

РИГА

29 марта 2021 года

## **Финансовые мошенники постоянно совершенствуют свои цифровые навыки и отличаются изобретательностью**

Уже второй год подряд в Латвии вдвое увеличивается количество попыток финансового мошенничества. От них не застрахован никто, и, как показывают результаты эксперимента, проведенного Ассоциацией финансовой отрасли<sup>1</sup>, на попытку мошенничества реагирует каждый десятый человек. Поэтому стоит знать о методах, которые используют мошенники, чтобы не попасться на обман из-за спешки или по невнимательности.

«Мошенники активно используют пандемию Covid-19 и тот факт, что из-за ограничений большая часть нашей жизни «перенесена» в интернет. С прошлого года активно действуют мошенники, говорящие на латышском языке, которые, например, звонят от имени банка и предлагают работу, предлагают купить лекарства против Covid-19 или в период бума дистанционной торговли пытаются выманить данные платежных карт, имитируя популярные логистические компании. Недавно было публично рассказано о случае, когда у женщины выманили 3000 евро, обманув ее якобы предоставленным пособием на ребенка в размере 500 евро», – подчеркивает **Каспарс Бришка**, руководитель отдела информационной безопасности банка «Citadele».

### **Физические лица чаще всего сталкиваются со следующими видами финансового мошенничества:**

- **мошенничество с sms, электронными письмами или звонками:** мошенники отправляют текстовые сообщения, электронные письма или звонят, пытаясь получить личную информацию или банковские реквизиты. В большинстве случаев мошенники выдают себя за сотрудников службы безопасности банка или других сотрудников. Часто ссылаются на проверку безопасности данных и просьбы на обновление данных, отправляют уведомления о лотерейных выигрышах, наследстве, бесплатных авиабилетах, поддельных благотворительных кампаниях, рекламе, конкурсах в социальных сетях. В прошлом году в Лиепае женщина лишилась 1000 евро, сообщив свои данные телефонным мошенникам. Прикинувшись сотрудником банка, мошенники сообщили женщине о якобы подозрительной транзакции на банковском счете и, чтобы ее отменить, попросили назвать номер карты, ПИН-код и другую конфиденциальную информацию. Она попала на крючок мошенников о якобы существующей опасности для находящихся на счете средств.
- **мошенничество с инвестициями и кредитами:** мошенники предлагают нулевые риски и огромные возможности для получения прибыли или очень

---

<sup>1</sup> Эксперимент Ассоциации финансовой отрасли был реализован в феврале 2021 года путем рассылки поддельных мошеннических электронных писем в интернете 500 случайно выбранным получателям по всей Латвии.

выгодные кредиты. Обычно обещают высокодоходные вложения в акции, облигации, криптовалюту или другие финансовые активы или собственность. Мошенники часто торопят, стараются убедить, что предложение действительно очень короткое время и предназначено только для вас, просят никому не разглашать информацию об этом предложении. Мошенники призывают установить программное обеспечение, чтобы делать вложения. Могут также просто попросить перечислить деньги на счета мошенников. Они часто создают веб-сайты, на которых жертва может следить за «растущей прибылью», потому что обманчивый успех снова и снова поощряет инвестировать еще и еще. И в прошлом году в результате мошенничества с инвестициями житель Лиепай потерял 104 000 евро.

- **мошенничество при покупках в интернете:** мошенничество с использованием услуг, предоставляемых различными интернет-магазинами, когда деньги уплачены, но полученный продукт или услуга не соответствуют обещанию или не доставляются вообще. Попытки связаться с продавцом товара обычно безуспешны. В худшем случае человек не только теряет деньги, но и продавцы получают его данные, чтобы использовать их в мошеннических целях. В прошлом году была привлечена к уголовной ответственности преступная группа из 12 человек за продажу несуществующей сельхозтехники, которая выманила у людей 63 463 евро.
- **поддельный веб-сайт банка или интернет-магазина:** электронное письмо содержит ссылку на мошеннический веб-сайт. При нажатии на нее используются различные методы для получения данных банка. На поддельных веб-сайтах обычно появляются «всплывающие» окна с просьбой ввести данные. Такие не используются ни банками, ни интернет-магазинами. Веб-сайты обычно очень похожи на оригиналы. Так, например, в начале января мошенники, выдавая себя за «Citadele», разослали электронные письма с просьбой обновить информацию о себе в интернет-банке, и содержащаяся в письме ссылка вводила на мошеннический веб-сайт.

«Мошенники обнаружили способы подделки входящих телефонных номеров. Поэтому не всегда можно доверять звонкам с, казалось бы, известных латвийских номеров. Еще одно нововведение – включение мошеннических ссылок на интернет-банкинг в объявления Google. Мошенники становятся более креативными и технологичными, поэтому людям нужно быть бдительными и при первом подозрении, интуитивном ощущении, что что-то в рассказе все же не чисто, лучше позвонить и проконсультироваться с вашим банком. Лучше дважды перепроверить, чем попасться на удочку мошенников», – подчеркивает **Каспарс Бришка**.

#### **Дополнительная информация:**

Сабине Спурке

Эл.почта: [sabine.spurke@financelatvia.eu](mailto:sabine.spurke@financelatvia.eu)

Т. +371 20604166

Руководитель по коммуникации Ассоциация финансовой отрасли