The end of digital trust is near. How calibrated trust can help us

Dr. Remco Wijn, Drs. Caroline van der Weerdt, Dr. Rick van der Kleij, Dr. Heather Young, TNO

Trust is paramount for creating social and business relations, adopting technology, cooperating and creating economic value. With an increasingly digital economy, no wonder the importance of digital trust is advocated by so many scholars and businesses alike. However, contrary to purported common wisdom, we propose that actual trust is not created through communicating one's trustworthiness, and should not be an isolated goal in itself. Rather, real trustworthiness comes from actively practicing fair and transparent policies and conduct, the establishment and maintenance of which rests with both the trustor (e.g., a customer) and the trustee (e.g., a supplier). In this paper, we introduce the concept of calibrated trust, and how it relates to the need for increased customer involvement.

Concepts of digital trust

Digital trust is considered the "new gold" for organisations and crucial for the development of the digital economy (NLdigital, 2019). It is even considered by some to be a prerequisite for doing business (Buijs and Vermeulen, 2016). Digital trust could "stimulate 2.8 percent additional growth for large organisations, potentially creating value estimated at 5.2 trillion dollars for society as a whole" (Abbosh & Bissell, 2019). Statements as these logically motivate organisations to ask how they can gain trust among their customers, leading to suggestions that "With the right people, the right means and flexibility you can reach the ultimate goal of communicating trustworthiness", or: "Digital

March 8 9 11

Citrix investigating unauthorized access to internal network

TLS 64bit-ish serial numbers mass revocation

Citrix hacked by password-spraying attackers

trust is not just about cybersecurity, but also ethics, privacy and reliability" (Naber, 2019), or: digital trust is "a strong focus on security combined with transparency on the use of customers' data" (Buijs and Vermeulen, 2016).

Although such statements are largely true, the problem is that they often suggest that trust is a goal in and of itself or a means to create economic value. It ignores the end user's (or the customer's) role and behaviour in the digital environment. Moreover, a focus on winning trust underappreciates the needs, deliberations and goals of individual customers, and the functioning of trust itself. We argue that this approach stands in the way of cybersecure behaviour at the customer end, and therefore in the way of a durable trust basis.

Digital trust in practice

Let's take a moment to think about what happens when we trust. Suppose someone is exploring the domain of smart home appliances. The consumer starts by installing a smart door lock with which one can see who is at the front door and unlock the front door using an application on a mobile device. A consumer may be wary that hackers could find ways to intercept the communication between the mobile device and the door lock or find other ways to control the lock. The lock vendor tells the customer that a particular lock uses first class software and protocols, which cannot be intercepted or hacked. The vendor gains the customer's trust and the lock is sold.

What the vendor did not focus on, however, are other vulnerabilities that may pose a risk to the door lock, such as the need to change the password or to install software updates. Because the consumer trusts the device, basic cyber hygiene measures, such as updating the software, are neglected, leaving the device vulnerable. If the customer's home network is compromised, for instance through another weakly secured device or vulnerabilities in outdated software, and the front door is hacked, this may leave the consumer not only victimized but also untrusting of the vendor, manufacturer, the lock, and digital smart home solutions as a whole. Extending this line of reasoning: too much trust may harm the development of the digital economy and perhaps even society as a whole.

In this example, the customer trusted the lock manufacturer to build a sound and secure lock and the predictability with which it does its job. The customer trusted the vendor to be knowledgeable about home appliances and security, to sell the customer a product in his best interest, and his integrity to give complete an accurate advice. Thus, trust, which we define as a willingness to depend on another, is a result of beliefs about the competence, benevolence, integrity, and predictability of the other on whom one chooses to rely (McKnight & Chervany, 2001).

Some trusting beliefs seem primarily functionally based (i.e., competence and predictability). These beliefs are often influenced by assurance cues such as a modern, well-functioning, or normal appearing website, and security heuristics such as security information displayed in the address bar of browsers (Cheshire, 2011; Li, Hess, & Valacich, 2008). However, such measures do not influence trusting beliefs regarding benevolence and integrity which seem primarily intrinsic and value-based (Krauter & Faullant, 2008). Studies on online banking, for example, show that security measures and perceived security do not influence consumer trust. According to these studies, trust is more influenced by privacy perceptions of online bank services (Law, 2007), which relates much more to the core of companies' intrinsic values and identity.

