iproov

The Threat of Deepfakes

The consumer view of deepfakes and the role of biometric authentication in protecting against their misuse.

What are deepfakes?

Deepfakes are videos, images or audio recordings that have been distorted to present an individual saying or doing something that they didn’t say or do.

If you think of the thing that you are least likely to ever say, and then imagine your friends, family or employer being shown a (convincing) video of you saying it, it is easy to see the potential for malicious misuse.

Deepfakes are created using artificial neural networks, which means that they can be produced increasingly easily to look authentic and convincing.

Although deepfakes have been used for social sharing and entertainment, they have also been employed in hoaxes, revenge porn, and increasingly, fraud and impersonation.

Both government and commercial enterprises have been called upon to address the threat of deepfakes, particularly with the US election in November 2020. Facebook announced in January 2020 that it would ban the use of deepfakes.

How do deepfakes affect consumers?

Consumers could be affected by deepfakes in a number of ways, including:

- Fake accounts could be set up on social networking sites to impersonate individuals and cause reputational damage.
- Existing accounts could be hacked using images or videos stolen from social network profiles to bypass authentication processes.
- Fake news can be shared and believed very quickly, to potentially devastating effect, if consumers see manipulated videos of someone they trust saying something.
- Employees can be tricked into divulging information or making payment transfers by criminals posing as their boss.
- Trust will disappear. Video evidence will become less trustworthy, leading to plausible deniability - “that wasn’t me, it’s a deepfake”.
- Identity theft can result in consumers being victim to fraudulent transactions if their credentials are used to apply for credit or purchases.

It is estimated that the associated costs of deepfake scams will exceed $250million in 2020.

iproov

How can you prevent deepfake fraud?

Both government and commercial enterprises have been called upon to address the threat of deepfakes.

iProov's biometric authentication technology enables organizations to protect themselves and their customers against deepfake fraud.

iProov was established in 2012 to solve the challenge: how can we trust that an online user is who they say they are? Banking, government services, healthcare, travel, legal services...all aspects of our lives are moving online. How do we ensure maximum security and reliability in a way that is easy for the user?

Genuine Presence Assurance

iProov is a world-leader in assuring the genuine presence of human beings online. Our unique patented Genuine Presence Assurance technology detects if a remote user is the right person (and not an imposter), a real person (and not a photo or mask), and authenticating right now (and not an injected deepfake replay attack). **Read more: www.iproov.com**

The iProov Security Operations Centre (iSOC)

Our global threat intelligence platform for biometric assurance uses machine learning technology, people and process to detect and block cyber attacks, including deepfakes. By learning from the attacks, iSOC helps prevents fraud, theft, money-laundering and other serious online crime today and tomorrow.

Summary of Findings

- **88%** of respondents believe online security threats are growing (88% US/88% UK)
- **Only 13%** know what a deepfake is (12% US/14% UK)
- **37%** think they could spot a deepfake (38% US/36% UK)
- **85%** agree deepfakes will make it harder to trust what they see online (86% US/84% UK)
- **75%** would use an online service that could prevent deepfakes (75% US/76% UK)
- **58%** agree that deepfakes are a growing concern (59% US/56% UK)
- **52%** worry most about deepfakes being used as part of identity theft for setting up bank accounts or acquiring credit cards (54% US/50% UK)
- **46%** worry about identity theft to steal from people they know (47% US/45% UK)
- **42%** think the financial services sector is at risk from deepfakes (42% in UK and US)
- **72%** believe authenticating identity is more important than ever (72% US/71% UK)
- **81%** believe biometrics will be used to assure identity online (82% US/81% UK)

