>🔗 ttV302QbdKj8bBL5UA03uTjdMBFD5jho SV1</p>	
<p>Type: 3D Liveness Request</p> <p>Liveness: Not Proven</p> <p>🕒 8/30/24 at 7:14:03am PST</p> <p>📱 FaceTec Android App</p> <p>📱 Android 9.7.30 (SM-S901U1)</p> <p>📍 San Diego, CA</p> <p>💰 000.00.000.000 SV ADMIN</p> <p>✉ qatester@facetec.com</p> <p>🔗 fj6sQcE17HVX2oMaxumeL4nwBt10PZlj SV1</p>		<p>Type: 3D Liveness Request</p> <p>Liveness: Not Proven</p> <p>🕒 8/29/24 at 9:13:13pm PST</p> <p>📱 FaceTec iOS App</p> <p>📱 iOS 9.7.30 (iPhone14,5)</p> <p>📍 San Diego, CA</p> <p>💰 000.00.000.000 SV ADMIN</p> <p>✉ qatester@facetec.com</p> <p>🔗 mSdlj47LjCuyCiuV3GARHmR98j1HikFH SV1</p>	

FaceTec's 3D Liveness proves to a very high level of confidence (+99.999%) that the physical user is present and the camera feed is not being tampered with. This is done by determining that the app is not running on an emulator, a virtual camera is not being used, and a camera hardware adapter bypass is not being attempted. Over the last two years, the FaceTec Spoof Bounty Program has rebuffed over 150,000 attacks, providing FaceTec with the data to closely examine the real-world attacks our software must defend against.

The Spoof Bounty Program incentivizes attackers to employ their most effective methods to claim the bounty. All attacks are analyzed, and if a new potential spoof method is identified, the proper steps to mitigate the threat are taken immediately. This means that new threats are patched before they can be exploited by fraudsters in real-world applications. Security is about staying ahead of bad actors, and FaceTec is the only company that pays creative white-hat attackers to help uncover potential vulnerabilities *before* they can be maliciously used for actual fraud.

Many Liveness vendors cite outdated third-party testing conformances to get credibility, preferring lowest common denominator standards and methods that provide a false sense of security, rather than actively and successfully addressing attacks from deepfakes and video injection. The primary reason FaceTec's competitors do not provide spoof bounty programs is their AI would not be able to rebuff any sophisticated attacks and be quickly compromised, which would result in massive bounty payouts.

The European Union Agency for Cybersecurity's (ENISA) 2024 [Remote Identity Proofing - Attacks & Countermeasures](#) report discusses the most recent threat vectors, highlighting the need for 3D data to be used in the Liveness assessment, as well as explains how spoof bounty programs are currently the most effective way to test known and unknown threats.

FaceTec Internal Security Self-Assessment

Over the last nine years, FaceTec's internal "Red Team" has attacked the FaceTec Liveness AI in hundreds of different ways and with 10's-of-millions of attacks. Over these years and the millions of attacks, FaceTec has trained its AI to detect and reject attacks of all types.

These internal attacks are over and above the attacks from the iBeta Level 1 & 2 testing (total of 3,300+), the Bixelab Level 2 PAD Testing (1,200) and 150,000+ attacks on the Spoof Bounty Program.

About FaceTec's 3D Liveness Detection AI

A user performs a 3D FaceScan™, which is the result of real-time processing on the video selfie. The 3D FaceScan is encrypted and sent to the organization running the FaceTec Server SDK. When the user's Liveness is deemed "true" by the AI, a 3D FaceMap™ (~170kb) is created, and the 3D FaceScan (and its Liveness data) can be deleted. In the future, the 3D FaceMap can be used to perform the most accurate face matching against 2D user photos that are on file, as a photo ID or in an NFC chip.

The 3D FaceScan (~350KB) is an encrypted byte blob that contains 3D data from 100-plus video frames captured during the two-second user selfie. 3D FaceScans are always encrypted during transit and storage and are not human viewable. 3D FaceScans *do* contain Liveness data, but after Liveness is proven, the derivative, as 3D FaceMap (~180kb) is stored for future matching. 3D FaceMaps do *not* contain Liveness data, and don't need it because new Liveness data is always recollected and processed, prior to matching every time there is a new access request.

