

# **ACME FINANCIAL SERVICES**

**Powered by GLESEC**

## **CYBERSECURITY NEWS CUSTOM REPORT**

## Deal: Cloud And Networking Certification Training ~ Get 97% OFF

02/20/2020 03:08

# The Essential Cloud & Networking Certification Training Bundle



CCNA Routing & Switching Training



AWS Certified Solutions Architect - Associate



Implementing Microsoft Azure Infrastructure Solutions (70-533) Training Course



Graphical Network Simulator-3 (GNS3) Training



Advanced Microsoft Excel Training

Cloud computing and networking are two of the most significant areas of growth in the IT business. Companies need engineers who can maintain distributed software and keep the company connected.

If you want to work in either niche, the Essential Cloud & Networking Certification Training Bundle offers 93 hours of essential knowledge. You can pick up all 5 courses now for only \$39.99 via the THN Store.

This bundle focuses on the key skills and certificates the technical recruiters are currently looking for. It would be best if you came away with the knowledge to ace top exams, and the experience to handle real-world challenges.

First up, the CCNA Routing & Switching Training helps you master Cisco networks. Professionals with these skills earn around 9% more on average.

The AWS Certified Solutions Architect (Associate) covers the most popular cloud computing platform, showing you how to design, configure, and optimize cloud software. Implementing Microsoft Azure Infrastructure Solutions looks at similar skills on the other big platform.

This bundle also gives you access to Graphical Network Simulator-3 (GNS3) Training, which helps you gain experience in a digital environment. You also get a crash course in Microsoft Excel.

Each course includes a certificate of completion, and you get one year of unlimited access.

Worth \$1,957 in total, the training is now only \$39.99 with this bundle.

