**Increased Usage of Mobile Devices in Africa Resulting in Greater Security Risks**

In June 2016, the Internet World Stats highlighted an internet penetration of only 28% in Africa, as compared to 89% in North America. This is because of limited availability of landlines in the entire African continent. However, this lack of connectivity is being filled in by a whopping increase in mobile device penetration in the continent. In fact, a survey done by Pew Research Center in 2015 showed that in some African countries, mobile phones were as commonly used as they are in the United States.

Conversely, knowledge ratio of security risks associated with mobile devices in Africa is very low, which is why companies that commonly send and receive confidential documents over mobile devices are particularly at risk, especially when it comes to sharing customer data on mobile phones.

Moreover, many customers choose to receive their bank statements, invoices and salary slips online via mobile, to be able to easily access them. This is why it is the responsibility of companies sending over such information to take all necessary steps for protecting customer data. But they can only succeed if the customer at receiving end is also knowledgeable about security risks and remains vigilant. In this context, the sender is responsible for encrypting sensitive documents while the receiver has to make sure that the device on which the confidential information is received has itself all security features installed.

Since the sender does not have any control over the device where he is sending information, it is better to assume that the receiver’s device is unsecured and all necessary steps are taken for encoding and encrypting the information. The company also needs to train and educate users regularly about secure mobile usage. In case confidential document is being sent through an application, make sure that it does not automatically sign the user in. As a user, it is important to set up a password or pin code for locking your device and be careful about the applications you download on your phone. Update your apps regularly and never allow apps to “store” your password.