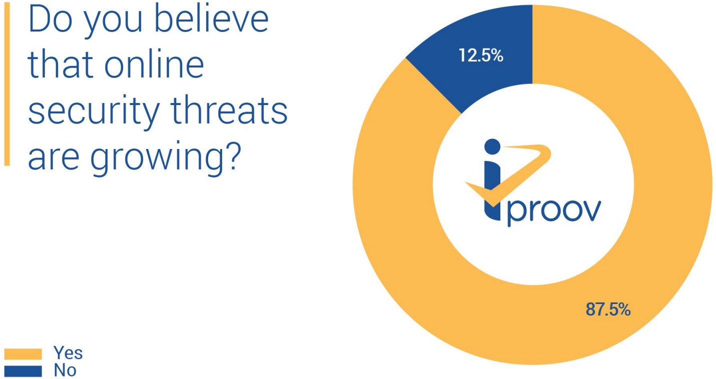
iproov

88% of consumers believe online security threats are growing

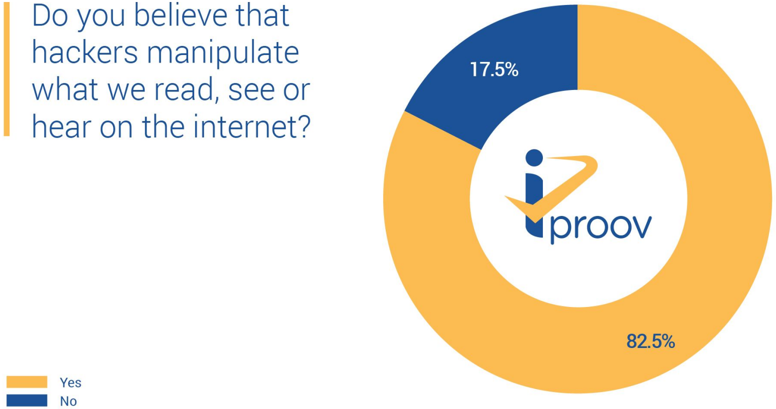
The vast majority of consumers believe that online security is being threatened:

- 97% of the 65+ age group believe online security threats are growing, compared with 81% of 18-24s.
- The US and UK are aligned: 88% in both countries believe online security threats are growing.

Do you believe that online security threats are growing?



Do you believe that hackers manipulate what we read, see or hear on the internet?

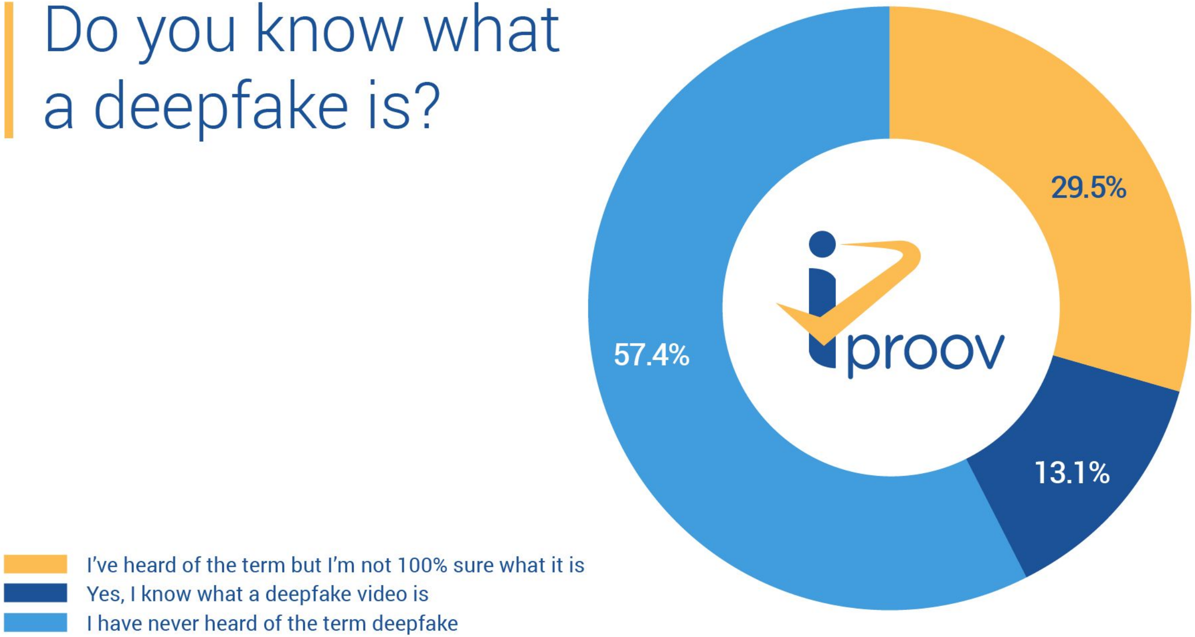


Only 13% of consumers know what a deepfake is

Consumer familiarity with deepfakes is limited:

- 57% have never heard the term deepfake.
- 30% have heard of deepfakes but aren't sure what they are.
- 68% of women say they have never heard the term, compared with 48% of men.

