**Mobile Devices and mPOS: Best Practices to Accept Payments**

Large organizations are now accepting payments through mobile devices. Customer-centric businesses like McDonald’s and Nordstrom’s have seen an increase in their sales after introducing Mobile Point of Sale (mPoS) systems. According to a research the number of mPOS installed worldwide will be 54 million units in 2019, four times the number of those in 2015. According to another research report by Juniper, one or more in three POS systems shall be mobile by the year 2021.

mPOS solutions are becoming popular because of their convenience and benefits like scalability capability, lesser transaction times, line elimination, and lesser dependency on cash. This, in turn, increases customer satisfaction which leads to an increased sales. Any form of data transfer, however, has risks associated with it.

a

Below are some common best practices to ensure that your mPOS experience is safe and secure:

1. **Become PCI DSS certified:** This is not only very important but a mandatory step to take when your company is dealing directly or indirectly with payment cards. PCI DSS is a set of 12 requirements that every merchant has to comply with to protect customer cardholder information. If a merchant does not comply, they can get heavy fine or even lose their merchant account. The PCI app security ensures that all companies that store, process or transmit cardholder data have taken all possible steps to keep this data safe from cyber criminals.
2. **Only Store Important Cardholder Data:** In case of service absence or delay, do not let the mPOS app store your data to be used at a later time. The longer it is in your mobile the risker. Disable the “store and forward” feature of your mPOS system.
3. **Do not Root or Jailbreak your Device:**

Rooted Android phones and jailbreaked iPhones give users the authority to install all kinds of applications without adhering to manufacturer restrictions and warnings**.**

1. **Keep your Operating System and Applications Updated**

Regularly updating your mobile operating system and applications to the latest versions enhances your security.

1. **Only Install Reliable Apps**

Never install applications from unknown or unreliable vendors.

1. **Use Antivirus for your Phone**

Install Anti-Malware / antivirus on your phone just as you do on your PC. Some reliable options for you to choose from are AVG, McAfee, Avast, Lookout, etc.

1. **Choose a Strong Password for your Mobile**

Avoid losing your critical data at the hands of a criminal in case your device is stolen or lost. Choose a strong password that is difficult to guess.

1. **Provide Training to Staff in mPOS**

To take full advantage of these best practices, educate and train your employees about how to keep data secure and follow best practices.