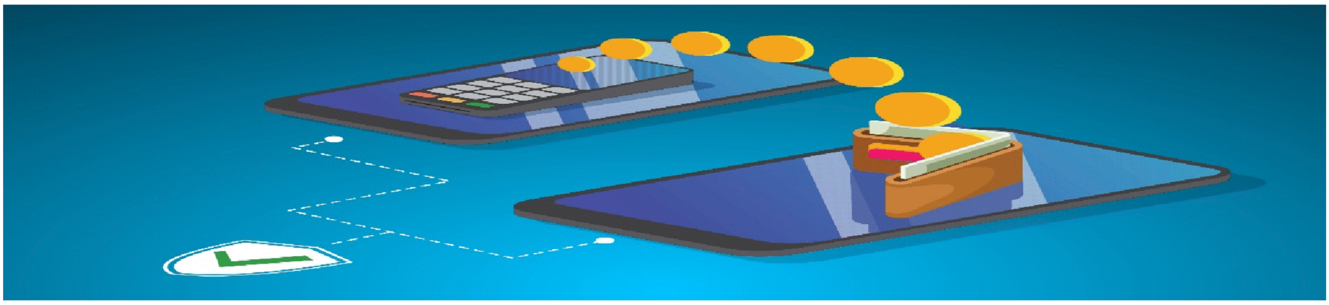
August 2023

BWN COMPUTER NEWSLETTER



Are Digital Wallets Safe to Use?

With the embrace of smart mobile devices, digital wallets have grown popular. Also known as e-wallets or mobile wallets, these apps store payment information virtually. The convenience is undeniable; the question is whether digital wallets are safe to use.

Popular examples of digital wallets include Apple Pay, Google Pay, Samsung Pay, PayPal, Venmo, Alipay, WeChat Pay, and others. A digital wallet can store:

- credit card details;
- bank account information;
- store loyalty cards;
- tickets;
- other virtual assets.

This enables online purchases, money transfers, bill payments, and in-store payments, all done through mobile devices. Plus, you don't have to manually enter the payment details each time. Many digital wallets use near-field communication (NFC) for contactless payments. When you tap your smartphone or smartwatch on a point-of-sale device to pay, you're taking advantage of NFC.

Digital wallets allow people to travel light. Integrating them with food delivery and ride-share apps can simplify those payments, too. And you no longer have to worry about a thief getting their hands on your credit or debit card. Consider the pros and cons of trusting a digital wallet application.

Weighing Up Digital Wallet Security

On the plus side, digital wallets use various security measures that include:

- encryption, which converts your data into random code in transit and storage;
- biometric authentication, such as fingerprints or facial recognition;
- tokenization, which replaces your payment information with non-sensitive data.

At the same time, there are risks. For one, NFC works wirelessly. This means there's always a chance an attacker could intercept your payment once you authenticate it. They'd need to be near your device to access the information, but it's possible. Using a digital wallet application also means you're relying on technology. Additionally, it's possible someone could hack the digital wallet app. Still, a physical wallet also risks theft and exposing your financial information. So, there's no real reason to avoid digital wallets, just take precautions.

Secure Your Digital Wallet

Protect your digital wallet and financial information by taking the following steps:

- Download digital wallet apps from official app stores or reputable sources only.
- Regularly update digital wallet apps.
- Use strong passwords or biometric authentication for your digital wallet.
- Enable two-factor authentication when possible.
- Secure the devices linked to your digital wallet and financial information.
- Review your transaction history and statements to detect any unauthorized or suspicious activity.

Digital wallets can be a safe and secure way to make payments. Follow these suggested precautions and be mindful of potential risks.

RANSOMWARE ATTACK
ALL OF YOUR DATA HAS BEEN ENCRYPTED!
PAY $500 TO THIS BITCOIN ADDRESS:

The Dangers of Smartphone Ransomware

You've likely seen news coverage of ransomware targeting large companies or hospitals. Maybe you've seen Homeland when Claire Danes' character falls victim to laptop ransomware during a surveillance mission. But did you know that ransomware attackers can also target your smartphone?

A smartphone, after all, is a portable computer in your palm. Take a moment to imagine being locked out of your own phone. The hackers could gain access to your saved passwords and emails. You could lose access to your contacts, notes, and images, and even your three years' worth of effort on Candy Crush.

What You Need to Know About Smartphone Ransomware

Also known as mobile ransomware, these attacks infect your smartphone. Instead of stealing the actual device, the bad actors take it hostage. They typically encrypt your data and make it so you can't do anything.

It may not be as widely publicized, but there's already a long list of smartphone ransomware programs. The list continues to grow with examples such as ScarePackage, LeakerLocker, and LockerPin. ScarePackage can infect more than 900,000 phones in a single month.

And before you think, "That won't happen on my iPhone," know that no smartphone manufacturer is secure. The type of ransomware may vary due to the different operating systems, but you can be at risk on both Android and an iPhone.

Unlike other malware, the hackers usually want you to know they've gained control. Typically, they will notify you on your lock screen or home screen. You'll often see a list of demands and a deadline to comply. That said, some mobile ransomware stealthily steals your data.

What To Do About Mobile Ransomware

The first thing to do? Be cautious. Keep these best practices in mind always:

- Regularly update your device's operating system and applications to patch any security vulnerabilities.
- Exercise caution when downloading or installing apps from untrusted sources.
- Avoid clicking on suspicious links or opening email attachments from unknown senders.
- Enable app and system updates to ensure you have the latest security patches.

If you become a ransomware victim, try to disconnect your device from the internet. Turning off Wi-Fi and mobile data limits communication with the attacker's server.

Avoid paying the ransom. It's tempting but not recommended. You are counting on hackers to keep their word and provide the encryption key.

You can find decryption tools online for less complex ransomware. If the ransomware came from a malicious app, immediately delete that app if you can.

What you can do will depend on the specific ransomware variety. In general, it's best to seek professional help. Work with an IT expert who can remove ransomware without further compromising your device. We can also help you restore clean, unaffected backups.

Whether you need help with digital wallets OR with securing your smartphone...we are here to help.

Contact us today at 940-282-0290.