Do you know what a deepfake is?

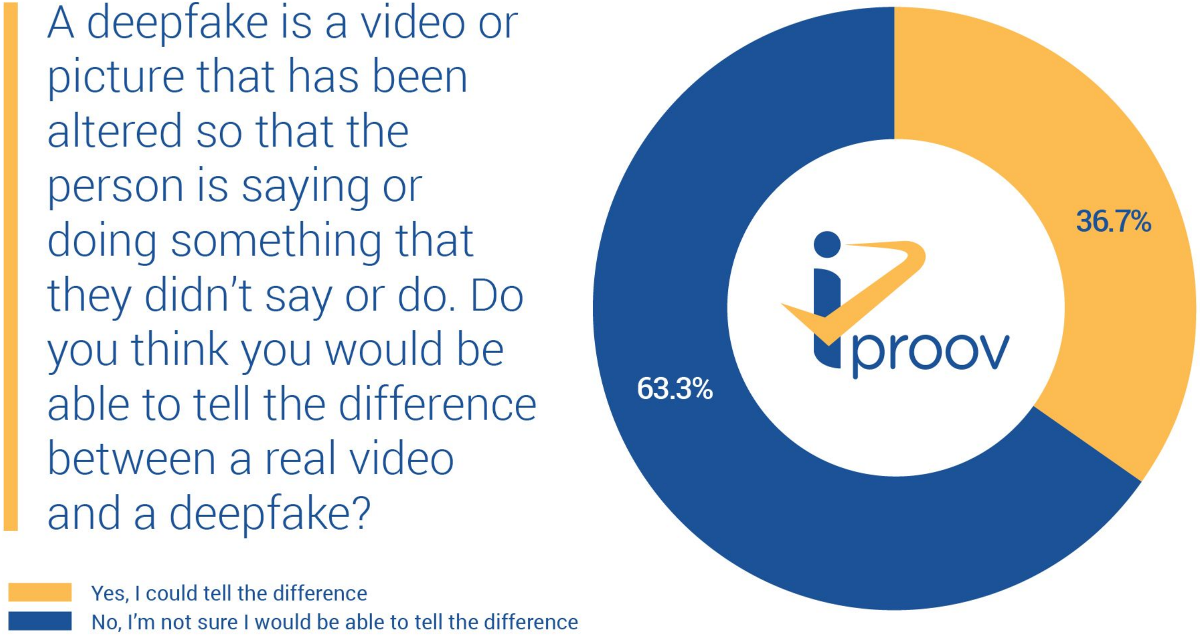


37% think they could spot a deepfake

Deepfakes are now so sophisticated that even the trained human eye cannot tell them apart. However:

- 37% of consumers think they could tell the difference.
- Men are 20% more confident than women that they could spot a deepfake video.
- The most confident age group in the UK was the 18-24 year olds (60%).

A deepfake is a video or picture that has been altered so that the person is saying or doing something that they didn't say or do. Do you think you would be able to tell the difference between a real video and a deepfake?