## 7 Ways to Improve the Security of Mobile Banking Apps

 S

02/19/2020 21:46

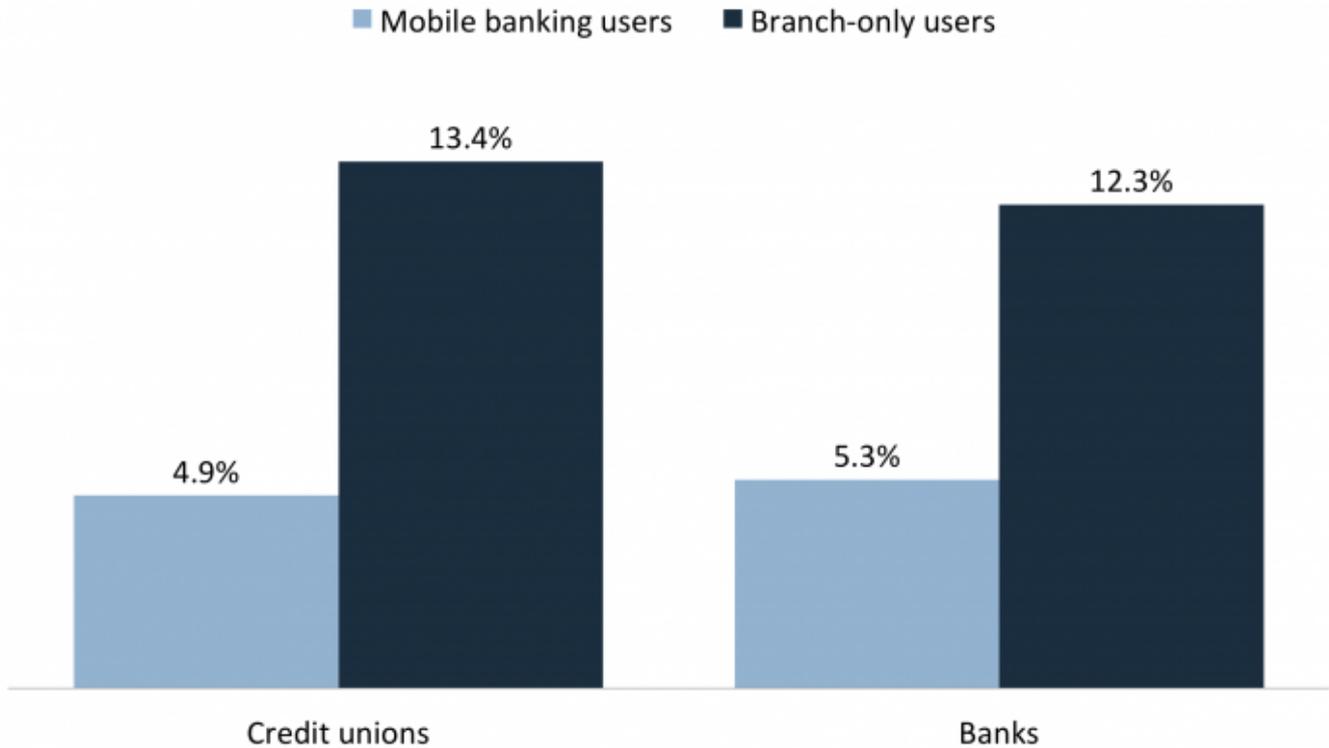
Scarlett Rose Feb 19 · 6 min read

When I wrote this blog, I presumed that most of us are always on the go! With the advent of mobile applications, and its amalgamation to various industries, be it investments, food ordering, bill payments or travel bookings, the majority of us are totally dependent on these applications for easy and quick solutions.

Today, a majority of the population is making use of online mobile banking apps for various things, however, the numbers are still lower than what you would expect! The question here is "WHY?" People work through their lives in order to generate a corpus. Losing it over a mobile application is the last thing they want!

## Mobile Banking Vs. Branch-Only User Attrition Rates

US credit unions, 2014-15



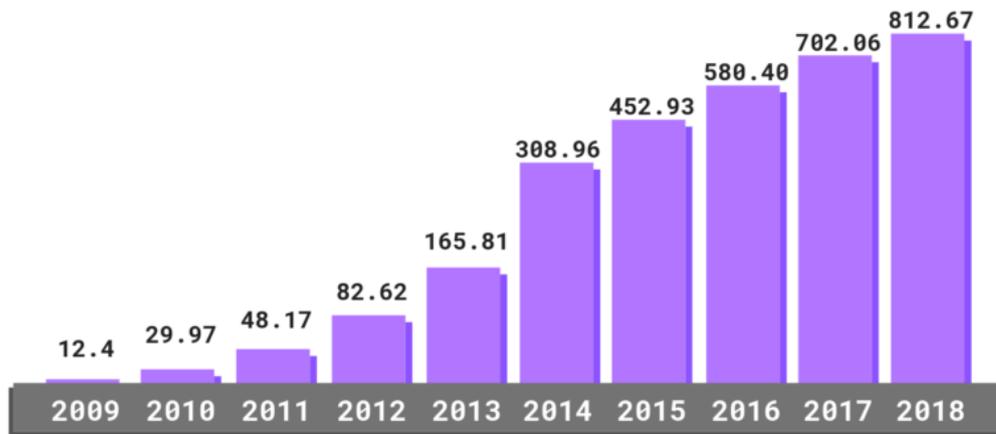
Source: Fiserv Mobile Banking Adoption White Paper

BI INTELLIGENCE

Source

Online mobile banking app security is of the most talked-about concerns that need to be addressed in order to achieve the expected number of mobile banking app users. The 21st century has been the pillar for innovations and digitalization. People across continents yearn for versatility and freedom to make transactions at any time of their convenience, regardless of the day, venue and device.

Yes, online mobile banking apps bring in a lot on the table for customers but then, at the same time, it also exposes you to the possibilities of threats and attacks, essentially slowing down the digital revolution.



Total Malware Infection Growth Rate (In Millions)

Source

Mobile applications are one of the primary targets for cybercrimes. With the growth in the demand for such applications, enabling payments at any time from anywhere, a lot of companies, providing mobile app developers are literally stretching the limits of safety, pushing users towards online threats.

