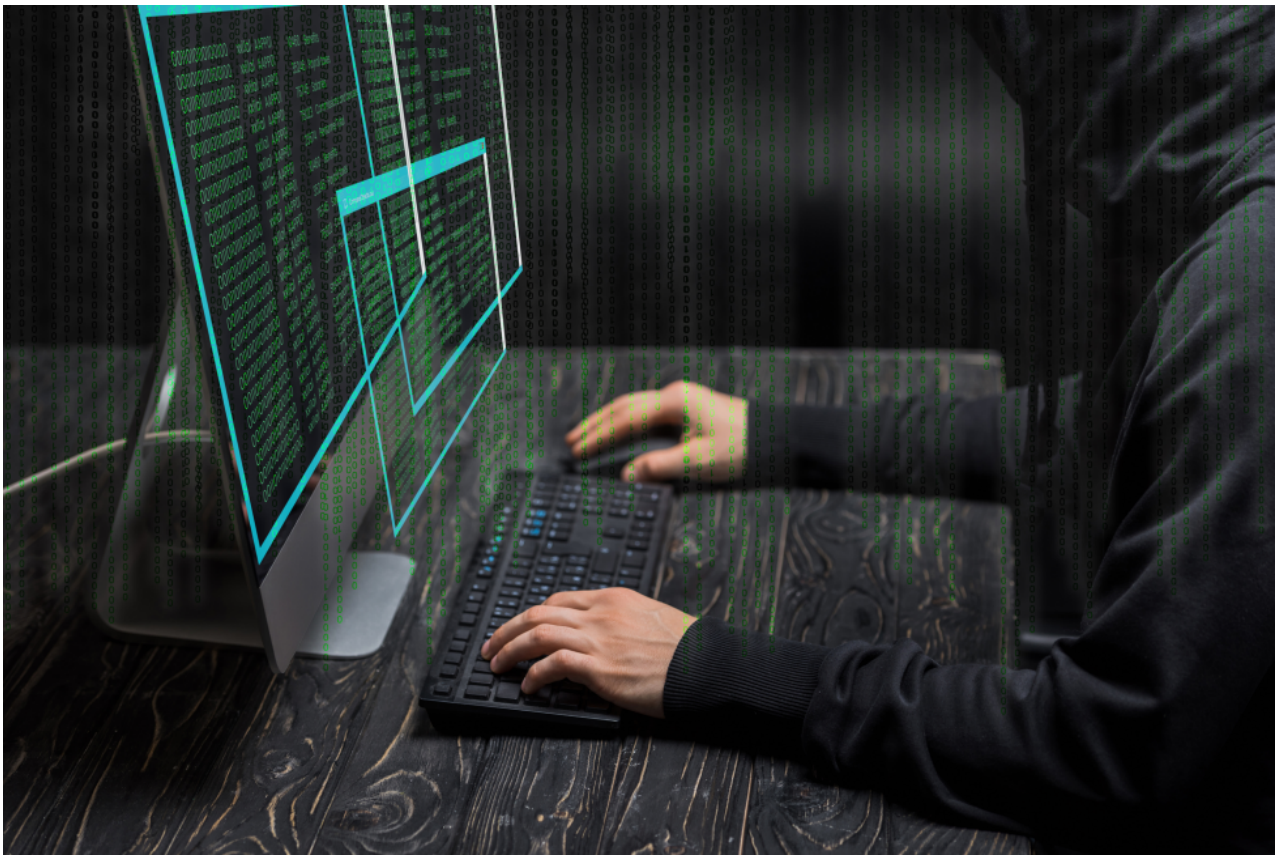
The Rise of Digital Banking Brings Fresh Security Concerns

internationalbanker.com/banking/the-rise-of-digital-banking-brings-fresh-security-concerns

December 24, 2020



Thanks in large part to the rapid evolution of digital banking, customers are finding it much more convenient to manage their finances through online channels. Applying for a loan, opening a new account or investing in financial markets—processes that previously might have taken hours, days or even weeks to complete—can now be concluded in a matter of seconds. Mobile apps, for instance, allow users to execute a range of tasks with just a few taps on their smartphones and are thus making the overall banking experience much more enjoyable and user friendly. Accompanying these impressive advancements is a plethora of new security risks that financial firms must address if they are to continue delivering the best, safest experiences to their customers.

