



The fundamentals of establishing digital trust

Telesign's Brendon O'Donovan on how to establish and nurture trust



Brendon O'Donovan

O'Donovan leads key high-priority transformation objectives as well as the product marketing and portfolio management teams at Telesign, the leader in providing continuous trust to global enterprises by connecting, protecting, and defending their customers' digital identities.

Digital trust: It's the present and immediate future of how enterprises and customers do business, says **Brendon O'Donovan** of Telesign. But what are the fundamentals to create it and the tools to ensure it throughout the customer relationship?

In this interview with Information Security Media Group, O'Donovan discusses:

- The essential elements of digital trust;
- How to balance security with the customer experience;
- Tools and techniques to nurture digital trust.

Defining digital trust

Tom Field: We hear an awful lot about digital trust these days. How do you define this concept?

Brendon O'Donovan: The definition of trust is having a firm belief in reliability or truth. Having a connection with somebody or something gives you that reliability. It's a feeling of safety. Trust is used throughout

“In a digital world, you have to be able to trust that the company you’re working with is going to follow through on its promise. You have to trust that it’s going to protect you and be transparent enough that you understand that you are safe working with it.”

digital security to talk about the interactions in which you have firm trust between two partners—a firm belief that there is security on either end. So digital trust is about feeling that you can trust the interaction between the company and the customer or the user, and their relationship with the platform.

In network cybersecurity, there is the concept of zero trust, where you shouldn’t trust anything and you should always verify. In zero trust, you create trust when you verify that it is the person and they do have access. Now, when you extend that digital trust to a consumer perspective, it’s a little different because then you don’t have control of their network. You have to work with them to understand who they are. You have to build monitoring and a system to check, verify and confirm that the person you’re working with is real and that, for the consumer, the company that they’re working with can be trusted.

The immediate future

Field: In a previous conversation, you told me that digital trust is the immediate future of how enterprises and customers do business. Expand upon that a little bit, please.

O’Donovan: In more and more of the interactions that happen online, it’s no longer just you logging into your email. You’re now doing commerce. The lines between your physical world and the online world blur. You order your food; it shows up at your door. You order a car from your phone; it shows up at your door to pick you up. These interactions are no longer just about your information online. They are about the convergence of the physical world and the online world. So, trust is the way that we do business today. In a digital world, you have to be able to trust that the company you’re working with is going to follow through on its promise. You have to trust that it’s going to protect you and be transparent enough that you understand that you are safe working with it. Digital trust is the immediate future because it’s here. And it’s a two-way street. It’s the emerging way of viewing security trust relationships between consumers and enterprises.

Balancing customer experience and friction

Field: The question every organization wrestles with these days is: How does one balance security with the customer experience to find the right amount of friction?



O'Donovan: Anything digital is always about balancing the amount of information that a company wants to know about the consumer and how much the consumer wants to give to the company. Security is no different. It's about: How much security can you put in place to make sure that the person you're working with is the right person and that they are who they say they are, that they are safe to work with and that there's some reputation there?

Field: No friction is not ideal, and too much certainly is going to turn customers away. What's right?

O'Donovan: It's a constant balancing act. No one solution is right, and no one solution is wrong. With friction, you have to go through some levels of sign-up or verification that you are who you say you are. This can be filling out a form, verifying your phone number or verifying your email address—confirming that the information you put in is right. That's commonly what friction refers to: How many steps do you have to go through to become a customer?

The immediate perception is that friction is bad, but it's not always bad. It gives you security that the company is checking on who you are to make sure you're not a scammer or a bot. Balancing security and friction is about adding enough security and trust in the friction to communicate that you have a good working relationship. It's easy for the customer to work through, but it still gets enough from that customer to verify who they are. It's not a "right or wrong" situation. It levels up or down, depending on the type of relationship you need to have.

If you are a bank or somebody that's dealing with transactions, the friction should be higher. You should have some level of trust that the bank is verifying your information and other people's. If you are just signing up for a social network, do you need to go to that same level? Probably not. But do you need a higher level than you would when signing up for a library card? Probably. It's fluid, depending on the situation. You need to build digital trust signals to be able to understand where you need to

challenge more and when to signal to the customer that the situation is secure for them, but also to make sure it's secure for you as well.

Establishing digital trust

Field: What are the fundamentals of establishing digital trust?

O'Donovan: The fundamentals of a lot of the online world are similar to the concept of zero trust and network security in that you're trying to validate that the people that you are working with are who they say they are and they have permission, or they have the right to be doing what they're doing, and they're authentic. But network security, which usually involves a work environment where you have employees that have to do something on your network and adding friction is just part of the work contract, doesn't really translate down to a consumer relationship.

