Security Risk Posed by Smartphones: Paying with Your Smartphone

Student's Name

Institutional Affiliation

Security Risk Posed by Smartphones: Paying with Your Smartphone

The advent of smartphones and information communication technology has had supplemental implications in highly conservative sectors such as banking. In the past, people used credit cards or cash to pay for goods and services. However, smartphones are slowly changing this as they have applications that allow one to make these payments without having to swipe one's card. Though the use of digital wallets has security challenges, these issues can be minimized. In addition to being safe and convenient, the risks of a digital wallet are significantly lower than those of cash and credit cards.

Placing one's cash or credit cards in a physical wallet can pose a challenge as one can misplace the wallet or forget it at home, limiting one's movement and purchases, and as such, inconveniencing an individual. Alternatively, someone might steal the wallet and use one's credit cards to make numerous online purchases (Wood, 2015). In most cases, the owner of the wallet bears the loss since suspects are often difficult to apprehend.

With a digital wallet, one is always assured of its convenience because people are more likely to notice when they have left their phones at home or in an establishment compared to when they leave their wallet. The payment system is also highly convenient for making miscellaneous transactions. While the threat of fraud has been linked with the use of digital wallets, smartphone manufacturers have responded commendably by incorporating encryption codes in the apps used to facilitate these payments hence protecting the user and their accounts from hackers and fraud (Wang, Streff, & Raman, 2012). The users of digital wallets are cautioned against relying on public Wi-Fi since hackers are known to plant malware, thus linking a victim's phone to theirs and consequently wiping their accounts.

In the case where one loses their phone, no one cannot access the device since it is password-protected and has other security measures such as screen lock requiring fingerprint access or voice recognition. One can use another phone with similar settings to report and close their accounts immediately, thus protecting their money (Raphael, 2020). In contrast, it is difficult to take security precautions against the loss of a physical wallet since the pickpockets have already caused significant damage by the time one realized the item is missing.

The other threat that some people associate with digital wallets is sensitive data such as bank information being accessed by hackers. However, one's information and data require one to be cautious when using their phone as they would use their computers at home or in the workplace. One should avoid suspicious emails, as hackers are known to use this method to implant malware in the phone and gain access (Raphael, 2020). Additionally, one is advised to avoid using one password or code in their security encryption. It will give criminals easy access since they will only need to know that one code to access and steal from you. Furthermore, one should avoid downloading applications that have a lot of free features as some of them collect sensitive data (Wang, Streff, & Raman, 2012). Users should always check which applications have access to their camera and messages.

The threat posed by using a physical wallet is higher compared to that using a digital wallet since one cannot predict the behavior of a thief who is afraid of being caught. In the case of a digital wallet, one can close or delete an account. Furthermore, it would be hard for a thief to access the account since it is encrypted and protected from malware. All the owner needs to do is practice caution when downloading content and using secure Wi-Fi to access their account. Thus having a digital wallet is much safer and convenient compared to a physical wallet as a means of payment.

References

Raphael, J.R. (2020, February 25). 8 mobile security threats you should take seriously. Retrieved from https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer*, *45*(12): 52-58. doi:10.1109/mc.2012.288

Wood, C. (2015). Why mobile wallets are safer than physical wallets. Retrieved from https://blog.capterra.com/mobile-wallets-are-safer-than-physical-wallets