Your Money: Mobile Wallet

What is a mobile wallet?

Mobile wallet is an app on your smart phone or watch that stores your credit card, debit card, and bank information —then allows you to make purchases with merchants (stores, restaurants, or other places that sell things for you to buy). The mobile wallet app subtracts the money you spend from your credit card, debit card, or bank account.

Different types of mobile wallets apps match different types of smart phones. Most common mobile wallets apps are Apple Pay, Google Pay, Samsung Pay, and Android Pay that may be installed on your smart phone. You can download other mobile wallet apps from banks such as Wells Fargo and Capital One. Also, you can download mobile wallet apps from merchants such as PayPal, Walmart, and Starbucks. Your mobile wallet app only works with merchants that accept the app as payment method.

What are the benefits of a mobile wallet?

Mobile wallets are easy to use for people who like to use smart phones. You do not need to carry your plastic credit or debit cards in your purse or wallet when shopping because the information is installed on your smart phone. When you are ready to pay, you: a) Unlock your phone. b) Type the pass code or use your fingerprint to unlock the mobile wallet. c) Touch your phone to the "mobile wallet reader" next to the register. The mobile wallet and reader use NFC (Near Field Communication) to electronically communicate information to each other.

How do I set up a mobile wallet?

a) Select the mobile wallet app you want to use. b) Open the app and add each credit card, debit card, or bank account that you want to store in the mobile phone app. You may use your phone camera to scan the card, or enter information using the keyboard. c) Set "default" payment option. Even though all your plastic cards and bank accounts are stored within the mobile wallet app, you need to select the "default" payment option — the one card or account that will be the one used to process the purchases you make.

Are mobile wallets safe? Yes and No

Yes. Plastic credit and debit cards print your name and account number on the card. Mobile wallet apps "encrypt" your banking information before sending the information electronically to your bank. Encrypt is an electronic process that changes your information into a scrambled unreadable code. Also, you need to keep your mobile wallet app updated to the newest version for safe use.

No. You can use your mobile wallet when your phone has battery life. If your battery runs out of power, your mobile wallet stops also.

Yes. When your phone is locked, your mobile wallet is safe. The mobile wallet app can process payments only when your phone is unlocked with pass code or your fingerprint. If you use pass code, you need a STRONG pass code. The best way to keep a criminal out of your phone is to require a 2-step unlock — strong pass code with "biometric" authentication. Fingerprint, facial, or iris (eye) scan on a smart phone is called "biometric" (or body) authentication.

No. In 2017, hackers found a way to pass Samsung Galaxy 8's iris scan with a person's photo and contact lens. Hackers are trying ways to pass biometric authentication on other types of smart phones and watches.

No. Studies prove only 40% of smart phone users keep their phone locked. Criminals may "shoulder-surf" when you are the cash register to see you enter your pass code, then steal your phone. What do you think happens when your unlocked phone is stolen, and your pass code is known from a shoulder-surf?

No. If you add your credit card, debit card, or bank information using public Wi-Fi network, hackers can grab the information, then "spoof" or re-create your mobile wallet and quickly use it to purchase stuff.

No. Your smart phone can become infected with malware that will steal pass codes and information. Malware enters your phone when you click on infected advertisement or fake e-mail link sent by criminals.

What do I do if my mobile wallet phone or watch is stolen or lost?
1) Immediately report the theft or loss to your wireless carrier. Your carrier may be able to disable your phone. 2) Immediately report the theft or loss to your bank so that your bank can freeze your accounts to stop all transactions (purchase money flow). 3) If your phone is stolen, report the theft to the police and get copy of the report. Some wireless carriers or banks require proof that your phone was stolen, and a police report can provide proof.

QUICK CHECK:

1. a) What is a mobile wallet? b) Money you spend is subtracted from what 3 places?
2. List 3 common mobile wallet apps.
3. a) Why do you not need to carry your plastic cards when shopping? b) List the 3 steps to use when you are ready to pay with mobile wallet.
4. a) What do mobile wallet and reader use? b) To do what?
5. a) List the 3 steps to set up the mobile wallet app. b) What is a default payment option?
6. a) What is "encrypt"? b) Why do you need to keep your mobile wall app updated?
7. What happens if your phone battery dies?
8. When can a mobile wallet process payments?
9. a) What is best way to keep a criminal out of your phone? b) What is called biometric authentication?
10. What did hackers find a way to do in 2017?
11. a) What percent of phone users keep their phone locked? b) Do you keep your phone locked?
12. Why do criminals shoulder surf?
13. What happens if you add your bank information when using public Wi-Fi network?
14. When does malware enter your phone?
15. When mobile wallet phone is lost or stolen, what 2 things do you IMMEDIATELY do?
16. a) If your mobile wallet phone is stolen, what else do you do? b) Why?
17. a) Will you use plastic credit card or mobile wallet when shopping? b) Give a reason for your answer.

Your Money: Mobile Wallet
QUICK CHECK ANSWERS:

1. a) App on smart phone that stores credit card, debit card, and bank information, then allows you to make purchases with merchants.
   b) Credit card, debit card, bank account.
2. Student's choice of 3 mobile wallet apps.
3. a) Because the information is installed on your smart phone.
   b) Unlock phone. Type pass code or use fingerprint to unlock mobile wallet. Touch hour phone to mobile wallet card reader.
4. a) NFC (or Near-Field Communication).
   b) To electronically communicate information to each other.
5. a) Select mobile wallet app. Open app and add credit card, debit card, or bank account. Set default payment option.
   b) The one card or account that will be the one used to process the purchases you make.
6. a) Electronic process that changes your information into a scrambled unreadable code.
   b) For safe use.
7. Your mobile wallet stops.
8. When your phone is unlocked.
9. a) Require 2-step unlock.
   b) Fingerprint, facial, or iris (eye) scan on smart phone.
10. Pass Galaxy iris scan with person's photo and contact lens.
11. a) 40%.
    b) Student's answer.
12. To see you enter your pass code.
13. Hackers can grab the information, then spoof or re-create your mobile wallet and use it.
14. When you click on infected advertisement or fake e-mail line sent by criminals.
15. Report theft of loss to wireless carrier. Report theft or loss to your bank.
16. a) Report theft to police and get copy of report.
    b) Police report can provide proof.
17. a) Student's answer.
    b) Reason for answer.