**Did you know** — 98 percent mobile malware targets Android platforms.

Today, with technology being a pillar to every industry, there are multiple ways of winning over this problem. Here are the top 7 Ways to improve the security of mobile banking apps

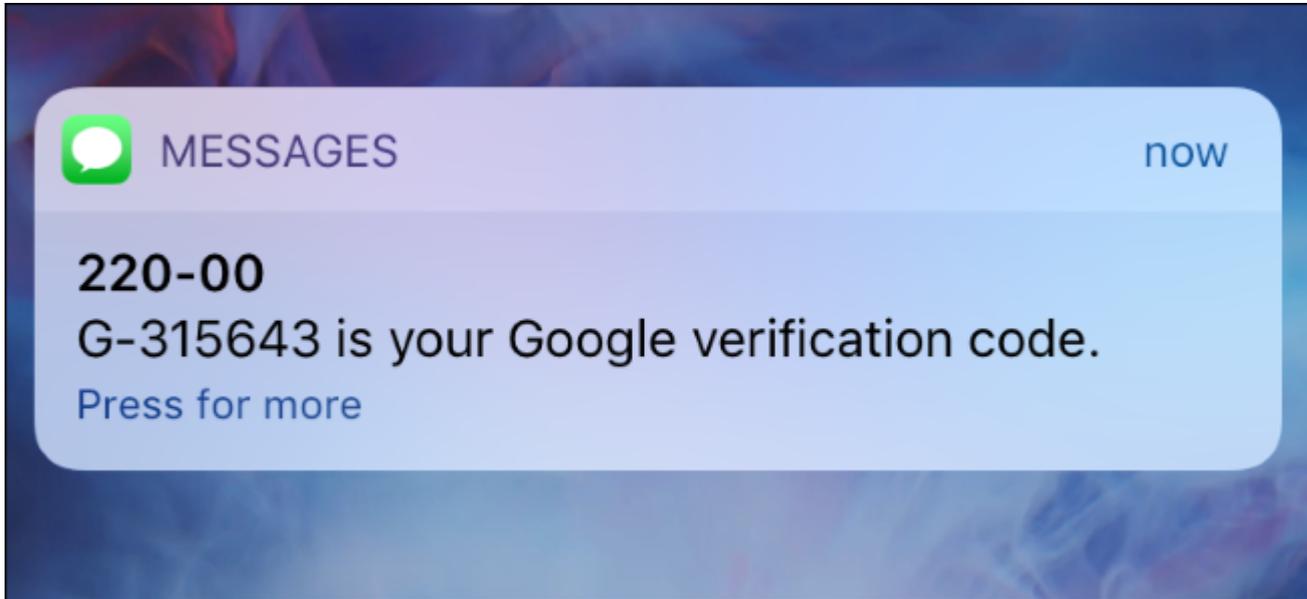
Mobile app development is a complex task. Optimizing the mobile app to its fullest potential and then, amalgamating it with organizations’ work process is not a child’s play! There are many issues you would come across trying to do so.

Every time you make an online transaction, there are many safe layers of data supporting different platforms. What this essentially means is that, whether you are working on android app development or iPhone app developers/ iOS app development, it is absolutely imperative to make sure that your app supports all platforms and devices.

Keeping the real-time-problems in mind, here are 7 ways to improve the security of mobile banking apps !

Why do we need a multifactor authentication feature? Today, this is the need of the hour because submitting a single password in order to access the customer’s bank details is a defense mechanism, that is no more up to the mark.

With the introduction of multifactor authentication, which is essentially an OTP or fingerprint, an additional defense layer is created, making it a lot safer.

