

# Digital Wallet Do's and Don'ts: Sleep Soundly When Your Online Finances Are Secure

Digital wallets are increasingly being developed to perform more than simply monetary transactions; they are also being designed to authenticate the holder's credentials.

A digital wallet, alternatively referred to as an e-wallet, is an electronic device, internet service, or software application that enables one party to conduct electronic transactions with another party in exchange for digital currency units.

This approach can include shopping online with a computer or utilizing a smartphone to make in-store purchases. Users can transfer funds into a digital wallet before any transactions, or in some situations, they can link the digital wallet to their credit card or bank account.

## Are Online Transactions Putting Your Security at Risk?

Without question, digital wallets have gained popularity across the globe and are projected to potentially replace cash as the primary form of payment in the future.

As millions of people increasingly rely on modern conveniences for payment and account access, and as cybercrime continues to grow, e-wallet security becomes more essential.

Keeping data secure in our digital age is not always as simple as creating a couple of [clever passwords](#). Experienced thieves and hackers often bypass these checks entirely. Fortunately, there are methods for safeguarding your digital wallet and ensuring that you may access it when necessary. The following are a few strategies for staying safe:

### Deny Unsolicited Links

Avoid uninvited connections. A friend's phone may be infected with malware and sending you texts to infect you and everyone else in your contact list. Even if a source appears familiar, [exercise caution](#). If you think a friend sent you a link, text back and ask about it before clicking.

### Sidestep Public WiFi

Avoid accessing public WiFi to view confidential information or surf websites that capture and keep your data. It's best to avoid using public WiFi at parks, libraries, and cafés unless you want someone other than you to keep an eye on your bank account.

### Read The Fine Print

Avoid downloading apps without reading the fine print. Apps increasingly use GPS data to establish where you live, eat, and shop. Additionally, they have access to your calendar and contact list.

This access is accomplished through "terms of service" agreements that most users accept without reading. Although they are frequently complicated and challenging to comprehend, you should not download the app if you do not agree to the terms.

## **Use Two-factor Authentication**

If you haven't already, you should check to see if your accounts enable two-factor authentication (2FA). It is a highly effective means of stopping unauthorized users from gaining access to an account.

With typical 2FA, when you enter your standard password, the website sends a four to six-digit code to your email or phone. This strategy creates two obstacles for hackers, and it'll also notify you if your account is compromised.

## **Employ a Security Service**

A security service like [LifeLock](#) guards your credit and finances against identity theft and fraud.

Of course, not everyone is equally vulnerable to identity theft. Individuals with a busy travel schedule may require a different level of protection than those concerned with online shopping or everyday encounters.

Services like LifeLock make it simple to select the plan that matches your lifestyle and online activities the best. If you're looking to regain peace of mind concerning your digital wallet, this type of service might be your best bet.