



January 2026

Are We Overcomplicating Authentication?

*Simple communications in an age of passwordless and
growing threats*

FINN
PARTNERS

Contents

Introduction	3
How authentication has changed	4
Challenges communicating authentication	6
Top tips to simplify authentication and encourage adoption	11
Conclusion	12
About FINN Partners	13
References	15

Introduction

As authentication technology evolves, brands face a growing challenge: how to communicate the benefits of increasingly sophisticated solutions without alienating their audience.

Marketers tasked with communicating about authentication must navigate the — often fine — line between explaining robust security measures and promoting a seamless, user-friendly experience.

In this whitepaper, we explore the communications challenges marketers face in this area and offer insights on how expert public relations ([PR](#)) strategies can help address them.



How authentication has changed

Identifiers have always been used to authenticate we are who we claim to be. In person, we have signatures and physical documents like passports. In the digital realm, we need another way.

This commonly involves a username and password, sometimes supplemented with an emailed verification link that the person registering must click on.

However, this isn't a strong method of authentication. People can't remember passwords, they frequently write them down, and they often reuse one or a small number of passwords across multiple applications and online services. If any of their passwords are compromised, it opens the door to many aspects of that person's digital life to the password thief.

For these, and many other reasons, passwords offer only weak authentication. For a long time, communications to businesses and consumers have acknowledged this and offered advice on choosing more complex passwords, not reusing them and keeping them hidden by not writing them down.

Then more advanced ways to verify valid users and protect systems, applications and devices from unauthorised access were introduced. These newer, stronger methods include multi-factor authentication (MFA), single sign-on, social sign-on, biometrics, hardware-based security keys and other passwordless systems.



Technology providers, and their communications teams, educating businesses and consumers about these methods have a more complex message to communicate. They must continue to promote the basic premise that people must keep data and online assets secure, explain how to do that and encourage stronger, probably less familiar, ways to authenticate.

However, people don't like change. Despite all the warnings, they stick to what they're used to and continue to rely on, and reuse, weak passwords. Passwords come with drawbacks of usability and strength, but they endure because anyone can use them, anywhere, at any time.

What's more, customers don't want extra steps to authenticate access and, if they believe that is the alternative, they won't get on board with the methods companies want them to use, despite the superior security they offer.

How then, can marketers and PR teams best [communicate authentication](#) and convince audiences to act?

Challenges communicating authentication

Communicators must begin with understanding the challenges, if they are to develop persuasive, convincing authentication communications. These include:

1. The balancing act: security vs. simplicity

The shift from traditional passwords to MFA, biometrics and passwordless solutions represents significant progress in authentication security. But with this progress comes complexity, which can be a barrier for users and decision-makers. Indeed, [according to one study](#), over a quarter (26%) of employees gave up doing something at work because of the hassle of logging in.

Against that perception, the challenge for communicators is to promote the advanced capabilities of more secure solutions but communicate them in such a way that they feel approachable and intuitive.

The goal should be to balance robust security with user simplicity. Overloading customers with technical jargon risks alienating them, while oversimplifying can undermine the perceived value of the technology. Finding this balance requires a deep understanding of both the product and the audience — a space where expert communicators can add immense value.



2. Understanding the audience: businesses and consumers alike

With authentication, there is a blurred line between business-to-business (B2B) and business-to-consumer (B2C) communication. Authentication brands must engage business decision-makers, who care about operational security and efficiency, while also reaching everyday users who prioritise ease and convenience.

Effective communications strategies must cater for both sides of the equation. Business leaders need to understand how advanced authentication solutions will protect their data, reduce security risks, and improve workflows. Meanwhile, consumers want to know how these technologies will protect their digital lives without adding complexity.

The role of expert PR teams is to develop narratives that resonate across these diverse audiences, using clear, relatable language that highlights benefits over technical features.



