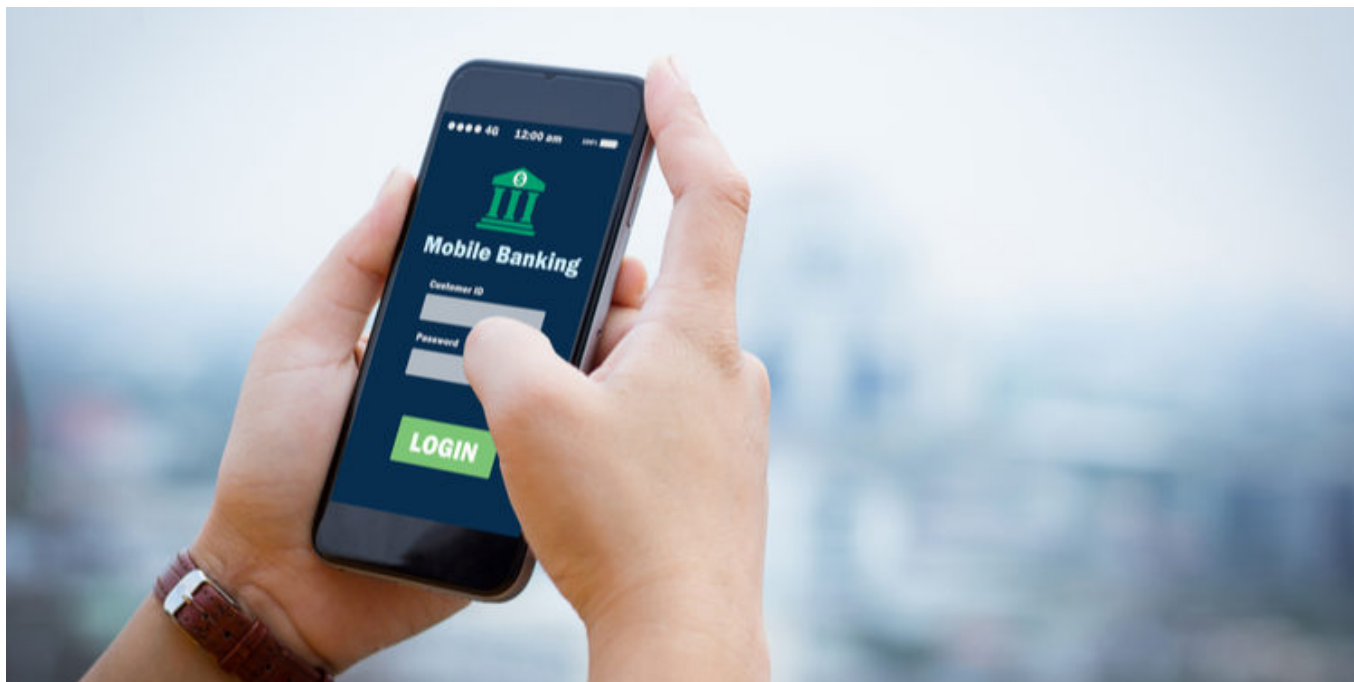


Home » Security » Security concerns undermine faith in digital banking

Security concerns undermine faith in digital banking



At the back end of 2020, data from comparison website Finder found that 27% of British adults had an account with a digital-only bank, which represents growth of around 300% from 2019. The survey underlined the importance of security in the minds of consumers, as it was rated as the most important feature of any digital bank.

Unfortunately, recent [research](#) from Nanyang Technological University, Singapore suggests that poor security may be undermining the faith people have in digital banking. Like Finder, the researchers found that security was foremost in the minds of digital banking customers, with 40% saying that it was the most important consideration when using things like mobile banking applications.

The priority given to security dwarfed that of things such as service quality and system quality, both of which were roughly half as important. The researchers highlight the significant growth in digital banking, particularly during the Covid-19 pandemic when things such as touchless payment systems became increasingly popular.

this study highlights implications for banks' strategies for retaining their mobile banking users, as well as exploring how to capture new customers,"

— the researchers explain.

Building loyalty

The researchers believe their findings illustrate how important it is for banks to provide robust security if they aim to ensure their customer base is happy and loyal to them. Importantly, they found that while banks were putting considerable effort into designing apps and interfaces that optimize system quality, there was less emphasis given to security levels.

The paper outlines a number of steps banks can take to not only provide security to users but visibly show that they're doing so. Being visible is crucial so that consumers feel a strong sense of security whenever they're using their banking app.

The multi-level security features recommended include things such as the use of pop-up messages to alert users to possible risks when using mobile banking tools. The researchers also strongly advocate a robust policy statement that is not only legally rigorous but accessible to end-users.

The security threat

Cybersecurity is an enduring challenge for the finance industry, as while clear progress has been made, the sector is in a constant battle against attackers whose threats are increasing in terms of their volume, velocity, and variability.

The move onto mobile platforms adds an additional attack surface for attackers to exploit, with the Covid pandemic adding an extra challenge to the cyber resilience of banks, not least due to the widespread adoption of remote working as countries locked down.

This is set against a macroeconomic picture that is highly uncertain, with many banks struggling to maintain cybersecurity budgets even as they are attempting to significantly expand their digital capabilities. Throw in a skills shortage that leaves many banks under-resourced in this vital area and it's a challenging situation, to say the least.

This website uses cookies. By continuing to use this website you are giving consent to cookies being used. Visit

our [Privacy Policy](#). I Agree

Achieving transformation while remaining secure

So is it possible to digitally transform one's operations while also maintaining security against this increasingly complex threat landscape? Yes, and the key is to ensure that effective preventative controls are deployed while also implementing processes to allow for rapid recovery from any adverse effects that may befall the business, whether it's ransomware, malware, or any other form of attack.

As highlighted by the Singapore research, it's also vital that banks adopt a security-by-design approach so that cybersecurity is a fundamental part of any digital infrastructure and architecture decision. Central to this will be a robust assessment of the risks faced.

The best cyber risk assessments not only include a range of third-party evaluations, but also an accurate and robust assessment of things such as the culture and capabilities of the business, the governance policies in place, and the financial risk of attacks.

These reports are valuable because they allow boards to understand the risk their organizations face, even while not having strong technical skills.

There is undoubtedly considerable potential for the banking sector in the new digital platforms that are emerging to give users the flexibility and service levels they crave. This potential will only be realized if a security-first approach is taken to the digital transformation, however, as above all else, consumers crave security as well as flexibility in their digital banking.

“By providing a stable and secure mobile banking system that boasts fast responses and efficient service, banks can encourage customers to continue using their mobile banking application, while ultimately strengthening user loyalty,” the Singapore researchers conclude. “The results can also help improve their overall mobile banking strategy and cater the functions of their apps to the needs of different age groups.”