The global coronavirus pandemic has only accelerated the shift towards the digital realm. With lockdown restrictions preventing regular bank-branch activity from taking place, and with social-distancing measures further reducing the opportunities for in-person engagement, virtually every part of the world has seen the use of online- and mobile-banking services skyrocket since the onset of the virus at the end of the first quarter. According to market-research firm Research Dive, for instance, COVID-19 has

“immensely impacted” digital banking, such that the researcher has forecast that its global market will rise at a CAGR (compound annual growth rate) of 10 percent between 2019 and 2026, generating a revenue of $1,702.4 million during the period.

Does such growth imply more opportunities for cybercrime to transpire? Absolutely. The financial-services sector is the most targeted of all industries, with research suggesting that firms in this sector are 300 times more vulnerable to cyber-attacks than any other. And with the bulk of the attacks aimed at banking customers rather than institutions, it means that digital banking—a technology that seeks to give more authority to customers from the outset—remains exposed to a myriad of security risks. “Digital banking provides faster processing of financial transactions, more convenience, and a model that allows for the continuation of a financial industry even in the face of a pandemic,” observed Ben Hartwig, the chief security officer and web operations director at data provider InfoTracer, in *Security Magazine* in September. “However, digital banking makes banks vulnerable to cyberattacks. Banks are now facing fresh security challenges that were brought on or affected by COVID-19.”

The research illustrates just how vulnerable banks have become, moreover. A study published in January 2020 from analytics firm FICO, for instance, found that almost four in five Asia-Pacific banks (78 percent) believed the introduction of real-time payment platforms such as P2P (peer-to-peer) transfers and mobile payments had resulted in increased fraud losses. Almost a quarter (22 percent) said that they expected fraud to rise significantly over the following 12 months, while an additional 58 percent expected a moderate rise in fraud. “While the convenience of real-time payments is great news for customers, increasingly, banks have zero time to clear a transaction or payment. AI can’t slow down the clock, but it can help create systems that are radically quicker to recognize a transaction that smells likely to be fraudulent,” said Dan McConaghy, president of FICO in Asia-Pacific. “Banks will need to move beyond passwords and OTPs [one-time passwords] and add biometrics, device telemetry and customer behaviour analytics to keep up with the changing payments landscape.”

As such, it is of paramount importance that banks provide a wholly safe environment for customers to manage their financial lives—a goal that has not yet been achieved, it seems. Customer-experience tech company Lightico and digital-identity verification-solutions firm MiTek surveyed 1,329 Americans in July about their views on online transactions. Asked how secure they felt about online transactions, 20 percent said they felt “very secure”, 46 percent believed they were “secure”, 31 percent said they considered themselves to be “somewhat secure”, and 3 percent confessed they were “not very secure”. Somewhat more positively, however, around 95 percent of respondents had completed at least one online financial transaction in the previous three to six months (with 100 percent of those aged 66 and above having done so); and less than 10 percent agreed with the statement “No, I don’t feel online transactions are secure”, with a minimum of 0 percent for the 18-to-24-year-old age bracket and a maximum of 10 percent for the 66-to-75-year-old age bracket. As far as various industries are concerned, however, most respondents considered the finance/banking industry as the most secure, at 26 percent.

So, what are some of the key areas in digital banking about which customers don't feel particularly secure? Arguably, identity theft elicits the most concern. According to the Consumer Sentinel Network, which is maintained by the US consumer-protection body the Federal Trade Commission (FTC), there were 3.2 million consumer-fraud and identity-theft complaints filed in 2019, either with federal, state or local law-enforcement agencies or privately. Of those filings, a hefty 651,000 were complaints related to identity theft, with credit-card fraud the single-most reported identity-theft complaint. And with online retail becoming more vital to consumers with each passing day, those in possession of stolen credit-card information can buy goods over the internet much more easily than they would physically manage to do in a shop.

