Digital Wallets

Leave your wallet at home.

What are they?

A digital wallet is a virtual wallet that stores payment information on a mobile device or online. Bank account, debit card and credit card information is stored and can be used for online or in-store transactions. Digital wallets offer a more convenient and secure way to complete transactions when compared to traditional payment methods. In addition to payment methods, digital wallets can store the following items:

- Membership cards
- Plane tickets
- Driver's licenses
- Loyalty cards
- Gift cards
- Hotel reservations
- Event tickets
- Coupons

Often the terms “digital wallet” and “mobile wallet” are used interchangeably, but they do slightly differ.

A **digital wallet** is a virtual wallet that can be accessed on a desktop computer, laptop or mobile device.

A **mobile wallet** is a type of digital wallet that is available on mobile devices. Mobile wallets store payment information and facilitate contactless transactions at physical locations.

Some examples of digital wallets are Apple Pay, Google Pay, Samsung Pay, and Garmin Pay. Although there are many types of digital wallets, some are dependent on the phone being used. For example, Apple Pay cannot be used on an Android phone. However, the Pay Pal, Cash App, Venmo and Zelle apps are available for download from both the Apple and Google Play stores.

How do they work?

Most digital wallets have an app that can be downloaded onto a computer, phone, watch or other smart devices. When making a purchase, the transaction can be completed by holding your device near a terminal that has the contactless transaction symbol.

The technology behind digital wallet transactions can include:

- **QR Codes** –The device’s camera scans the QR code and the digital wallet's scanning system initiates payment.
- **Near-field Communication (NFC)** – NFC enables the transfer of information through short-range wireless technology between two devices.
- **Magnetic Secure Transmission (MST)** – MST allows mobile devices to mimic the swipe of a magnetic stripe of a physical card. This action is simulated and emitted by the smartphone to the payment terminal.

Are they secure?

Accessing a digital wallet involves authentication layers, such as requiring a PIN or biometric information such as fingerprint or facial recognition.

For an additional layer of security, a screen lock password can be added to mobile devices.

Digital wallets themselves offer enhanced security compared to traditional wallets due to features like **encryption** and **tokenization**.

Encryption is used to secure sensitive information, such as personal or card details. When information is added into a digital wallet it is converted into a unique code via encryption that can only be accessed by authorized entities.

When making a payment, the encrypted data is securely transferred. The data is not able to be deciphered without the decryption key, which prevents unauthorized entities from retrieving sensitive information.

Tokenization is another security measure used in digital transactions. When a payment is initiated using your digital wallet, one-time-use tokenized card information is sent to the merchant instead of sending your actual credit or debit card details (debit or credit card number, expiration, and CVV). The token is used to process the payment, while your personal information remains secure. Tokenization minimizes the risk of debit or credit card information being stolen in a data breach.

Pros and Cons of Digital Wallets

Pros

- Digital wallets provide additional security by limiting exposure of financial and personal information.
- Data encryption and tokenization can make digital payments safer than traditional debit or credit card transactions.
- Using a digital wallet can reduce the amount of items necessary to take to a store. This helps reduce the chance of losing an item since less is being carried.
- Availability of digital wallets gives people in underserved areas additional payment options.

Cons

- Not all merchants accept payments through digital wallets.
- If Bluetooth or Wi-Fi are unavailable, digital payments may not work.
- If an internet setup or electronic point-of-sale network are not functioning, it may not be possible to pay using a digital wallet.
- If a mobile device is stolen and is not protected by a password or biometric data, or if a digital wallet is hacked, personal and sensitive information could be obtained.

If a mobile device is lost or stolen, owners can use apps to remotely lock or erase the device's data. Device security can be increased by using these apps and by setting up additional security, like fingerprint ID and password protection.

Just like other forms of payment, digital wallets can be vulnerable to hackers and scammers. It is essential to practice good password hygiene, account monitoring, and avoiding making transactions on unsecured Wi-Fi networks.