If you have too much added friction for security, you tend to lose customers. So the fundamental in that relationship is: How do you start looking at the digital signals – the

patterns associated with good customers versus bad customers? Do you need to understand who they are from a standpoint of their biometrics or their phone number, or do you need to understand their geo locations? What signals do you need to understand and what patterns do you need to watch for so that you can build digital trust?

When you start building that foundation, you start to understand what “good” looks like and what “bad” looks like. An example in the physical world is going into a bank and walking up to a teller to sign up for a bank account. The teller will ask you for your ID. When they start seeing you come in regularly to cash checks and understand who you are and what your pattern is, however, they probably won't require an ID anymore. But if you come in and want to drain your bank account, change the name on the account and put new signatories on the account, they're probably going to ask for your ID and question you because that behavior is outside of your norm. It's the same concept in digital trust. Understanding what safe and unsafe patterns look like and what is normal and not normal for a customer are part of building the foundation of the digital trust experience.

“The phone is now one of your primary devices and the primary way you interact with the internet. As one of the biggest mobile identity providers in the world, Telesign connects who you are in the online world with what you have in your pocket.”

Digital trust tools

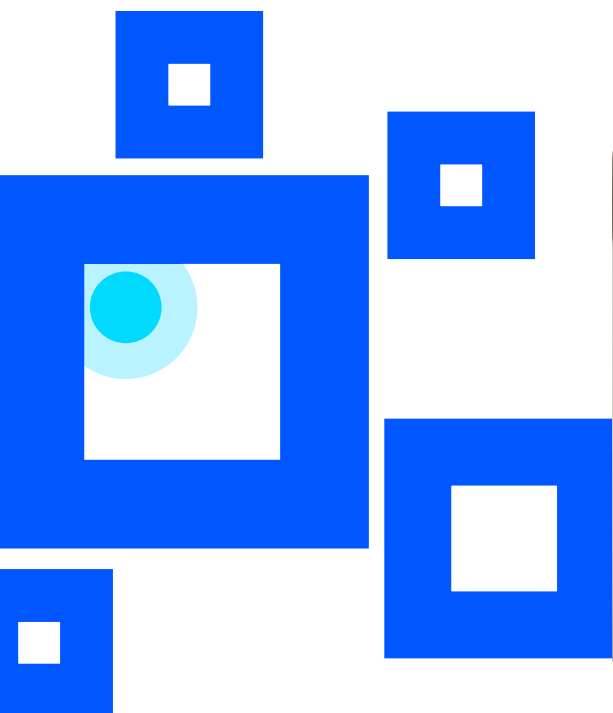
Field: What types of tools ensure digital trust?

O'Donovan: Use new passwords. Use knowledge-based questions to challenge what's going on in an account. Use two-factor authentication or multifactor authentication to guarantee possession of something that you know that person owns. Use biometric physical documentation verification. All of these things go together to create the digital pattern or profile of the way someone works, where they're coming from and what devices they're using. Increasingly, companies are using machine learning and artificial intelligence networks, which can make these connections faster and better. That's important because we expect a seamless experience. We don't expect to sit and wait 30 minutes for a company to check to make sure we are who we say we are. New and emerging technologies are required to make the reality meet the expectations—to put all of those signals together to make split-second decisions.

The Telesign approach

Field: What is Telesign doing to help its customers establish and nurture digital trust?

O'Donovan: Telesign is an interesting intersection of the physical world and the online world. Anywhere you go, you have a phone. You have some relationship with a carrier somewhere. You've signed up for that phone number. The phone is now one of your primary devices and the primary way you interact with the internet. As one of the biggest mobile identity providers in the world, Telesign connects who you are in the online world with what you have in your pocket. We do that through your phone ID, which gives companies access to key, crucial information about a phone number. We do a lot of risk scoring around phone numbers and interactions globally, so we can return a risk score around a phone number to tell you how risky it is and why. We also do multifactor authentication. Putting those three things together gives you an anchor point around something that is very strong, that brings the digital world and the physical world together.





Leaders in digital identity and programmable communications

Telesign connects, protects, and defends companies, customers, and the digital interactions between them. With powerful AI that delivers identity with speed, accuracy, and global reach, we enable continuous trust. Empowering companies to transact, communicate, and engage with their customers free of fear, continuous trust makes the promise of the digital economy possible.

Click here to learn more: www.telesign.com

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

 **BANK INFO SECURITY®**  Just for Credit Unions **CU INFO SECURITY®**  **GOV INFO SECURITY®**  **HEALTHCARE INFO SECURITY®**

 **infoRisk**
TODAY

 **CAREERS INFO SECURITY®**

Data Breach.
Prevention. Response. Notification. TODAY

CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io