Consequences of trust

Trust enables us to create durable social relationships, to work together toward common goals, to invest in each other, to do business, et cetera. Abbosh and Bissell (2019), among many others, focus on positive commercial and financial effects of trust. However, an elemental part of trust is that it involves uncertainty or risk, such as of not receiving an online purchase (Cheshire, 2011). It also involves the absence of direct control. For example, typically, most societies offer legal safety nets for situations in which trust is violated. But these do not offer a direct way of controlling the behaviour of the other person or organisation, nor will they always be effective. Thus, from the perspective of consumers, trust is a leap of faith to overcome uncertainty with a chance of being duped and without much control to restore any harm done.

And people and institutions do get duped. Instances of misplaced or manipulated trust lead to an average annual costs of EUR12 million per large organisation worldwide (Ponemon Institute, 2019). Other consequences include negative emotional and practical consequences as a result of identity and data theft or abuse, or even physical harm in the case of online trade in counterfeit pharmaceuticals.

Need for calibrated trust through engagement

In light of this leap of faith to overcome uncertainty, we introduce the concept of calibrated trust as a more effective approach to developing enduring digital relations. We colloquially define calibrated trust as healthy distrust. That is, companies and organisations should help consumers understand what they trust, when they trust, and to take ownership of their own cybersecurity whenever possible. It means that companies should not only help customers take the leap of faith, but also help them cope with the uncertainty and risk inherently present in trusting relationships. In order to do this, we posit that organisations should

help consumers gain the capabilities, opportunities and motivation to determine the security of their services and products, and the trustworthiness of individuals and organisations providing those services and products. This means disclosure of possible cybersecurity strengths and weaknesses, coupled with proactive tools for protection and resolve on the customer level. Moreover, it implies partnering with customers, teaching them, tooling them and motivating them to prevent victimization and warrant a positive online experience. This goes beyond customer engagement purely on the experiential level of a product or service; it requires engagement on a far-reaching procedural and functional level. This is not an easy task, and requires a different type of relationship with the customer. However, we believe that adding this layer of customer engagement will in the end induce a better customer experience overall.

Research agenda

Organisations' current practices to establish and maintain digital trust often revolve around their own measures to communicate trustworthiness, but exclude the crucial role of the end user. We posit that companies should partner with end users and customers to focus on introducing calibrated trust within their (digital) portfolio. In a shared research program with Dutch financial institutions, we are presently conducting research on the workings and consequences of this calibration process in relation to security and how real trust is fostered. This research includes questions on how to prevent false perceptions of security, how these perceptions are influenced and how they differ between consumers and per technology, how we can optimally support consumers in making the right security decisions, and how to change (false) perceptions that customers may hold, for instance, through better security design. By answering these questions, together with our business partners, we aim to support the goals of both cyber secure behaviour and economic benefit.

Literature

Abbosh & Bissel (2019). https://www.accenture.com/pl-en/insights/cybersecurity/reinventing-the-internet-digital-economy retrieved on 1-11-2019.

Buijs & Vermeulen (2016). https://www.accenture-insights.nl/nl-nl/artikelen/digital-trust-oracle. Retrieved on 1-11-2019.

Cheshire, C. (2011). Online trust, trustworthiness, or assurance? Daedalus, 140(4), 49–58. doi:10.1162/DAED_a_00114 PMID:22167913

Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: the influence of internet trust. International Journal of bank marketing, 26(7), 483-504.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. European Journal of Criminology, 12(2), 226-241.

Law, K. (2007). Impact of perceived security on consumer trust in online banking (Doctoral dissertation, Auckland University of Technology).

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

Naber (2019). https://www.pwc.nl/nl/actueel-en-publicaties/themas/digitalisering/bouwen-aan-digitaal-vertrouwen.html retrieved on 1/11/2019.

NLDigital (2019). https://www.nldigital.nl/thema/vertrouwen/ retrieved on 1/11/2019

Ponemon Institute: The cost of cybercrime study (2019). Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 on 1-11-2019.

March

15 Hackers stole 20 million from Mexican banks

20 PuTTY releases important software update to patch 8 high-severity flaws

LockerGoga ransomware disrupts operations at Norwegian aluminum company