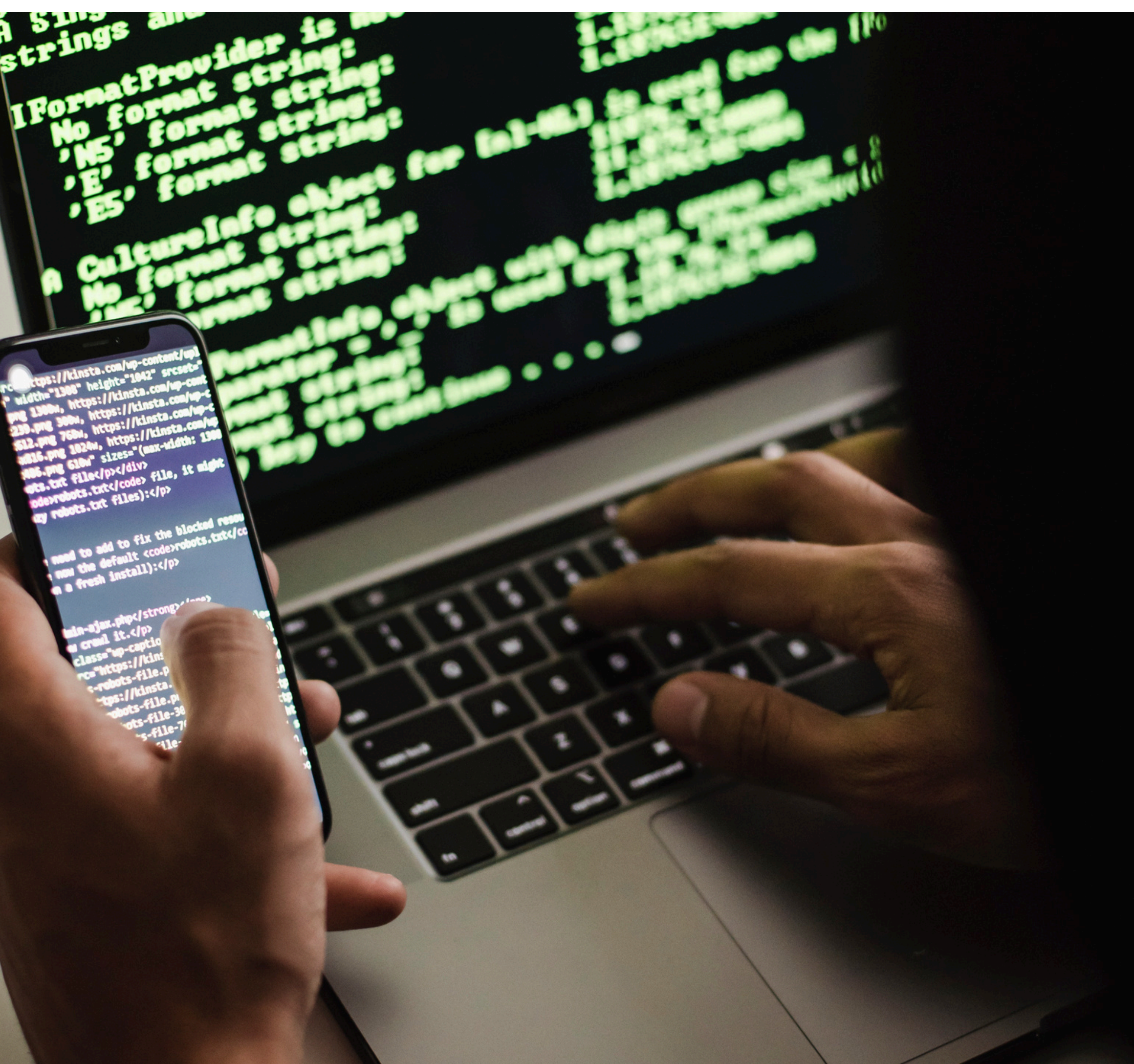
3. Overcoming security fatigue and building trust

Security fatigue is a real issue. Both businesses and consumers are bombarded with constant reminders about new threats and the latest security protocols. This can lead to disengagement, especially if the messaging around authentication technologies feels overly complex or irrelevant.

The evidence tells the story. Over half (54%) of office workers [surveyed by CybSafe](#) said they often or sometimes ignore important cybersecurity alerts and warnings due to information overload.

Marketers must navigate this fatigue by focusing on outcomes that matter to users. For businesses, this might mean highlighting how passwordless systems reduce IT overhead, mitigate the risk of costly breaches, and improve compliance. For consumers, the emphasis should be on convenience—how these solutions can eliminate password management headaches and provide seamless access across devices.

Expert communicators help distil these messages, crafting narratives that break through the noise, build trust, and encourage adoption without overwhelming the audience.



4. Outcomes over features: simplifying the message

One of the most common traps in marketing complex technologies is the tendency to focus on features rather than outcomes. Authentication brands are often tempted to dive into technical details, from encryption algorithms to MFA protocols. While these elements are important, they don't drive customer decisions.

What customers—both businesses and consumers—really care about is how these technologies will make their lives easier or their operations more secure. By shifting the narrative from technical specifications to tangible outcomes, marketers can better connect with their audiences. Validated messaging that focuses on outcomes like "fewer breaches," "faster access," and "reduced operational costs" is far more compelling than jargon-heavy descriptions of how the technology works.

5. Keeping it real and avoiding hyperbole

Robust authentication protects data and systems by granting access only to authorised users. Whichever identifiers are used, be they something the person knows (like a password), something they have (such as a security key) or something they are (like a fingerprint), the end goal is the same—verify accurately that they can be admitted.