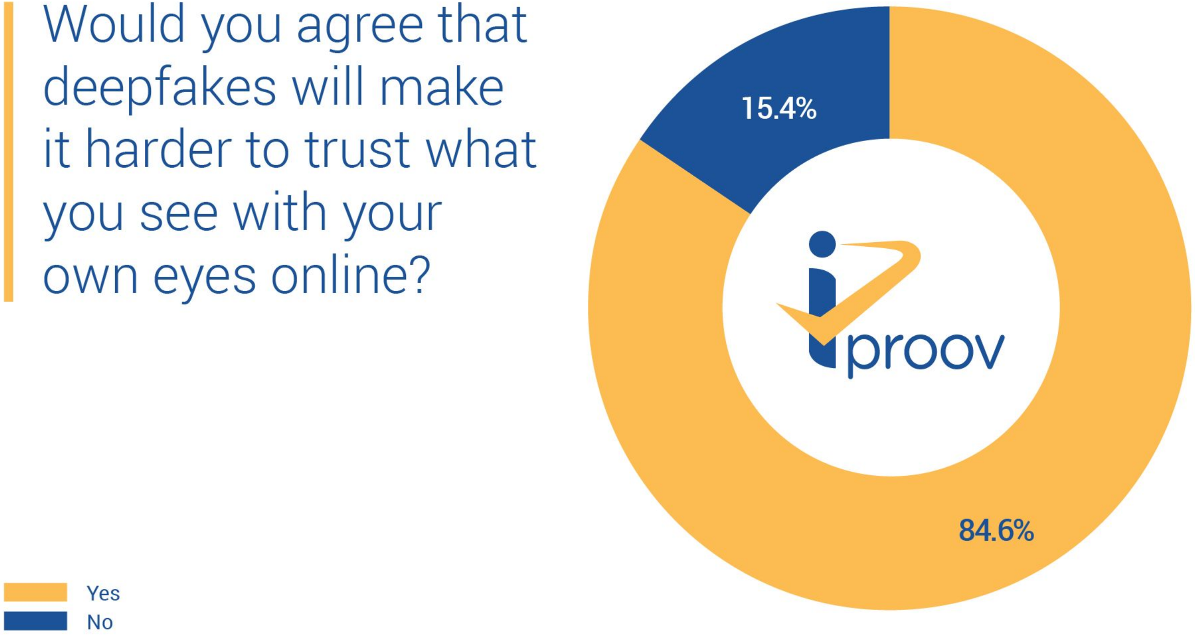


85% agree deepfakes will make it harder to trust what they see online

The vast majority of consumers think that deepfakes erode trust online:

- Older people would find it harder to trust what they see: 95% of the 65+ group say it would be a problem.
- 62% of consumers also said they had read, seen or heard something online that was fake.

Would you agree that deepfakes will make it harder to trust what you see with your own eyes online?

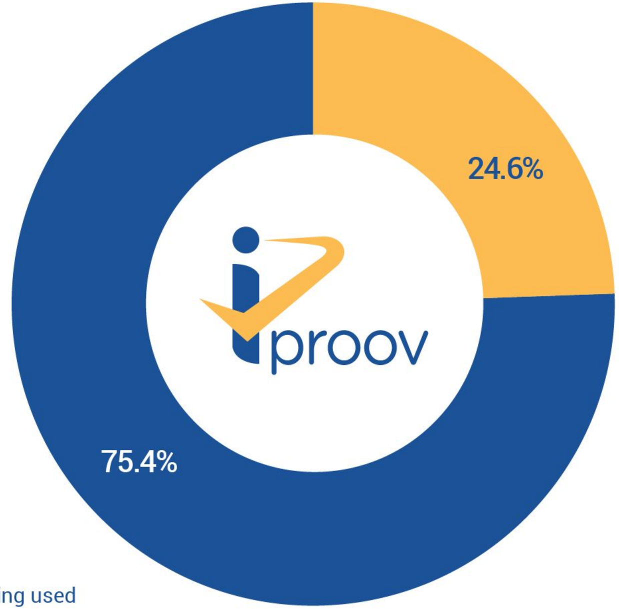


75% would be more likely to use an online service that could prevent deepfakes

The majority of consumers would choose an online service that offered deepfake protection:

- Only 25% said it wouldn't make a difference to them when choosing an online service.

Would you be more likely to use an online service that had measures in place to prevent deepfakes being used?



🟨 No, it wouldn't make a difference

🟦 Yes, I would be more likely to use an online service that had measures in place to prevent deepfakes being used

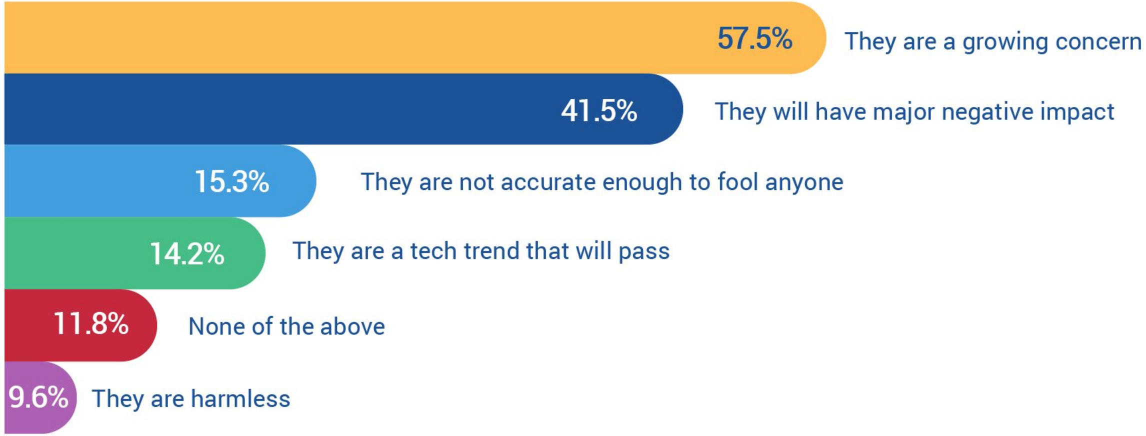
58% think that deepfakes are a growing concern

