UDC 336.717.061

**Antonina Farion**

Phd, associate professor,

Department of the economic security and financial investigations

Ternopil national economic university

**Mykhailyna Farion**

Phd, associate professor,

Department of the economic theory

Ternopil national economic university

**SECURITY OF MOBILE PAYMENTS AND DIGITAL WALLETS**

We live in the age of digital technologies. Usage of mobile payments and digital wallets becomes more popular nowadays. In Wikipedia we can find the next explanation of mobile payment (mobile money, mobile money transfer, and mobile wallet) – payment services operated under [financial regulation](https://en.wikipedia.org/wiki/Financial_regulation) and performed from or via a [mobile device](https://en.wikipedia.org/wiki/Mobile_device) [1]. [Brady Porche](https://www.creditcards.com/credit-card-news/authors/brady-porche.php) stresses that mobile payments are characterizing by using virtual smartphone wallets such as Apple Pay, Samsung Pay and Chase Pay to make purchases and they have [grown in popularity among consumers](https://www.creditcards.com/credit-card-news/infographic-mobile-payments-climb-slowly.php) since 2011 [8]. Collins dictionary adduces the digital wallet as an [application](https://www.collinsdictionary.com/dictionary/english/application) or device which [enables](https://www.collinsdictionary.com/dictionary/english/enable) the [user](https://www.collinsdictionary.com/dictionary/english/user) to make payments electronically [2]. With digital wallets people can store capital in digital form and they allow them to purchase goods or services online or send funds to friends or families. IT gives possibilities to combine all necessary information about person – financial date, debit, credit, loyalty, health, driver’s license and other ID information. Alex Rolfe (November 26, 2018) admits that after Apple launched the first mobile wallet app followed others mobile companies, its popularity increased rapidly. It is expected that the transaction value of mobile payment apps will reach nearly $14 trillion by 2020 and every country has own date (fig. 1) [3]. In the current conditions, technology for digital payments is equal to consumers demand. The mobile payment market continues growing and even faster than before. The whole digital industry is gearing up to enable mobile payments on a global scale. The numbers of phone users are predicted to rise to 5.07 billion in 2019 [5]. Mobile apps accounted for more than 30 percent of global digital commerce volume in 2017 [6]. The availability of digital payment is increasing significantly in almost all countries translating in consistently growing non-cash transaction volumes.

# Figure 1. Global statistics for usage digital wallets 2018 [3; 4]

# Attitude to payment by mobile devices is analyzed in table 1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Legal Tender | Convenience | Direct settlement | Anonymity | Availability | Reliability | Secure | Efficient | Remote payment | Higher value payment >5000 EUR |
| Mobile payments | × | ✔ | × | × | × | ± | ± | ± | ✔ | × |

# Formed by using source [7].

# There are three most risks linked with mobile payments (figure 2).

Risks linked to mobile payments

Cyberthieves who spoof mobile **wallets**

Malware on cellphones

Losing phones

# Figure 2 Types of risks linked with mobile payments [8]

When people add credit and debit cards to mobile wallets, the card numbers are stored securely by via encryption that disguises them with codes created by algorithms. Except that, the main mobile wallet providers try to use randomly generated payment tokens to ensure person card information has not been seen by users or even the wallet providers when owners make shopping [8]. These actions are taken through the financial services industry is the top target for cybercriminals looking to steal valuable data. Many consumers put confidential information on devices that can be easily lost or stolen. Smart botnets and polymorphic malware are the most dangerous for mobile payments and digital wallets. A botnet is a [group](https://dictionary.cambridge.org/dictionary/english/group) of [computers](https://dictionary.cambridge.org/dictionary/english/computer) that are [controlled](https://dictionary.cambridge.org/dictionary/english/controlled) by [software](https://dictionary.cambridge.org/dictionary/english/software) [containing](https://dictionary.cambridge.org/dictionary/english/contain) [harmful](https://dictionary.cambridge.org/dictionary/english/harm) [programs](https://dictionary.cambridge.org/dictionary/english/program), without [their](https://dictionary.cambridge.org/dictionary/english/their) [users](https://dictionary.cambridge.org/dictionary/english/user)’ [knowledge](https://dictionary.cambridge.org/dictionary/english/knowledge) [9].Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection [10]. The worldwide mobile payment revenue is expected to [1 trillion](https://www.statista.com/statistics/226530/mobile-payment-transaction-volume-forecast/) U.S. dollars in 2019, which is more than 22,000% increase from 450 million in 2015. But statistic shows that many mobile payments are not protected properly (fig. 3).

Figure 3. Opinion about security of mobile payments [11]

The next steps to secure digital payments must be taken – users authentication, devices’ authentication and date protection (limited use security keys, tokenization, device fingerprinting, and transaction risk analysis).

**LITERATURE:**

1. Mobile payments. Wikipedia. URL: <https://en.wikipedia.org/wiki/Mobile_payment>
2. Digital wallet. Collins dictionary. URL: <https://www.collinsdictionary.com/dictionary/english/digital-wallet>
3. Rolfe, A. The rise of digital and mobile wallet: Global usage statistics from 2018. URL: <https://www.paymentscardsandmobile.com/mobile-wallet-global-usage-statistic>
4. Number of smartphone users in Japan from 2015 to 2022 (in millions). URL: <https://www.statista.com/statistics/275099/number-of-smartphone-users-in-japan>
5. Brown, M. What 2018 has in store for mobile payments. URL: <https://www.itproportal.com/features/what-2018-has-in-store-for-mobile-payments>
6. Global payments 2018: A dynamic industry continues to break new ground. McKinsey and Company. Global Banking October 2018. URL: <https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Global%20payments%20Expansive%20growth%20targeted%20opportunities/Global-payments-map-2018.ashx>
7. World cash report 2018. URL: <https://cashessentials.org/app/uploads/2018/07/2018-world-cash-report.pdf>

1. [Porche](https://www.creditcards.com/credit-card-news/authors/brady-porche.php), B. 3 major mobile payment security risks, and how to avoid them. URL: <https://www.creditcards.com/credit-card-news/mobile-payment-security-risks.php>
2. Botnet. Cambridge Dictionary. URL: <https://dictionary.cambridge.org/dictionary/english/botnet>
3. Definition of polymorphic malware. Data Insider. Digital Guardian’s blog.URL: <https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware>
4. What are mobile payments? URL: <https://cardconnect.com/launchpointe/payment-security/mobile-payment-security>