Combined with other cybersecurity measures, authentication throws protective arms around the digital spaces they secure, but they cannot eliminate threats. Risks still exist and communications must be honest about that and not over-inflate cybersecurity claims. Communicators must be able to back up the assurances they give whilst reassuring audiences who may be sceptical that more technology will make technology simpler.





6. Driving adoption and standing out in a crowded market

In the workplace, decision-makers and employees must be aligned if the introduction of new authentication solutions is to succeed. Employers are motivated to rollout advanced security initiatives because their companies are under constant attack and the fallout from data breaches is significant. However, employees are less likely to be so motivated. They want an easy life, dislike having to learn a new way of working and resent anything that adds stages to getting something done.

Employers need help to avoid confusing or inconsistent messaging that can hinder adoption, and lead to reluctance and resistance. The most effective communications strategies are clear, consistent, and tailored to the concerns of both business leaders and users.

In an increasingly crowded market, differentiation is key. Brands that can simplify their messaging and clearly communicate the tangible benefits of their solutions will stand out. Whether it's reducing operational costs for businesses or offering seamless user experiences for employees and consumers, focusing on real-world outcomes is a powerful way to cut through the noise.

Top tips to simplify authentication and encourage adoption

For marketers in the authentication space, the key challenge is to simplify without diluting the message. Sophisticated security technologies needn't be intimidating—they should feel accessible, valuable, and necessary. This is where expert communications strategies come in, helping brands to navigate the fine line between security and simplicity.

To simplify authentication and encourage adoption, technology providers should:

1. **Understand** the needs of business and consumer audiences
2. **Connect** with audiences where they are
3. **Tailor** messaging according to audiences' pain points
4. **Be relevant** and visible when audiences are motivated to improve authentication
5. **Focus** on outcomes rather than features
6. **Avoid** over-use of technical jargon
7. **Use** clear, relatable language that reflect audience wants
8. **Present** tangible outcomes, not technical descriptions
9. **Be honest** and prepared to back-up claims
10. **Stand out** through what they stand for



Conclusion

How we authenticate our identities to protect our digital assets has changed. Continued use of passwords online increases the risk of identity and data theft, unauthorised systems access and the personal and commercial pain these can cause.

There are alternative, stronger ways to manage and verify identities in the digital realm. These need a favourable public image to succeed in winning over sceptical audiences who want authentication to be strong, but practically invisible.

Thoughtful, strategic communication will be essential in driving the next wave of authentication technologies forward. By crafting consistent narratives and understanding the needs of both business and consumer audiences, authentication brands can improve adoption and build stronger trust with their customers.

Communications must be outcomes-based. It's easy to fall into the trap of over-explaining the technical bits of security, but most users don't need to know the ins and outs of time-based one-time passwords (OTPs) or encryption algorithms. They just want to know how these things help them.

Expert PR teams can play a pivotal role by helping authentication brands develop unified narratives that resonate across diverse audiences, ensuring that both decision-makers and end users understand how these technologies will enhance their lives or operations. By staying focused on clarity and value, authentication brands can drive higher adoption rates and establish themselves as leaders in the space.

Find out how FINN Partners can help you avoid overcomplicating authentication with compelling, impactful communications for a high-tech world, visit finnpartners.com/uk/sector/technology or [contact us](#) to discuss.

About FINN Partners

Founded in 2011 on the core principles of innovation and collaborative partnership, FINN Partners has grown from about \$24 million in fees to nearly \$200 million in fees over ten years, becoming one of the fastest growing independent public relations agencies in the world. The full-service marketing and communications company's record setting pace is a result of organic growth and integrating new companies and new people into the FINN world through a common philosophy. With more than 1,300 professionals across 36 offices, FINN provides clients with global access and capabilities in the Americas, Europe and Asia.

FINN Partners clients are also supported through longstanding partner agencies and its membership in the PROI network of leading agencies around the world. Headquartered in New York, FINN has offices in: Abu Dhabi, Atlanta, Bangalore, Bangkok, Beijing, Boston, Chicago, Delhi, Denver, Detroit, Dublin, Fort Lauderdale, Frankfurt, Hong Kong, Honolulu, Jerusalem, Kuala Lumpur, London, Los Angeles, Madison, Manila, Mumbai, Munich, Nashville, Orange County, Paris, Portland, San Diego, San Francisco, Seattle, Shanghai, Singapore, Vancouver, Washington D.C. and Yangon. Find us at finnpartners.com and follow us on Twitter and Instagram at [@finnpartners](https://www.instagram.com/finnpartners).