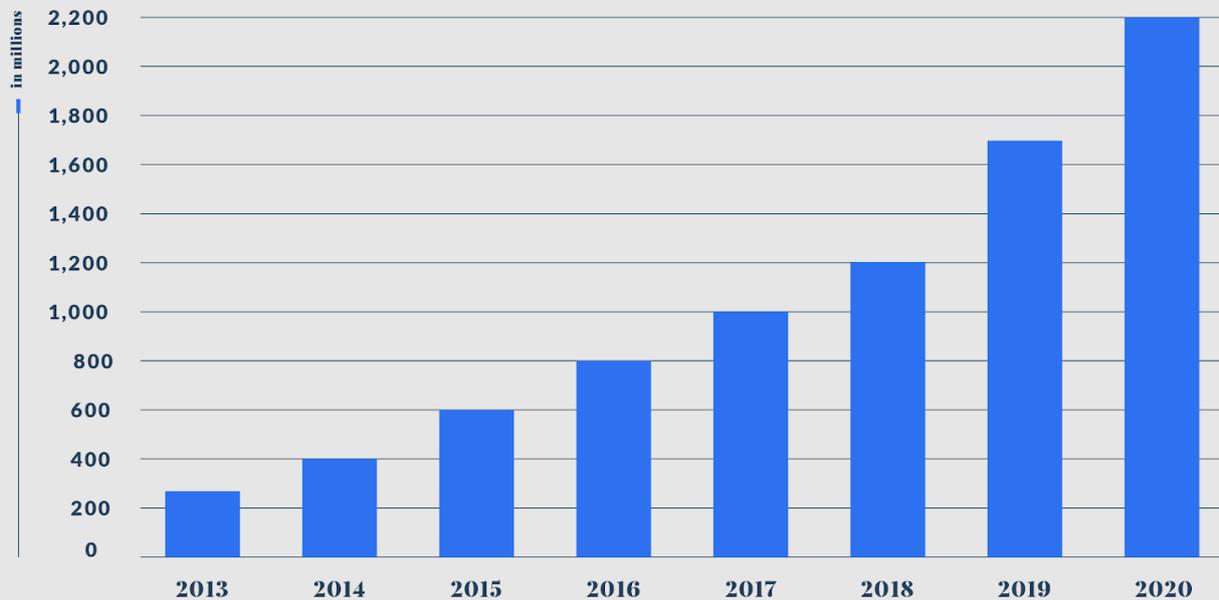


Source

Why NFC inserted sim cards? NFC embedded sim cards enable you to download all your credit card data from your credit card mobile app within their NFC sim card, securely.

How to secure mobile banking transactions? NFC inserted sim cards are safe and not only protects account data, but it also reduces the risk of compromising data and provides access to the application.