More than half of consumers think that deepfakes are a growing concern:

- 42% believe deepfakes will have a major negative impact, with the 65+ age group being most concerned (79%).
- 22% of men think they are not accurate enough to fool anyone, compared with 11% of women.

Which of the following statements do you agree with most about deepfakes?

Please select all that apply



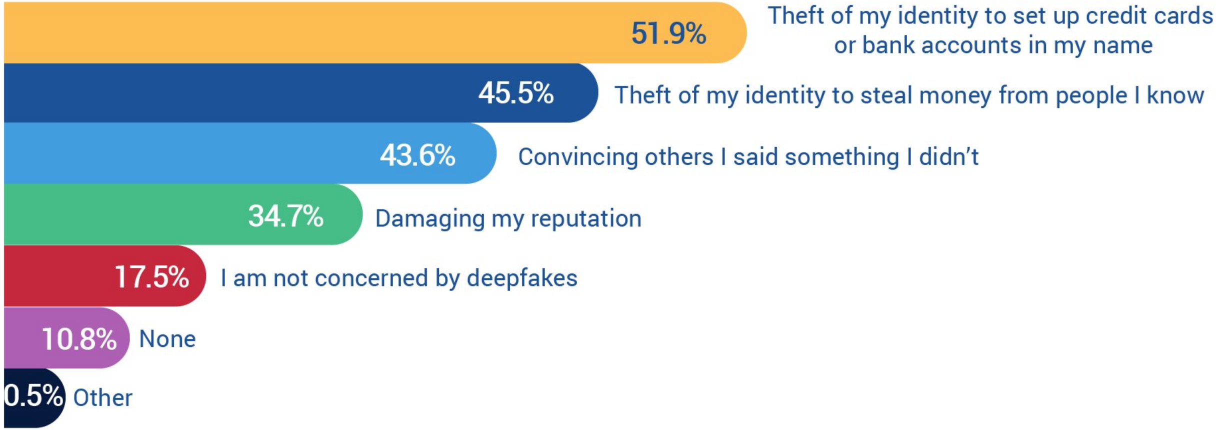
Consumers are most worried that deepfakes could be used for identity theft

Identity and money theft top the list of worries around deepfakes:

- 52% are worried about identity theft to set up credit cards or bank accounts.
- 46% worry about identity theft to steal from people they know.
- The younger generation is most concerned with reputation damage: 36% of 18-24's mentioned this.

Which of the following worries you most about how deepfakes could be used against you?

Please select all that apply



iproov

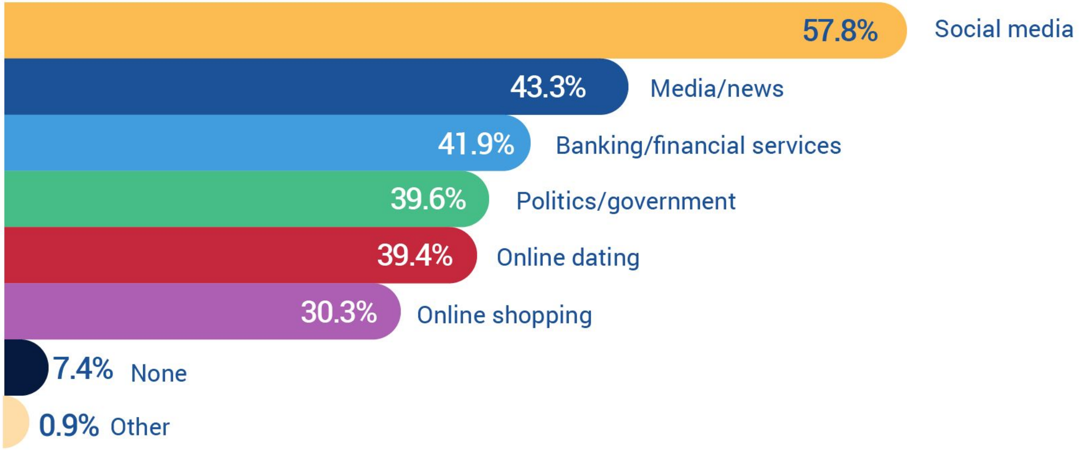
58% think social media is most at risk of being affected by deepfakes

Consumers see many sectors being at risk from deepfakes:

- Social media topped the list, with 58% saying it is most at risk, followed by media and news
- 42% think that banking and financial services are at risk

Which of these areas do you think is most risk of being affected by deepfakes?

