Bank of America Merrill Lynch

Corporate Treasury Embraces Mobile Banking

Businesses gain confidence from advanced security tools

In recent years, smartphone ubiquity and the rise of tablets have transformed consumer behavior and fueled the breathtaking rise of the mobile economy. But while much of the consumer world has already transitioned to mobile, the business community has lagged behind.

When you consider the fact that mobile access to business apps such as corporate banking portals has been available for some time, it is somewhat surprising that treasury staff members still conduct most of their payments, account management and other functions on office desktops. This is largely due to heightened corporate focus on cyber security and concerns that mobile networks and devices are less secure.

The good news is that business reluctance to embrace mobile access to corporate banking portals is starting to change. Treasurers are beginning to see the benefits of allowing treasury staff members to access their company's corporate banking portals on their phones. These benefits can include greater efficiency, convenience and employee satisfaction. Thanks to advances in mobile security and evolving employee demand, more businesses are taking advantage of this growing opportunity.

Why treasurers are going mobile

An increasingly secure mobile ecosystem is one factor driving business interest and creating more confidence in mobile access. Mobile has similar security safeguards as a desktop environment, with the added bonus of built-in biometric authentication that requires a fingerprint or retina scan to unlock the device. This feature isn't widely available yet for office desktop computers. Biometric security actually enhances mobile device security, as it alleviates the risks of treasury employees using unsafe passwords and sharing the same passwords across multiple internet applications.

Mobile devices can also have enhanced malware detection capabilities, plus built-in protections known as "native security" meant to keep the device and data safe. One example is application "sandboxing," which prevents apps from accessing data between each other on the device, and creates boundaries that separate apps from the mobile device's infrastructure. This limits the ability of a "rogue" app to access data from other parts of the device (though these boundaries can vary across mobile operating systems). A newer type of fraud detection based on the user's behavior patterns is also evolving on mobile, potentially adding another layer of protection.

There are also several additional security checks that come with mobile access. For example, mobile apps and their creators are typically vetted by Apple, Google and the other "app marketplace" owners before the apps are made available for download. This review helps reduce malicious apps — and apps with potential security gaps — from reaching the public.

Another factor driving mobile adoption is evolving worker preference. Many of the same treasury employees who have already migrated much of their personal lives to mobile are starting to expect that same convenience in their work lives. The ability to work outside of business hours — untethered from the office — is an option that more treasury employees want and need. After all, many of these employees are already conducting their personal banking on mobile devices. In 2018, nearly two-thirds of adult smartphone users in America have installed at least one financial app on their devices,[1] and 70% of those who have installed a personal banking app use it at least once per week.[2]

The consumerization of business apps

Taken together, mobile security improvements and evolving employee preference are driving the "consumerization" of business apps. Many service providers are launching apps that can deliver greater speed, convenience and flexibility for their business clients across a wide range of functions, including Human Resources, Enterprise Resource Planning (ERP), payroll, supply chain and banking.

The mobile app version of our CashPro® portal demonstrates how greater security, employee preference and consumerization are converging. CashPro® Mobile has experienced 142% growth in users over the past year. Currently, 52% of users unlock CashPro Mobile with some type of biometric security. And it has recently received a consumer makeover — including modern screens, simpler navigation and timely notifications — while greatly expanding its capabilities.

Staying safe

Mobile access to your banking portal can be as safe as desktop, as long as you follow mobile security best practices and rigorously train your employees on appropriate mobile use. The following are examples of some best practices that companies should follow.

Many personal devices, including smartphones, are set up to automatically connect to open networks. Reinforce to your employees the importance of using business apps through only secure Wi-Fi or wired networks, ideally protected by a virtual private network (VPN). Never run sensitive apps on a public Wi-Fi, or other unsecured network. In addition to Wi-Fi, disable Bluetooth when not in use to keep cyber criminals from attempting to access your devices.

Remind your mobile users to install software patches and updates immediately once they are released, since these often address security gaps and reduce the likelihood of a breach. Your IT department should send reminders as soon as software patches and updates become available. It's also essential to require employees to create strong passwords. Where possible, employees should take advantage of biometric protection in a mobile device for even stronger authentication. Although convenient, avoid setting auto-logins, digital password keychains or "remember me" options on mobile devices.

Author
Mary Rosendahl
Director of Digital Channels
Bank of America Merrill Lynch

Discourage employees from "jailbreaking" or "rooting" their phones, since disabling the device's native security features in this way can make it more vulnerable to damage and malicious apps. Some apps — including CashPro Mobile — can help protect against this security risk by detecting when a phone is jailbroken or rooted and preventing access to the app and its data.

When deciding to install a new app on a personal or corporate mobile device, employees should research available apps, ensure authentic branding, check user reviews and download only from official app stores provided by Google, Apple or their corporate technology team.

In addition, beware of bogus messages sent by cyber criminals. Phishing emails can victimize unwitting mobile users if they're not careful, and cyber criminals have adapted the tactic to text messages, called smishing, which requires a new level of vigilance. The same discipline applies across both desktop and mobile: Users should not respond, click on links or open attachments in unfamiliar emails or text messages, since malware can infect both mobile devices and desktops.

Lastly, since by nature your employees will always keep their mobile devices with them, they should keep track of them just as they would a laptop. Establish a process for using a mobile device manager — or MDM — to remotely wipe sensitive data from a device that's lost or stolen.

[1] https://www.mobilepaymentstoday.com/news/study-consumers-find-themselves-engaged-with-mobile-banking-apps/

[2] https://www.bankrate.com/personal-finance/smart-money/americans-and-financial-apps-survey-0218/