### SHIPMENTS OF NFC-ENABLED MOBILE HANDSETS

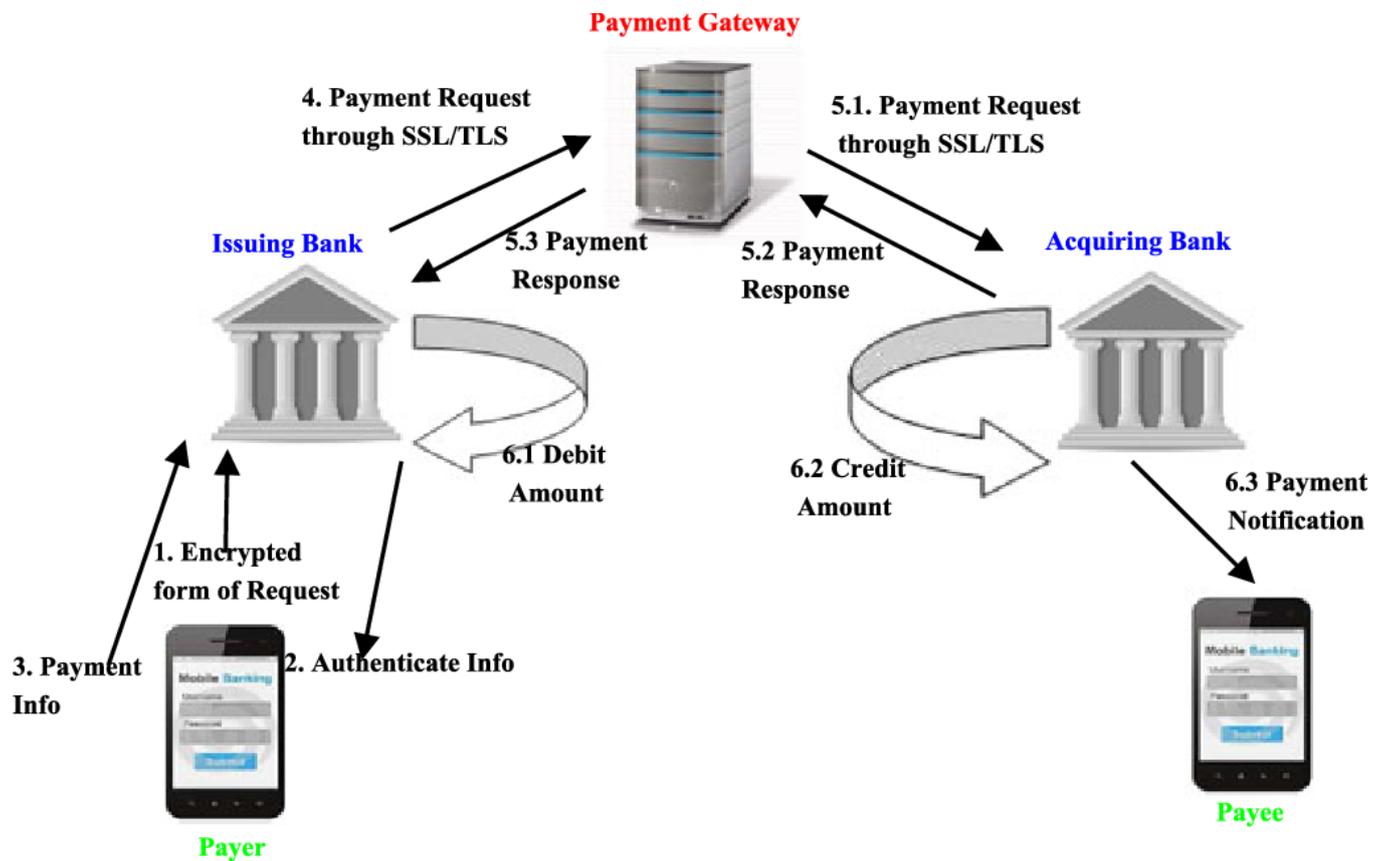


Source

In a digital transaction, various bodies such as the merchants, card brands, and various banks have different roles to play! Do you know, every year, sensitive data worth billions are exchanged.

It is not incorrect to say that transactions made online act as hotspots for cybercrimes and criminals. As we know, end to end encryption makes transactions a hell lot safer, this is one of the best solutions to avoid such cyber threats.

End to end encryption essentially does major checks and tests, taking safety measures to the next level.

