CASE STUDY

**NAME OF CASE STUDY: GOOGLE PAY SECURITY**

**SUBMITTED BY: PATHAN NAZIYA ASHRAF**

**ROLL NO: 60**

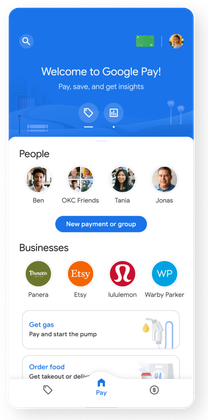
**SUBJECT: CYBER SECURITY ESSENTIALS**

**CLASS: B.SC.-II COMPUTER SCIENCE(ENTIRE)**

* INFORMATION:

**GOOGLE PAY Details-**

**Google Pay** (stylized as **G Pay**; formerly **Android Pay**) is a [digital wallet](https://en.wikipedia.org/wiki/Digital_wallet) platform and [online payment](https://en.wikipedia.org/wiki/E-commerce_payment_system) system developed by [Google](https://en.wikipedia.org/wiki/Google) to power in-app, online, and in-person [contactless purchases](https://en.wikipedia.org/wiki/Contactless_payment) on mobile devices, enabling users to make payments with [Android](https://en.wikipedia.org/wiki/Android_(operating_system)) phones, tablets, or [watches](https://en.wikipedia.org/wiki/Smartwatch). Users in the [United States](https://en.wikipedia.org/wiki/United_States) and [India](https://en.wikipedia.org/wiki/India) can also use an iOS device, albeit with limited functionality. In addition to this, the service also supports passes such as coupons, boarding passes, campus ID cards, car keys, event tickets, movie tickets, public transportation tickets, store cards, health records, and loyalty cards.



* About Google Pay

Google Pay is a way for merchants to accept quick and easy mobile payments for physical goods and services everywhere you do business, including in stores and online.

Customers add credit and debit cards to Google Pay. When they use Google Pay to make a purchase, the buying process is faster and easier than ever for you both because Google Pay stores and transmits the relevant customer details, all with a simple tap of their device in stores or the tap of a button in your mobile app.

1. Accept Google Pay in stores



Customers must "wake" their device in order to tap and pay. For some large purchases, they will be required to unlock their device as well. Google Pay processes their transaction using credit and debit cards they’ve previously added to Google Pay. Google Pay does all the heavy lifting and users don’t even need to open the app — they simply tap and pay.

After their purchase is complete, customers see a payment confirmation on the point-of-sale terminal and get transaction details directly on their mobile device.

2)Accept Google Pay for transit

For transit agencies that support contactless payments, the experience is similar to in-store payments. Customers tap their phones near the contactless NFC terminal on the transit gate or turnstile to open the gate. Their fares are charged at the end of each day.

Transit agencies can also use Google Pay for mobile ticketing with contactless cards. Transit agencies that integrate with Google Pay allow their users to:

* Create a digital transit card
* View balance and other ticket information
* Pay for rides in-app

3)Accept Google Pay online

Google Pay API lets customers check out in your app or website. When you integrate with the Google Pay API, customers can pay you with any credit or debit card in their Google Account, including cards saved to Google Pay.

* **BENEFITS OF GOOGLE PAY:**

Google Pay is one app that provides you with many ways to make your customers’ buying experience faster, more convenient, and more rewarding. Google Pay’s powerful-yet-simple suite of mobile payment integrations helps you connect with customers to drive sales and brand loyalty. Get started now and tap into millions of Android users in just a few steps.

