Cyber Byte

October 2025.

“Digital Pickpockets” …are they a thing?

There can be no doubt we are living in an increasingly digitised age where we see the integration of technology in almost every area of our lives. That innovation transforms and, in some cases, streamlines the way we function both online and offline.

One of the most common examples of that transformation and streamlined functionality is e-commerce and in particular the increasing use and dependency on digital wallets where we store our bank and credit cards. They can be used from mobile phones, tablets or computers to make payments online, in-store shopping to transferring money to friends and family.

They provide convenience, eliminating the need to carry physical cards. Some digital wallets allow users to store ID cards, boarding cards, event tickets and QR codes. That convenience for some is not just at their fingertips, as digital wallets feature on smart watches and digital wristbands, allowing users to manage their transactions directly from their wrists.

Globally, it is estimated there are 4.3 billion digital wallet users, this is more than half the population and is set to increase with some predictions estimating that 68% of the global population will be using digital wallets by 2030.

Unlike physical contactless cards, which are typically limited to £100 per transaction, digital wallets do not have arbitrary spending limits, this makes it easier for criminals to make large purchases when they get access to digital wallets and the card data stored in them.

However, as much as they provide convenience and do have security features, they also present a target for cybercriminals to target users.

Cybercriminals will impersonate well known retailers on social media, advertising products and closing down sales with goods at knock down prices which appear too good to be true.

They will send out phishing emails and scam texts to lure victims to their and fake websites asking for card details as they complete the shopping transaction. Once the victim has provided their card details on the fake website, the cybercriminal steals these and adds to their own digital wallet to commit fraud. The victim will be unaware and won’t receive the goods they have seemingly purchased.

All information correct at time of distribution - Police Scotland Cybercrime Harm Prevention Team.

Common Types of Digital Wallet Scams.

Phishing Scams: Scammers send emails and text messages appearing to be genuine but trick victims' users into revealing their login credentials. These messages may contain links to fake websites and QR codes designed to capture personal information.

Fake Wallet Apps: Fraudsters create fake apps mimicking legitimate digital wallets. Users unknowingly download these and upload their card details, which are then exploited.

Social Engineering: Scammers impersonate trusted entities, such as customer support in a legitimate organisation, to manipulate users into disclosing personal data or **One Time Passcodes** OTPs sent by their bank. Always pay close attention if you receive a request to approve a OTP, make sure it is genuine and relating to you making or authorising a payment.

Account Takeovers: Cybercriminals may gain access to a user's digital wallet account through their stolen credentials, allowing them to make unauthorised transactions.

So how can we protect our digital wallets.

- **Use Strong Passwords** to ensure that your digital wallet account is protected with a strong, unique password and enable 2 step verification whenever possible.

- **Download Apps** only from official app stores and verify the authenticity of websites before entering your personal information.

- **Monitor Transactions** and regularly check your account/s activity for any unauthorised transactions and report suspicious activity immediately.

- **Stay informed** about the latest scams and tactics used by fraudsters to better protect yourself and your finances and if your bank notifies you that your card has been added to a digital wallet and you did not do this, call the bank immediately to investigate. Many banks can be reached via the **fraud helpline 159** it works in the same way as 101 for police or 111 for the NHS.

- **Avoid links** and don't click on links in emails or messages that claim to be from your bank or credit card company. If you're unsure if a message is legitimate, contact the organisation directly using a trusted phone number or website.

- **Check website data** when shopping online, make sure the web address is correct and use a **Domain checker** to verify the site and be cautious of ads with prices that seem too good to be true.

- **Turn on notifications** on your banking app. This allows you to receive push notifications whenever money is spent on your account. This can help you spot fraudulent activity as soon as it occurs.

- **Check statements** regularly and report any suspicious transactions to your bank immediately.

All information correct at time of distribution - Police Scotland Cybercrime Harm Prevention Team.

By understanding the risks associated with digital wallets and implementing these preventive measures, you can significantly reduce your chances of falling victim to scams.

The following links will provide additional guidance for you to review and implement.

Top tips for staying secure online - NCSC.GOV.UK

Protect yourself | Take Five

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

All information correct at time of distribution - Police Scotland Cybercrime Harm Prevention Team.