Please select all that apply



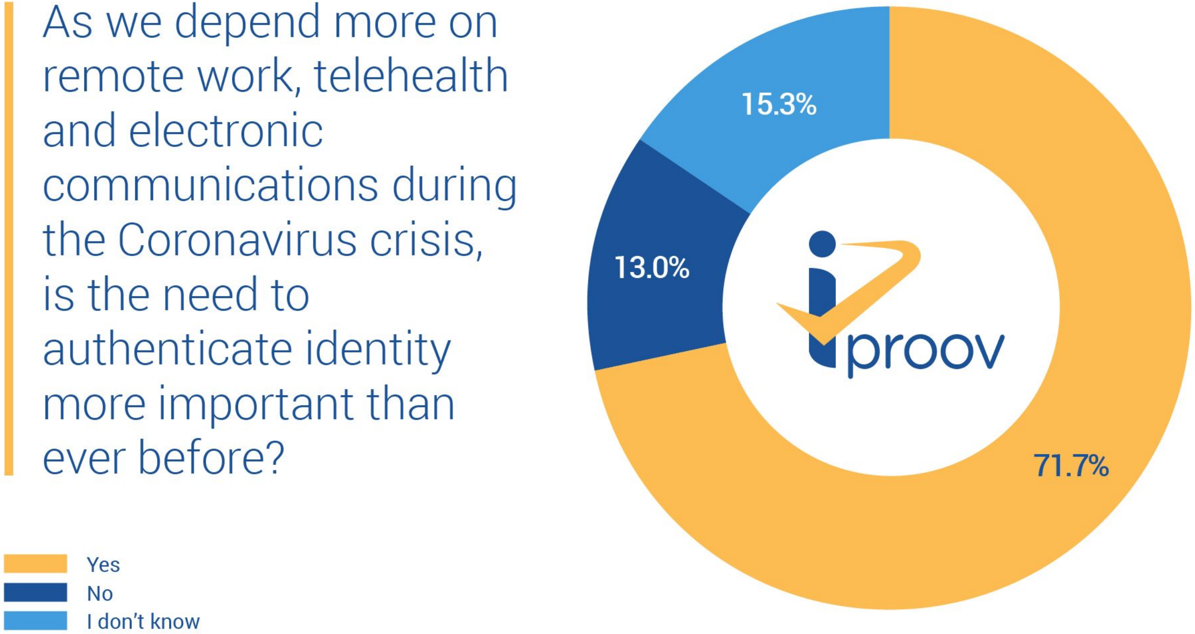
iproov

72% believe the need to authenticate identity is more important than ever before

Increased dependency on digital channels during the pandemic is making consumers appreciate the need for authentication:

- The older generation is most concerned about authentication; 86% of the 65+ age group agree it is more important
- The 18-24 age group is least worried (61%)

As we depend more on remote work, telehealth and electronic communications during the Coronavirus crisis, is the need to authenticate identity more important than ever before?

