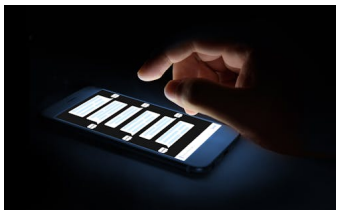

Does more convenience mean less security?Shutterstock

Soon, you will be able to check your bank balance or transfer money through Facebook Messenger and Twitter as banks experiment with chatbots . Companies like Ikea have used customer service chatbots for close to a decade. But their use in financial services represents a new tension - do we want convenience or a feeling of security from our banks?

Research shows that when it comes to online banking, customers are prepared to trade security for convenience. But when customers think there is a threat to their security, this feeling reverses.

Researchers at QUT recently found that a sense of insecurity is one of the reasons consumers do not already interact with financial institutions on social media. And the feeling of insecurity actually increased between 2010 and 2014, as social media became more popular.

This means banks will likely have to design their chatbots to give a sense of security, just like they do with bank branches.

---

***Read more:*** *Banks can’t fight online credit card fraud alone, and neither can you*

---

The trade-off between the convenience and security of a service comes down to trust. Trust in the service provider to protect our personal details (“soft trust”) and trust in the platform and infrastructure you use to access the service (“hard trust”). Both types of trust are important to ensure a sense of balance.

For instance, it's of little use having an impregnable vault if consumers don't trust the person with the key. Likewise, trusting a staff member is of little value if consumers can see there are safety flaws in the system. Consumers need to know that their trust (both hard and soft) is well placed before they can enjoy the added convenience of emerging technologies.

## Designing a sense of security

Banks previously used physical design to create a sense of security and trust. This is called sig nalling
and involved the use of marble floors, metal bars, and imposing vaults in bank branches to reassure us that our money is safe.

As our banking shifted into apps and websites, we faced the same problem as chatbots currently do - the internet was undoubtedly more convenient but at the expense of a feeling of safety. This was also solved with design.

Websites and apps were designed to send similar signals as that of the physical bank branches. For instance, by using security symbols (such as the green padlock next to the URL of this website), logging customers out if they're inactive for too long, and moving keyboards for entering online banking passwords.

Research has found consumers feel more secure when a system generates a unique password for each login, than they do when they are allowed a permanent password. Even seeing the initials of an employee in a Tweet can humanise the interaction and instil trust.

All of these design aspects evolved to signal trust and security. But chatbots do not have access to these same design capabilities - you can't do something as obvious as having a big vault or green padlock.

## So what does all this mean for chatbots?

Research from Accenture indicates Australians are ready for artificial intelligence in the financial sector - 60% are open to entirely computer-generated banking advice.

And a World Retail Banking Report found that while 51% of consumers still prefer face-to-face interaction for more complex products and services, they also demand greater levels of digitised customisation and personalisation from financial institutions.

All of this means chatbots could work for banks. On the back end, chatbots can be secured just like websites and apps
- using two-factor authentication and encryption etc.

It's important to promote this feeling in users too. A big part of it will be "humanising" the interaction. For instance, chatbots can be programmed to seem more human - achieving the same thing as staff members' initials on social media. They can be given names, personalities, and even emotions.

But this will just be the start. As artificial intelligence and chatbots become a part of daily life, the trust signals will need to be built, one digital brick at a time.

*The authors do not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and have disclosed no relevant affiliations beyond the academic appointment above.*

Authors: Kate Letheren, Postdoctoral Research Fellow, Queensland University of Technology

**Read more** http://theconversation.com/banking-with-a-chatbot-a-battle-between-convenience-and-security-81328