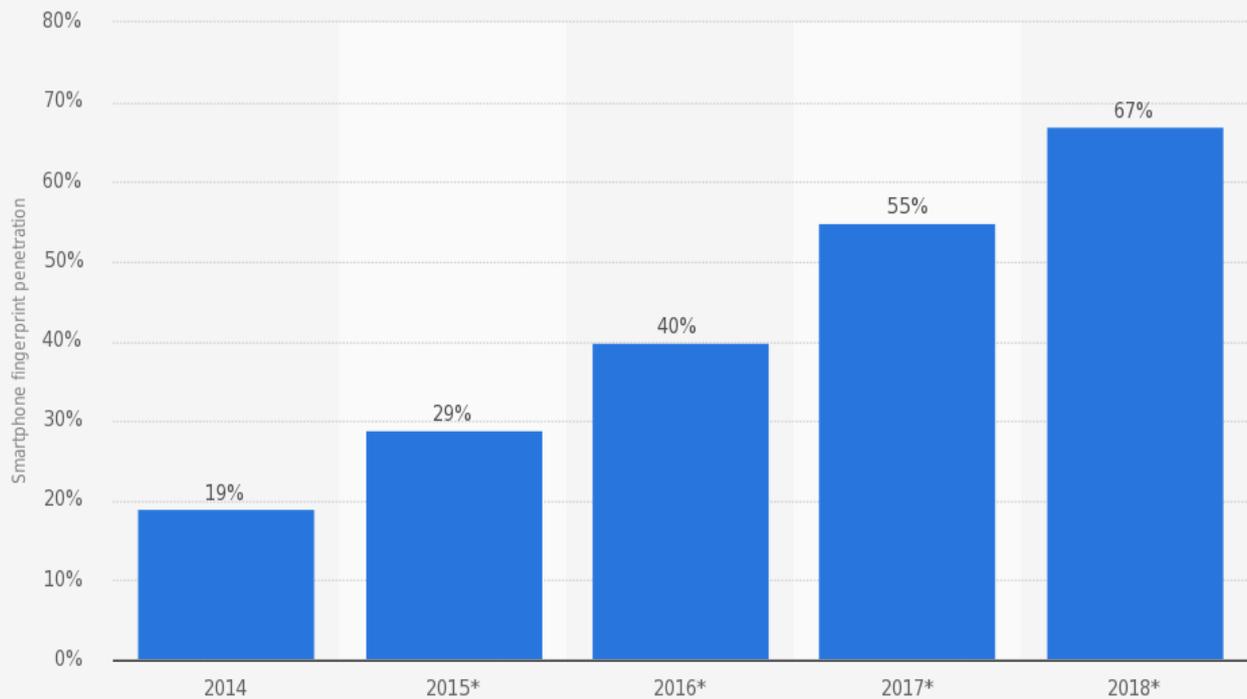


Source

Here is another feature talking about how to secure mobile banking transactions! The 21st century is all about smartphones. With the amalgamation of fingerprints in smart devices, online mobile banking apps have found another layer of security. The fingerprint scanner enables the device to get access to vital information such as IP address, location, type of device and time of transaction.

Are you looking to hire mobile app developers from mobile application development platforms? Make sure the app company you decide to work with have the potential to develop your app with such features,

### Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018



Source:  
Credit Suisse  
© Statista 2016

Additional Information:  
Worldwide, Credit Suisse

statista

Source

The logic is straight and simple. If you are using a mobile banking app, it is obvious that you have access to text messages and email. The powerful real-time notification feature enables the customer to receive notifications on the spot, helping them easily avoid frauds.

As an example, every time you swipe your card, you do receive an SMS telling you that such an amount has been debited from your account. If it's you, cool. If not, you can report fraud and get your money back.

Essentially, these on the spot notifications allow users to find out if their account is under attack while guiding them to take the necessary steps.

## Alerts and push notifications (2010-2019)



Source: Javelin Strategy & Research

CreditCards.com

Source

Just like all the other sectors, technology today has successfully transformed most of the banking sector as well. Today, with the advent of digitalization, banks are going paperless in terms of a lot of processes.

Now, opening a bank account and managing transactions is also paperless. Digitalization in this sector has led to more transparency and higher efficiency. How? Today majority of the files are in the digital form which is accessible from anywhere

Today, banks are looking for mobile app solution providers who have the potential to provide them with enterprise mobile solutions, which are custom made and are of high security.

Read more — Paperless Banking



Source

Today, with the advent of technology, the market is equipped with custom-made software solutions, that are so feature-packed that it's no big deal to analyze activities, login locations and account activities of users.

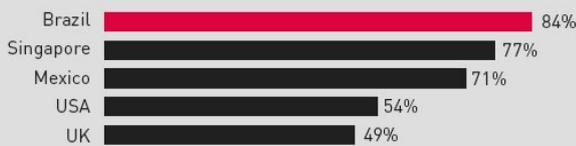
The best thing about this feature is that it flags unusual behavior or locations for further validation, helping avoid frauds.

Further investigation could be in the form of email or texts informing them of suspicious activities.

**Trust and security are issues to be addressed**

**67%** Are concerned about the security risks of using their mobile device for banking

Breakdown by country:



If users felt the app security was poor:

**48%** would switch banks

**38%** would just use the basic features

Source

With technology developing continuously, mobile apps have made banking as easy as ordering food. However, there is still the risk of being vulnerable to cybercrimes.

It is absolutely imperative to incorporate the above mentioned online Security of mobile banking applications in order to fight the big challenge, i.e, being prone to frauds.

In the end, I'd suggest that you get in touch with mobile app development companies, and ask them how to secure mobile banking transactions and make sure they incorporate the above-mentioned features in your app. All the best.