THE NATIONAL CYBERSECURITY SOCIETY

Mobile Banking

It is reported our use mobile devices is outpacing desktop usage. According to a KPCB report, adults with access to digital media use mobile devices 51% of the time as compared to 42% for desktop usage.

These statistics are far from shocking. Many businesses are using tablets and phones to access customer data, charge for services or submit invoices.

Financial institutions seeking to remain competitive are offering mobile access to their customers. Checking on account balances, lines of credit availability and payroll apps are all services small business often leverage through mobile devices. Yet are these safe?

Did you know?

- √ Never login to your mobile banking app over public Wi-Fi
- √ Enable two-factor authentication for all banking transactions
- √ https://www.turnon2fa.com/tutorials/ - Check out this great resource to turn on two factor authentication!
- √ Don't use third party apps - like Facebook for your credentials to login. Create a separate login and password.

FACT 1: MOBILE BANKING RISKS

The Major Mobile Banking Risks

In some cases, your financial institution may assume the risk associated with mobile banking. These risks include malware, corrupt apps, flawed authentication, and lost or stolen devices. A business owner's risk of using mobile devices can occur when the device is not secured properly, lost or stolen, or used through an unsecure wi-fi connection.

Mobile Malware

Malware specifically targeting mobile devices has become a very real and prominent threat. Mobile malware can consist of viruses, Trojans, spyware, malware advertising and rootkits.

Unsecure Wi-Fi Networks

Free Wi-Fi is a coveted luxury for mobile device users. It can be found in restaurants, coffee shops, airports and many other public places. But when accessing free Wi-Fi, it is important to understand that the activity you are conducting may be visible to someone else. As a business owner it is your responsibility to inform and educate your employees not to access business apps via a free wi-fi connection.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Mobile Banking continued...

Hotspots may be spoofed by fraudsters. For example, your local coffee shop's network may be called "Tedscoffee". A fraudster can set up Wi-Fi at or near that location called "Tedscoffeee" -- to trick you into using that network. You are busy and don't notice that the new connection has a slightly different name.

According to the Financial Consumer Agency of Canada, "When using public Wi-Fi hotspots, you could also expose yourself to packet sniffers. Thieves using packet sniffers want your banking details and your personal information, such as your name, address or phone number. These personal details may be harmless on their own, but once they are combined, you can be at a higher risk for fraud".

Poor App Design, Configuration or Corrupt Apps

Using mobile apps for banking tends to be safer than logging in via your mobile browser. However, every mobile platform has unique characteristics that these apps must prepare for. Developers may not fully understand the risks associated with mobile banking and accidentally leave vulnerabilities open for fraudsters to exploit as a result.

Third-party apps open users up to a multitude of risks since these programs may leverage credentials from other applications — even if these apps have weaker security in place. For example, a shopping app could leverage your banking login information (username and password) to access your bank's services and facilitate a transaction.

Mobile Device ID Vulnerabilities

Many financial institutions work to gather the device fingerprint for each mobile unit the customer uses. This involves collecting information about the device, which is then stored in a system to identify the true customer from a potential fraudster. However, fraudsters are a dynamic bunch of bad actors and have developed ways of fooling device fingerprinting methods.

Remote Deposit Capture Fraud

Check fraud is not a new issue. In fact, it remains one of the biggest types of fraud within a financial institution. Remote deposit capture allows for users to snap a picture on their mobile device and deposit a check. While financial institutions have put rigid customer agreements and monitoring of this technology in place, fraudsters have found flaws in the system. For example, they have found ways to access the remote-deposit database, copied the images of thousands of checks and provided those reproduced checks to money mules to be moved out of the financial system.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Mobile Banking continued...

Overall, mobile banking is considered safe thanks to professional-grade encryption, user-end authentication measures and decentralized storage of sensitive information. Still, as a consumer, there are several measures you can take to keep your money and identity safe when banking from your smartphone, laptop or tablet.

Using mobile data is more secure than public Wi-Fi due to the encryption automatically applied to CDMA/LTE and HSDPA/3G based connections by mobile operators. Even if your financial institution is doing as much as it can to make mobile banking safe, you must do your part to protect yourself. Never log into your mobile banking app over public Wi-Fi and we recommend you use two-factor authentication **always** to login to your bank account.

And keep your phone updated to avoid being exposed to security problems.

ADDITIONAL RESOURCES:

- NCSS Weekly Cyber Tip: Mobile Banking
- https://www.techradar.com/news/networking/wi-fi/why-you-should-avoid-hotel-wi-fi-like-the-plague-1292555/2

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.