Digital Wallet Security

Just "LOK" It

WHAT IS A DIGITAL WALLET?

The term digital wallet is broadly used to capture a variety of electronic and mobile payment services, typically through your mobile phone, that give you access to your accounts – just like the different cards you keep in your wallet today, but without the bulky leather and rubber bands holding it together.

Digital wallets can hold personal data, including your payment account numbers, shipping addresses, phone numbers, email addresses, etc.

They may also allow you to store multiple payment types (cards, bank accounts), including Visa, MasterCard, American Express and Discover accounts.

Digital wallet services may use a range of technologies, such as NFC (near-field communications) or QR (quick response) codes. Some services also offer the ability to make online payments through the use of a password rather than entering card information.

You may have the option to choose which account you want to use for a given transaction, and the same password or app could work across multiple devices.

In essence, a username and password gives you access to the accounts in your wallet. For online shopping, this allows you to skip the hassle of entering your name, address, card number and expiration date. In some cases, the retailer never sees your account information, helping to protect it against being compromised.

Mobile technology is changing the ways we pay, including what we think of as a wallet. Soon, along with using a card in a physical wallet, we'll also be able to pay with a mobile phone - what is often referred to as a "**digital wallet**."

The term "digital wallet" serves as a blanket definition, as many providers will offer a variety of services beyond what you would today consider as part of a wallet – digital or physical.

Digital wallets are generally designed to provide more convenience and control over your finances. They can even be considered safer than traditional wallets, since access to them requires passwords, passphrases or "keys." On top of being secure, the next generation of wallets may also help you:

- Manage your payments and accounts
- Receive offers from merchants you know and trust
- Track and spend reward or loyalty points
- Store digital receipts and warranty information
- Get alerts about your account and spending

SAFETY AND SECURITY

There are a number of companies that play a role in various electronic and mobile commerce products, from long-time payments companies, like Visa, to social networks, gaming communities, Internet search engines and telecom operators. All of these types of companies are handling and sharing information about your financial accounts and identity—so combating fraud, preserving your privacy and protecting your accounts is more important than ever.

Before signing up for a digital wallet, you should look for a provider to demonstrate:

A strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud). data and providing customer support (in the event of card loss or account fraud).

The ability to send alerts of possible inappropriate access and fraudulent transactions through multiple channels, including email, text messages and telephone calls.

Readily-available and clear information on how they collect, store and use your information. A provider should also make clear whether your private information will be stored on a physical device or in the "cloud" (or both), and how they are protecting it.

What's the "cloud?"

The "cloud" is where companies and people store and access information on remote servers, rather than on specific devices or desktops.

VISA

Industry & Consumers Working Together

Keep Your Money Secure: Just "LOK" it

We all have a role to play in keeping our financial accounts safe. Similar to the way you protect your physical wallet today, it's important to protect your digital wallet. You wouldn't let a stranger access the physical wallet that's in your bag or pocket right now, would you?

As electronic and mobile commerce options expand, the payments industry, with its long history of security and fraud prevention, is using advanced technology to protect consumers. At the same time, even the most secure application can be compromised, especially if you use a weak password or if your device is unlocked and ends up in the hands of someone else.

There are a few simple things you can do to help make sure access to your money is as secure as it is convenient. Keeping your sensitive information safe can be easy and inexpensive, while providing immediate benefit in protecting against identity theft and fraud.

Essentially, keep three letters in mind to "L-O-K" access to your money and keep it safe:

- Lock it down – Protect (physically and with passwords/passphrases) the devices you use to access your payment options: personal computers, mobile phones, tablets, etc.
- Only you access sensitive information – Safeguard sensitive data, including user names, passwords, PINs, passphrases and answers to security questions.
- Know who to call – Before anything happens, know who to call if your wallet were to be compromised.

Lock it down

ENABLE DEVICE PASSWORDS

Set phones, tablets, personal computers and other devices to require a password before they can be used. Enjoy the benefits of additional layers of security mobile devices or PCs offer.

CONNECT TO SECURE NETWORKS

Choose secure network connections you trust. A simple test: more secure WiFi connections require passwords and are easily identified as "WPA or WPA2." Highly-unsecure WiFi is wide-open for anyone to connect to, and may be labeled as a "WEP" connection.

INSTALL APPS FROM SOURCES YOU TRUST

Not all apps are what they appear to be. In fact, you could be getting more than you bargained for. A free game might not be just a game, but an app designed to illicitly collect personal data from you. Reading the user ratings and reviews can provide some clues about the integrity of the app.

KEEP YOUR DEVICE UPDATED

Hardware and software manufacturers release frequent updates to optimize performance and security. Stay aware of updates and their impacts, and ensure they are installed.

USE SECURITY SOFTWARE

Be smart about it – activate applications for detecting and removing threats, including firewalls. Also activate virus and malware detection and intrusion-detection systems.

Only you access sensitive information

KEEP YOUR PRIVATE STUFF PRIVATE

Don't share sensitive data with those you don't trust. This includes when you respond to email requests, phone inquiries or allow control to anyone you would not normally hand over a physical wallet to. Credible service providers and support staff will never ask for private information such as passwords or payment-account numbers.

KEEP LOGIN CREDENTIAL SECURE

Easy access to usernames and passwords leads to misuse. Don't write down information used to access your digital wallet in plain view or store in an unprotected file.

USE A PASSWORD THAT ONLY WORKS WITH YOUR DIGITAL WALLET

Don't use the same password you use for email or social networking sites. This increases the risk of unauthorized access. Instead, use an easily- remembered, yet hard-to-guess password unique to your digital wallet.

Know who to call

IDENTIFY WHO TO CONTACT IF THERE ARE ISSUES, BEFORE ONE ARISES

Financial institutions, payment networks and merchants are all needed to make electronic and mobile payments work. Make sure you understand the quickest way to resolve any issues that arise and who is responsible for any fraudulent activity on your account. Scenarios to consider:

- *Your phone is lost or stolen*
- *An individual card stored in the wallet is lost*
- *Your account has been or may have been hacked*

REVIEW CONTRACT TERMS AND CONDITIONS

This is where rights and liabilities are defined. Topics should address data privacy, opting-in and out of various features and impacts of enrolling and canceling accounts and services.

For more information, visit www.visa.com/security

VISA