2)Merchant benefits

Here are some of the benefits merchants enjoy with Google Pay:

* Easy online integration: The simple [Google Pay API](https://developers.google.com/payments/) helps you get up and running in no time. Backend or server-side work depends on your payment processor and desired method of implementation, but is typically minimal.
* Increased sales: Faster, easier checkouts in stores can lead to more store visits, more time spent shopping, and customers spending more money. When customers use Google Pay to make purchases online, they aren't redirected to a third-party site and stay within your checkout flow for the entire transaction. Google Pay not only saves customers time and effort but can lead to higher cart conversions for merchants.
* Traffic, brand affinity, and engagement: When customers save your pass through the [Google Pay API for Passes](https://developers.google.com/save-to-android-pay), merchants build brand affinity and engage with customers more intimately and more often. Google Pay API for Passes will even notify customers to use these passes when they’re near store locations, or notify them about their upcoming flight or event.
* No transaction fees: Merchants don't pay extra fees when customers use Google Pay to make purchases.
* Enhanced security: Google Pay’s [card tokenization](https://support.google.com/pay/merchants/answer/6345242) helps reduce merchant risk and exposure to fraud.

3)Customer benefits

Customers enjoy a better experience when they choose to buy with Google Pay, such as:

* Fast and easy purchases wherever they buy: In stores, customers speed through checkout when they use Google Pay on their mobile device to tap and pay.
* No cost: Google Pay is a free mobile app available in the [Google Play Store](https://play.google.com/store). Customers don't pay extra transaction fees when they use Google Pay to make purchases.
* Peace of mind: When customers use Google Pay to buy in stores, Google Pay doesn’t send their actual credit or debit card number to make the payment. Instead, it uses a virtual account number to represent the account information.

4)Security benefits

Google Pay’s tokenization process offers notable security benefits to both merchants and customers:

* Device lock screens, remote device wiping, and tokenized card numbers: Customers enjoy protections from loss or theft of devices containing token information.
* Easy integrations: TSPs and Google Pay do the heavy lifting when it comes to tokenization, making the integration with Google Pay simple for merchants.
* Reduced merchant risk: The tokenization process means less sensitive customer information for merchants to have to store, reducing your exposure and worries about data breaches.
* How payments work

Here’s how payments work when customers use [**Google Pay**](https://support.google.com/pay/merchants/answer/7137717) in stores and online.

Payments in stores

Google Pay gives customers fast, hassle-free checkouts and, at the same time, peace of mind that Google stores their data with multiple layers of security. Also, Google Pay does not send merchants their customers' actual card numbers when they pay in stores; instead, Google Pay facilitates a process called tokenization in which a [**token**](https://support.google.com/pay/merchants/answer/7151223) stands in for a customer’s actual credit and debit card numbers.

In order to complete the tokenization process, Google Pay works with:

* Mobile device manufacturers
* Payment terminal providers
* [Payment networks](https://pay.google.com/about/banks/)
* Token Service Providers (TSPs)
* [Card issuing banks](http://pay.google.com/intl/en_no/about/banks/)

Together, Google Pay and these organizations work to build the tokenization infrastructure so that the:

* Customer verifies their identity when adding a card to Google Pay (ID&V)
* Customer’s mobile device securely stores their tokens
* Google Pay app transmits tokens to the payment terminal during in-store transaction
* **GOOGLE PAY API TERMS OF SERVICE**

**Section 1: General Obligations**

**Section 2: Permissible Payment Transactions**

**Section 3: Use of the Google Pay API**

**Section 4: Prohibited Actions**

**Section 5: Data Privacy**

* + **End User Personal Information**
  + **Independent Controllers**.

**Section 6: Data Security**

* + - **Safeguards**.
    - **(b) Access Controls**.
    - **(c) Data Protection**.
    - **(d) Security Incident Response Program**.

