VONAGE

Verify is a simple API with:

- Instant global reach.
- Zero telco or 2FA experience required.
- High deliverability with Adaptive Routing
- SMS or voice selection and seamless intelligent failover
- Customization to local preferences such as watermarks in China and whitelisting in India

VIDEO INTERACTIONS ARE VULNERABLE

Protect your Video Conversations with the Vonage Verify API

With the rise of remote work and video conferencing—high quality and consistent connections are crucial, but it is also important to think about account security. Online threats are on the rise and costly:

Online fraud is expected to grow to **$48 BN in 2023 at 30%** according to Juniper Research.

Every dollar of fraud costs businesses 3X more in chargeback, insurance, replacement, and operational costs.

The Case for 2-Factor Authentication with Video

The growing use of video conferencing for doctor visits, online classes, and remote work creates new hot spots for fraud. Therefore, ensuring that the intended people are participating in a video call is paramount. Username and password are the first lines of defense—but they shouldn't be the only ones. Layering security with 2-factor authentication with options for text-to-speech verification and multiple languages helps better protect customers.

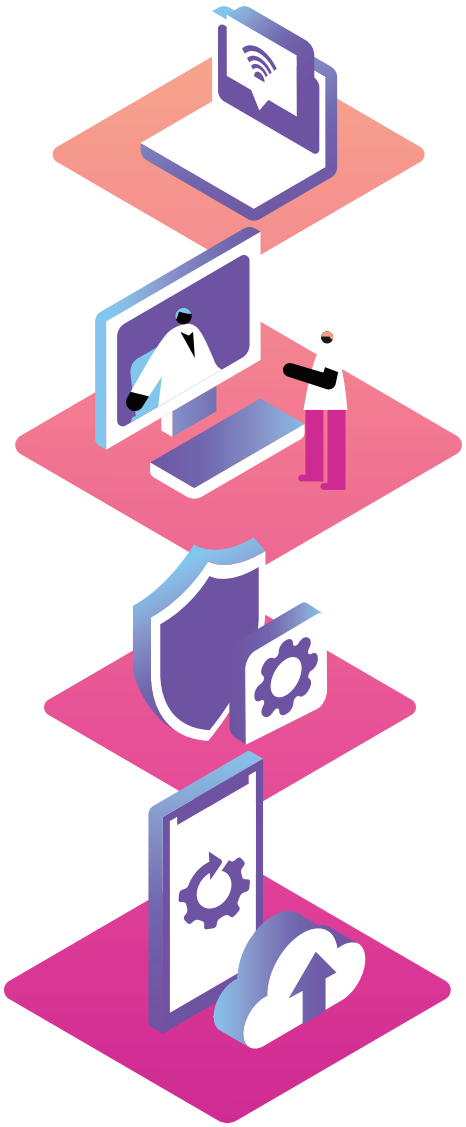
Authenticating users should come first before engaging with customers. 2-factor verification is an easy way to secure video conversations in various use-cases for different environments.

Vital Use Cases for User Verification to Secure Video Conferencing:

Telemedicine: There is an increase in doctors and healthcare practitioners serving patients remotely. HIPAA-compliant video conferencing has empowered doctors to continue with care via mobile, tablet, or laptop. Healthcare is one of the hardest-hit industries for privacy and data breaches. **75% of healthcare organizations have experienced cyber-attacks and data breaches.**

✓ *Adding 2-factor authentication is an easy way to add a layer of security that prevents fraudulent transactions, account takeovers, and other vulnerabilities.*

VONAGE



Remote work: Employees working remotely use group video meetings, private video calls, video-collaboration tools. Companies everywhere are therefore more susceptible to enormous risk, especially if administrative controls and mandatory authentication are not implemented. You'll want to ensure your employees can authenticate even in the event that someone loses, damages, or upgrades their phone.

✓ *Using 2FA enables accounts to sync across laptops, desktop, and mobile devices to provide multiple device security.*

Education: Online and distance learning has become more relevant than ever in this health crisis. It has also drawn the attention of digital hijackers, troublemakers who hijack video calls to stream hate speech and offensive content—known as "Zoombombing". Educators need stronger online security in their digital classrooms.

✓ *Enabling SMS and voice-based 2FA helps secures online classes and is applicable to adult students and parents of younger students who can validate their identity by entering a time-based one-time password to access classes.*

Banking: Banking has always been targeted by fraudsters. With bank visits and financial advisor visits being replaced by video conversations, online security is even more important.

✓ *Use two-factor verification to validate every user with encrypted video consultations to work with customers. SMS verification is easy to implement, widely available and understood by most end users.*

Fitness and entertainment: As gym and fitness studios are closed, they are looking to live-stream online video classes to stay engaged with customers. Sessions are usually shared by sending members a video URL via email. But what if someone shares that link with non-members? Premium content can now be accessed without payment. In the economy today, every bit of income counts. The same goes for limited-access live showings, talks, and tours. This new normal of video showings need to be protected.

✓ *With a few lines of code, add a second factor to the verification process to ensure you are accepting logins from the right person and safeguarding your premium content.*

Getting started is simple!

Learn more and contact an expert at **vonage.com/verify**

Secure Valuable Video Conversations with Verify

Video collaboration and streaming has replaced in-person interactions and is here to stay. As sensitive information is shared, maintaining trust between users and platforms will be key. Adding 2-factor authentication is an easy way to prevent fraudulent transactions, hacks, and malicious activity.