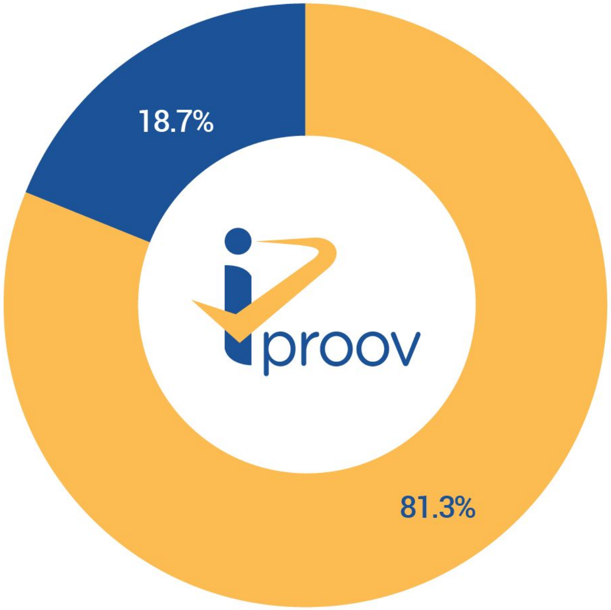


81% believe biometrics will be used to assure identity online

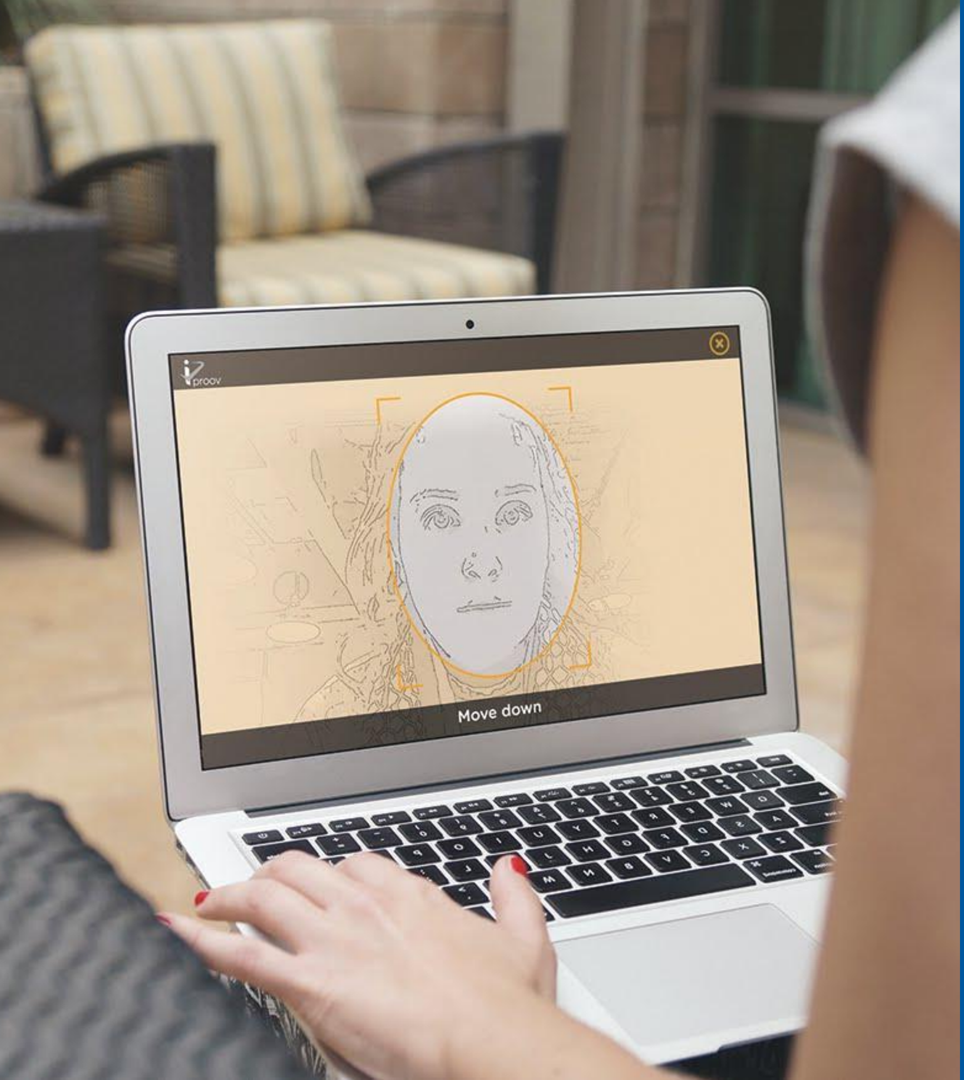
Consumers believe that biometrics are the future of online identity assurance:

- All age and gender groups were aligned on this

Do you believe that biometrics will be used more in future to assure someone's identity online?



🟧 Yes
🟦 No



iProov Genuine Presence Assurance provides:

- ✓ Effortless Usability
- ✓ High Security
- ✓ Spoof Protection

Genuine Presence Assurance:
Right person, real person, right now?

enquiries@iproov.com