FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Publications and press releases

Press release 19 March 2024

Payment-related frauds and scams are a growing phenomenon – Financial Supervisory Authority investigation reveals scope for improving security of banking transactions

Various payment-related frauds and scams have been sharply increasing in recent years. The means used by criminals are also constantly evolving. According to an investigation by the Financial Supervisory Authority (FIN-FSA), there is scope for improving the security of banking transactions, for example by developing security restrictions on online banking and mobile payments and by more effectively monitoring and blocking fraudulent transactions. Users of services themselves also bear responsibility.

Based on a survey of banks conducted by the FIN-FSA in 2023, banks have, for the most part, identified and implemented the key aspects of online payment security appropriately.

"Online banking, mobile banking and online payment security as well as strong customer authentication technology solutions need to respond to new security threats in electronic payments. Our investigation reveals that this is generally the case, but since the race against criminals is intense, it is necessary to implement all possible measures in security solutions," says **Samu Kurri,** Head of Department.

Banks have means available to improve the security of online transactions, which the FIN-FSA encourages them to use. Payment service users have the option to set more versatile payment security limits for card payments than for credit transfers and payments made via online and mobile banking. The FIN-FSA recommends that banks develop controls for online banking and mobile payments so that users would have the option to set more versatile security restrictions on their credit transfer -based payments. Such restrictions include, for example, geographical restrictions on payments and daily or one-time usage limits for payments.

Furthermore, the FIN-FSA recommends that banks develop their payment monitoring so that they could more precisely block payments that differ significantly from the customer's previous payment history, for example according to the recipient or the size of the payment. In these cases, it may also be necessary to request an additional confirmation of payment from the customer in a sufficiently informative manner.

"It is also important to provide information about different types of scams and to guide customers on secure online transactions. Banks must continue to communicate actively through various channels about the security threats to their services and continue to remind and guide customers on how to use their electronic services securely," says Kurri.

Users of services also bear responsibility

Banks are responsible for the security of the services they offer online, but the FIN-FSA reminds consumers of their own responsibility and of the security practices worth keeping in mind when making online and mobile payments.

When using online services, customers should be suspicious and also remember that banks or authorities will never ask for their bank credentials or payment card information by phone, email or text message. Customers should also be careful about clicking links. Bank credentials should never be used to log in to services via links in messages. Links even in genuine-looking messages may lead to a fake website and online banking credentials falling into the hands of criminals.

The risk of online banking credentials falling into the wrong hands can be reduced by using, for example, other strong identification tools, such as a mobile or citizen certificate, when identifying yourself to official services.

A so-called digital identity wallet application for mobile phones is currently being developed in the EU. In the future, it will be possible to use it for digital authentication of identity when logging into both public and private online services throughout the EU.

For more information, please contact

Samu Kurri, Head of Department. Requests for interviews are coordinated by FIN-FSA Communications, tel. +358 9 183 5030, Mon-Fri 9.00–16.00.

FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Publications and press releases

Supervision release 19 March 2024 – 13/2024

Security of online banking, mobile banking and online payments

Various payment-related frauds and scams are a constantly increasing phenomenon. Methods of fraud are constantly evolving, so online banking, mobile banking and online payment security as well as strong customer authentication technology solutions need to respond to new security threats in electronic payments.

Background to the survey

In a survey it conducted in October-November 2023, the Financial Supervisory Authority (FIN-FSA) investigated controls and processes related to the online banking, mobile banking and online payment security of banks operating in Finland, with the aim of ensuring strong customer identification and payment security against misuse of means of payment and other scams.

The results of the survey provide more detailed information than before about the security of banks' online payments and payment-related controls. The responses received will help the FIN-FSA to target its supervision both generally and on a bank-specific basis.

Survey conclusions and recommendations for banks

Based on a thematic assessment, banks have, for the most part, identified and implemented the key aspects of online payment security appropriately.

The responses to the thematic assessment show that payment service users have the option to set more versatile payment security limits for card payments than for credit transfers and payments made via online and mobile banking. The FIN-FSA recommends that banks develop controls for online banking and mobile payments so that users would have the option to set more versatile security restrictions on their credit transfer -based payments. Such restrictions include, for example, the option to set a daily or one-time usage limit for payments as well as to limit the countries or geographical areas and receiving parties to which payments are directed.

In addition, banks should improve the monitoring of potentially fraudulent transactions, blocking them and requesting further confirmation. The FIN-FSA recommends that banks develop their payment monitoring so that they could more precisely block ments that differ significantly from the customer's previous payment history, for example according to the size of payments or

the parties to which the customer has previously sent payments. In these cases, it may also be necessary to request an additional confirmation of payment from the customer in a sufficiently informative manner.

Important for banks to guide customers on secure online transactions

It is important to provide information about different types of scams and to guide customers on secure online transactions. Banks must continue to communicate actively through various channels about the security threats to their services and continue to remind and guide customers on how to use their electronic services securely.

For further information, please contact

Markko Koponen, Head of Division, markku.koponen(at)fiva.fi or telephone +358 9 183 5389

See also

Press release 19 March 2024: Payment-related frauds and scams are a growing phenomenon – Financial Supervisory Authority investigation reveals scope for improving security of banking transactions