**Section 7: Taxes**

**Section 8: Co-Marketing Agreements**

**Section 9: Governing Law and Arbitration**

* **Is Google Pay secure?**
* Theoretically, yes. When you're paying in store, Google said Google Pay doesn't share your actual card details. Instead, the merchant receives a unique encrypted number. Google worked with leading payment networks and financial institutions to deliver industry-standard security tokenisation. With tokenisation, the retailer receives a 16-digit number instead of your account number.
* As a result, Google Pay's tokenisation is different from Apple Pay's in that tokens aren't generated in a secure chip within the phone but rather within the cloud. Still, if you should ever lose your phone, Google recommends using [Find My Device](https://accounts.google.com/ServiceLogin?service=androidconsole&passive=1209600&continue=https://www.google.com/android/find?u%3D0&followup=https://www.google.com/android/find?u%3D0&ltmpl=findmydevice&rart=ANgoxcez6bLWwOYhO29OJ9oO3LjDWgEN3sqrvhAS-JjDiYP56qxgBqDLW_S3QFUWZaQn9JhaAPTCLy2EBqkY0IeGfRt6B1cFQA&authuser=0) to find or erase it in order to keep your local data safe from prying eyes. However, Google Pay does accept a PIN code, password, or pattern to authenticate transactions

## **Chargeback Alerts**

Our award-winning chargeback alert networks are guaranteed to prevent chargebacks.  [Alerts](https://www.chargebackgurus.com/blog/a-merchants-guide-to-chargeback-alerts) alone will stop 25% of your chargebacks - giving your team time to address disputes and prevent them from becoming costly chargebacks.



* **Can Google Pay Be Hacked?**

While it is theoretically possible, it is practically impossible due to the encryption and tokenization used. The real risk is not on Google's end, but on yours. Your login information is the easiest point of entry and should be protected carefully.

**Can You Get Scammed Through Google Pay?**

Yes. Sellers can be scammed by fraudsters using methods like sending a fake screenshot of a payment in order to get the seller to send the item, and buyers can be scammed by sending a direct payment to a fraudulent seller.

* **What to always keep in mind?**

Google Pay has provided certain guidelines that you should always keep in mind.

* Your UPI PIN is only needed to send money and check balance. Receiving payments needs no PIN. In case someone asks you to enter your PIN, it means you are approving an outward payment, i.e. a payment from your bank account.
* Never share the OTP you receive to log into your Google Pay account.
* Never make a financial transaction — be it a recharge, bill payment, or anything else while distracted.
* Never do it under pressure with someone on the phone line.
* Never share sensitive personal details on social networking sites.
* Never transfer funds without confirming a person’s identity.
* Never use screen sharing apps when you make a transaction.
* **Some helpful tips to make your Google Pay payments safe:**

|  |  |
| --- | --- |
| https://lh3.googleusercontent.com/ClS65wisgLl40vIDtF9IRXhR0bneTHrFrlBv6Mc6WLgQ6SUIfeddE5BvmLl8j7E33w=w48 | Keep your UPI PIN secret: Your UPI PIN is just like your ATM PIN. Never share it with anyone. |
| https://lh3.googleusercontent.com/wXzv1bj2sH1v0w-pzFGV2EJnmvidxNPS56FsW28KsR8rPUwTeFP1an-7pk_irRF5YVQ=w24 | Keep your Google Pay log in OTP a secret. Do not share it with anyone. |
| https://lh3.googleusercontent.com/YXkeaW4h3lC8dVHd4UMwYfdnA13RThL1FMM6YsRXu8UfX3VWZBoLatanfYHxINtxOSg=w48 | Only download[trusted apps](https://support.google.com/accounts/answer/6010255?hl=en): Harmful apps like [screen sharing apps](https://support.google.com/pay/india/answer/10768310/beware-of-screen-sharing-apps) can access personal information that you enter on your screen. |
| https://lh3.googleusercontent.com/RXdcJQUMMX_ifiG3TsUhrNp7JQG5jh2NfZ5u3MCtiPQfDo39DIMUAg9mesD4pTK11A=w48 | Be cautious of sharing your UPI PIN on websites or forms sent to you via a link. |
| https://lh3.googleusercontent.com/QOh2ez1YTE6jcJq8lUl6aoBG7x_VDjtGB1yABAtEwpyPdAval0T6Yq4xvntnquhNQ80=w48 | You don't need to enter your UPI PIN to receive money: Entering your UPI PIN means you are paying someone. Pay attention to which direction your money is moving. |
| https://lh3.googleusercontent.com/qzRyD-PZJ6MMMREZTvXdwRkpzFnO3A3nE30SF9rmPgSpAQ1Zqygj8KuFtyK7dGJ_9g=w48 | Only use your payment app to reach [customer care](https://support.google.com/pay/india/answer/7562363): Find genuine support details in the Help/Support section  of your Google Pay app. Avoid untrusted numbers which may be listed on the Internet. |

