

RĪGA

8 июня 2020 года

## **Пользователей Smart-ID призывают быть бдительными**

**На прошлой неделе появилась информация о попытках мошенников получить доступ к банковским приложениям жителей, используя Smart-ID. Разработчик Smart-ID компания SK ID Solutions, Латвийская ассоциация финансовой отрасли и банки призывают клиентов быть бдительными.**

Клиенты нескольких латвийских банков сообщили о поступивших им телефонных звонках с неизвестных номеров. Звонивший, как правило, представлялся сотрудником службы технической поддержки Smart-ID и пытался выманить информацию, уговаривая совершить действия, которые, возможно, позволили бы ему получить доступ к аккаунту Smart-ID, принадлежащему адресату звонка. На данный момент нет информации о том, что данные попытки мошенничества увенчались успехом и кому-то из клиентов был нанесен финансовый ущерб. Тем не менее, к подобным анонимным телефонным звонкам следует относиться с особой осторожностью.

Приложение Smart-ID обеспечивает двухфакторную аутентификацию и является значительно более безопасным, чем используемые ранее кодовые карты, в которых применялись статичные коды и которые легко можно было потерять. Несмотря на это, пользователям интернет-банка и мобильных приложений следует оставаться бдительными и самим заботиться о безопасности своих данных. Одно из основных правил: никогда не вводите ПИН-коды в свое приложение Smart-ID, если вы не используете интернет-банк или одно из банковских приложений и не инициировали никаких операций в этот момент. Подобный запрос ввести ПИН-код может свидетельствовать о том, что кто-то другой пытается получить доступ к вашим банковским счетам.

Председатель правления Ассоциации финансовой отрасли Санита Баяре подчеркивает: «Следует быть очень осторожным, если кто-то пытается уговорить вас воспользоваться устройствами, используемыми вами для доступа к банковским приложениям и подтверждения платежей. Напоминаю, что банки никогда не отправляют своим клиентам электронные письма с просьбой ввести аутентификационные данные или ответить на чувствительные вопросы. При получении любых запросов использовать выданные вам средства подтверждения платежей, которые не были инициированы вами, ни в коем случае не делайте этого и немедленно свяжитесь со своим банком!»

«Сотрудники содержащей Smart-ID компании SK ID Solutions никогда не будут звонить клиентам, чтобы выяснить их данные. Особенно бдительным следует быть в случае, если в телефоне вдруг появляется сообщение с просьбой подтвердить сделку с помощью Smart-ID, хотя сам пользователь приложения никаких действий, требующих подобного повреждения, не совершает. Это может означать, что мошенники пытаются получить доступ к системе, использующей для аутентификации пользователя приложение Smart-ID. Название поставщика услуги можно увидеть в верхней части запроса аутентификации», - предупреждает руководитель латвийского филиала SK ID Solutions Санита Мейере.

#### **Дополнительная информация:**

Санита Мейере  
SK ID Solutions  
руководитель латвийского филиала  
тел. +371 29488795  
[sanita.meijere@skidsolutions.eu](mailto:sanita.meijere@skidsolutions.eu)

Сабине Спурке  
Ассоциация финансовой отрасли  
руководитель коммуникации  
тел. +371 20604166  
[sabine.spurke@financelatvia.eu](mailto:sabine.spurke@financelatvia.eu)