Should cyber-attackers be able to hack into a bank's digital infrastructure, identity theft becomes a major risk for customers that is impossible to ignore. And in more recent times, account takeovers have become especially popular. A type of identity theft, this cyber-threat involves a nefarious third party gaining access to a user's account from which the criminal can change the account details by posing as the user. With all subsequent updates to the account being diverted to the criminal's contact address, the user is often none the wiser about the attack until it is too late.

Malware is also a serious and growing problem. Often this will take the form of automated threats, such as ransomware, designed to appear as normal, legitimate e-mails from known correspondents. In reality, however, they are phishing e-mails that induce the unwitting target to download an unsafe attachment containing the ransomware, which has the capability to block the user's access to his or her account; and the perpetrator then demands payment in exchange for the block to be lifted.

Last year, a report from cyber-intelligence company IntSights revealed that the global financial-services industry had been the recipient of more than one-quarter of all malware attacks, more than any other single industry. It also found that there had been significant annual increases in the number of compromised credit cards (212 percent), credential leaks (129 percent) and malicious apps (102 percent). "When it comes to financial crime, it's mostly a numbers game. The more stolen account numbers you can try to access, or phishing sites you can launch, the better your chances of success," the author of the IntSights paper, Hadar Rosenberg, told *Forbes*. "Around the globe, banks are seeing more frequent and more aggressive cyber-attacks, and the severity and sophistication of these attacks are increasing all the time."

And to illustrate the vulnerabilities inherent in customer login processes, the Verizon Business Data Breach Investigations Report found that more than 80 percent of hacking-related breaches involved brute force, whereby hackers use trial-and-error to guess login info, or through the use of lost or stolen credentials. Long gone are the days when a simple text password—coupled with a memorable word or the user's mother's maiden name—is considered a sufficiently robust defence against increasingly sophisticated hackers.

But to its credit, the industry is becoming increasingly aware of the risks that threaten the secure functioning of digital banking. According to a survey of 566 decision-makers in retail banking, fintech (financial technology) and merchant services commissioned by Visa and conducted by Forrester Consulting, 68 percent of respondents expressed concerns about fraud in mobile-banking payments, 60 percent in mobile wallets and 58 percent in peer-to-peer payments. However, 77 percent were ready to invest to meet these challenges head-on, while most respondents considered identity verification, data-privacy and data-theft management, and transaction monitoring as their top three fraud concerns.

What can banks do to resist these security risks successfully? Adopting an API (application programming interface) approach to deliver security services would seemingly help to achieve a more embedded security infrastructure, according to PwC (PricewaterhouseCoopers). “APIs in financial services are beginning to enable flexibility, customer choice through third-party, new product expansion, and new revenue streams—all key aspects for a digital bank,” the professional-services firm stated, whilst acknowledging that such a move would pave the way for industry standards such as OAuth, “which effectively empower banks to take greater ownership of customer data security, and bigger picture transformations such as a core banking to public cloud migration.”

Banks can also ensure that their staff are well trained so that they are equipped to spot potential security risks early and are sufficiently prepared to respond to them. This preparation should also ideally include an emergency plan that accounts for appropriate responses in various scenarios of the bank’s security being compromised, which employees can easily follow. And as far as customers are concerned, banks have a critically important role in communicating to them the appropriate security procedures that are in place and the security aspects of their accounts of which they ought to be aware.

Customers have a range of options at their disposal today to beef up their defences against cybercriminals. Multi-factor authentication (MFA), for instance, is proving to be highly effective. This means that, in addition to a regular text password, at least one additional form of identification verification is required before a customer can access his or her digital-banking account. Some of the most popular forms of verification include time-based one-time passwords (TOTPs) for logins, which typically involve codes being sent via SMS (short message service) or authenticator apps that expire after a short amount of time. Along with the normal password, therefore, the user must also have a mobile phone to receive the TOTP. With a hacker highly unlikely to also be in possession of the user’s mobile phone, therefore, this method greatly reduces the chance of the account being compromised. Other common forms of MFA tend to involve some form of biometrics, whereby fingerprint authentication or facial recognition is used to verify the user’s identity.

Additional measures that customers can consider include learning how to identify the scenarios during which they are most likely to be targeted by phishing scams, avoiding the use of public Wi-Fi networks when accessing their digital-banking accounts, periodically

updating their passwords and varying their passwords for different banking applications rather than using a single password for all logins.