* **What to do if you are a victim of a fraud transaction?**

Instantly report any irregularities in your transactions to your bank and the government’s Cyber Cell. We recommend you to do the following if you suspect fraud on your Google Pay transaction:

* Report transaction to your bank
* We suggest you reach out to the cyber crime police department in your local jurisdiction.
* Please use this [form](https://support.google.com/pay/india/contact/report_activity) to report it to us. We will evaluate your request against our policies and take action accordingly.
* Protect your Google Pay information

Google Pay protects your information using Google Pay's collection of top security features that help detect fraud, prevent hacking and protect your identity.

Your Google Pay information is stored on secure servers in a safe location, and our team monitors it at all times.

Important: If you think that there’s been a case of fraud or unauthorised activity in your account, [contact us](https://support.google.com/pay/india/contact/report_activity) to report it immediately. You should also contact your bank to dispute any charges from the unauthorised activity.

Spot suspicious calls, emails & requests

Below are ways that someone might fraudulently ask for personal information or access to your account.

Note: You’ll never get a direct call from Google unless you filled out a form or requested a call back from an agent.

* **Phishing:**

Phishing is when someone pretending to be someone else (for example, someone pretending to be a Google Pay customer care agent) asks you for personal information.

To spot a phishing attempt:

1. Check what information they’re asking for. Google won’t ask you to share personal information like payment account numbers, PINs or passwords over email.
2. Find out if the email address is fake. (See 'Spoofing' below.)

* **Spoofing:**

Spoofing is when someone fakes the identity of the email sender so it looks more trustworthy. Here’s how to see more details about the sender of an email.

1. In Gmail, click the drop-down next to the 'Reply' button and click Show original.
2. Make sure the 'From' address and the 'Reply to' address match.
3. Check that the address on the 'Message-ID also matches the 'From' address domain.

If you don't use Gmail, ask your email host for details on how to verify a sender.

Fraudulent money requests

When someone sends you a request for money, check to make sure that you know the person asking for it.

**Set strong account and device security measures**

* To make it hard for other people to use your account, you’re asked to set a Google PIN when you get started with Google Pay. If you don’t think that your Google PIN is strong enough, [you can change it](https://support.google.com/pay/india/answer/7296044).
* Make sure that you set a strong UPI PIN that only you know, and which cannot be easily guessed. Keep these PINs private and don’t share them with anyone.
* Using a screen lock (such as a pattern or a PIN) on your phone can help protect your information if your phone gets lost or stolen.
* **What should you do in the case of digital fraud?**

Sujay Vasudevan, Vice President, Cyber & Intelligence Solutions (C&I), Mastercard said that along with the application of best-in-class technology to prevent fraudulent transactions, the onus of keeping one's money safe lies with both - the banking and payment entities and the individuals. "Therefore, you need to be vigilant and stay guarded against fraudsters and avoid sharing confidential details like PIN, OTP etc. to keep your money safe,"

* **Some ways to protect yourself from fraud on UPI apps such as Google Pay**
* **Beware of engaging with fraudsters**
* **Be alert to transfer requests on UPI**
* **Limit third-party access to your mobile screen**
* **Counterfeit UPI apps galore**
* **Avoid fake helpline numbers on social media**
* **Moneycontrol's Take**
* **Different arrow directions for paying, receiving**