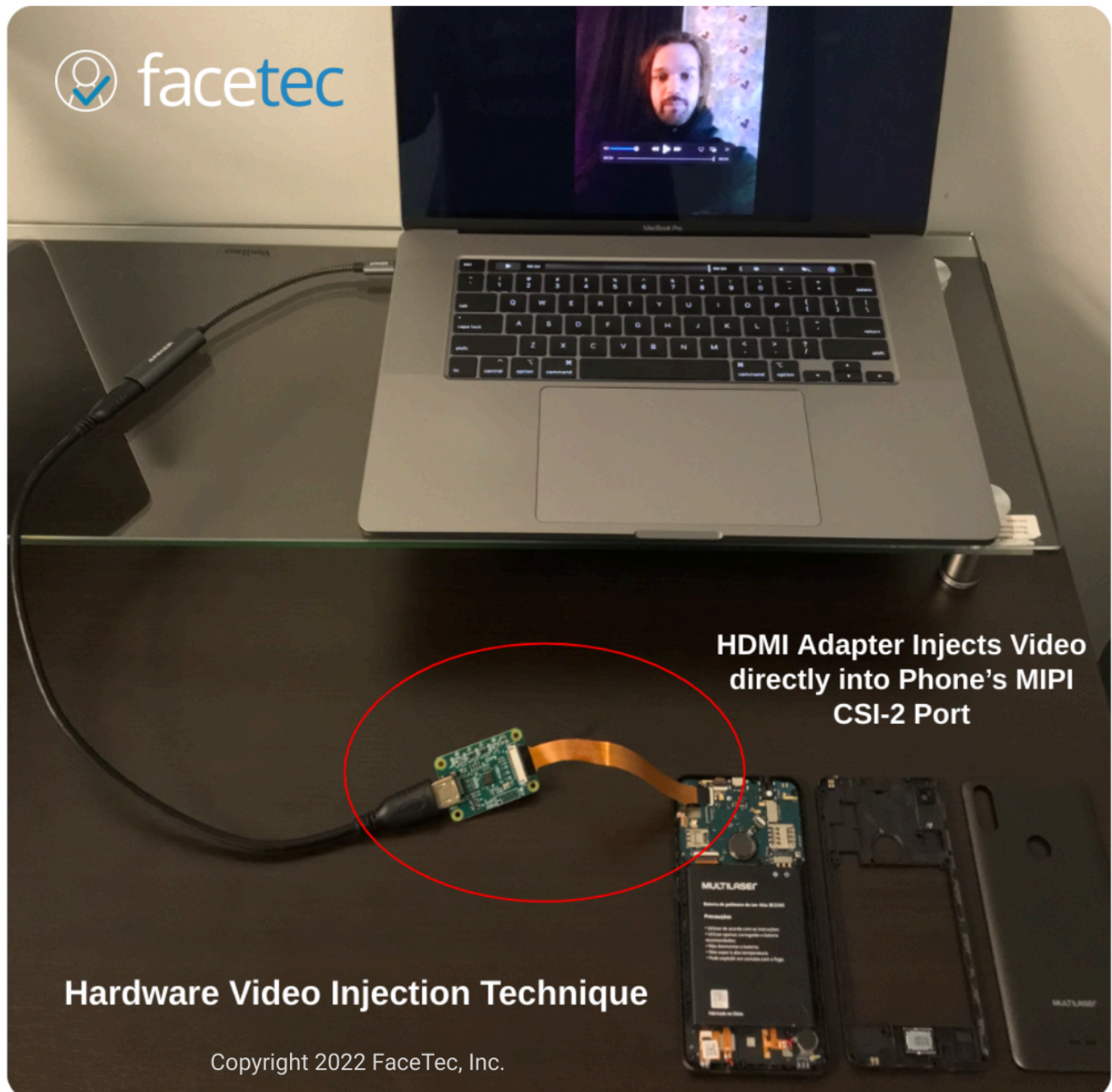
FaceTec now performs over 2,600,000,000 3D Liveness Checks annually with no fraud reports.

Understanding Video Injection Threat Vectors

There are two types of video injection attacks that can defeat most Liveness Detection systems, either software or hardware-based.

The software-based attack vector uses breakpoints in the Device SDK code or a virtual camera program to fool the system into thinking it is seeing data that was collected from a real camera. In 2022 FaceTec underwent over 14 days of video injection attack/penetration testing by a European biometrics testing lab. **The results:** the lab was unable to inject any video into FaceTec's UI without being caught even after nearly a thousand attempts using the latest video injection and hooking techniques.

Hardware video injection attacks use adapters to connect to the camera port of a device, and then video is played from another device. This simulates live video that is captured by a physical camera, but it is just receiving the incoming recorded video or synthetic deepfake video feed.



Resources

Educational Wiki-style site - www.Liveness.com

European Union Agency for Cybersecurity - [Identity Proofing Guidelines](#)

NIST 800-63 RFI - [Liveness Security Report Letter](#)

Deepfake vs. 2D Liveness Paper - [Seeing is Living?](#)

Deepfake Spoof Article - [Unite.ai](#)

Properties of 3D FaceScans & 3D FaceMaps:

- **Encrypted:** This is required and enforced by the FaceTec SDK APIs.
- **Proprietary:** 3D FaceMaps cannot be used by anything other than the FaceTec Server SDK.
- **Created via a patented process:** Users performing user sessions from any device are using FaceTec's patented interface to create 3D FaceMaps.
- **Cross-platform:** FaceMaps from iOS, Android, or Browser can be used interchangeably.
- **Data-rich:** FaceTec 3D FaceMaps are created by processing (in most cases) upwards of 100 frames of data from the raw camera data.
- **Future-proof & forward-compatible:** All FaceTec 3D FaceMaps are guaranteed to be compatible with all future FaceTec Matching Algorithm improvements.
- **No Honeypot Risk:** The 3D Liveness data used for Liveness Detection is deleted from 3D FaceScans after the session is processed; 3D FaceMaps do not contain Liveness data.
- **Flexible:** FaceTec 3D FaceMaps can be stored as files, in databases, in blocks, on a server, or on a device. Customer-specific encryption schemes can be applied in addition to FaceTec SDK built-in security mechanisms.