FINANŠU NOZARES ASOCIĀCIJA

Doma laukums 8A-6, Rīga, LV-1050
Reģ. Nr. 40008002175
Tālrunis: 67284528
info@financelatvia.eu
www.financelatvia.eu

РИГА

7 апреля 2021 года

Что делать, если вы попались на крючок финансовых мошенников?

Согласно результатам эксперимента, проведенного Ассоциацией финансовой отрасли[*], на попытку мошенничества отзывается каждый десятый адресат. Основная причина, по которой люди попадаются – любопытство, затем следует желание получить обещанную выгоду, а также зачастую спешка. К сожалению, каждую неделю таким способом обманывают население на суммы от нескольких десятков до нескольких тысяч евро. Ассоциация финансовой отрасли собрала самые важные советы о том, как поступать в случае, если вы попались на крючок финансового мошенника.

Если во время разговора вы раскрываете мошеннику доступ к банку и личные данные, немедленно обратитесь в свой банк и сообщите о ситуации, чтобы заблокировать доступ к своему счету или к возможности использовать данные платежной карты.

«Если есть подозрение в мошенничестве, например, перевод денег мошеннику или произошла утечка данных платежных карт или интернет-банкинга, то об этом как можно скорее необходимо уведомить банк. Также, если карта утеряна или попала в чужие руки, необходимо немедленно заблокировать ее в своем интернет-банке или позвонить в банк. Жители должны быть осторожны и помнить, что никогда нельзя разглашать информацию о доступе к интернет-банку или данные платежных карт третьим лицам. Я также призываю жителей позаботиться о своих родственниках, особенно о пожилых людях, и рекомендовать не отвечать на эти мошеннические звонки или электронные письма», – подчеркивает **Павел Мицкевич, эксперт по информационной безопасности «Luminor».**

Если вы нажали на ссылку в электронном письме, текстовом сообщении, сообщении в социальной сети или загрузили мошенническое вложение:

- немедленно выключите Wi-Fi на устройстве и / или отключите его от сети. Если вы сделаете это достаточно быстро, то сможете помешать мошеннику установить вредоносное ПО или предотвратить удаленный доступ к вашему устройству.
- проверьте свое устройство на наличие вредоносных программ и вирусов. Антивирусная программа проверит устройство, предупреждая обо всех файлах, которые могут быть инфицированы.
- проинформируйте об этом случае учреждение, от имени которого было получено мошенническое сообщение.

[*] 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.

«Мошенники нередко используют различные развлекательные тесты, чтобы побудить людей узнать, что вы за животное или герой фильма, но они предназначены для получения ваших данных и их последующего использования в мошеннических схемах.

Кроме того, людей часто вводят в заблуждение различными неожиданными выигрышами в лотерею с целью добиться, чтобы получатель данного сообщения открыл отправленную ссылку или вложение. Однако следует помнить, что мошенники используют различные психологические приемы, дабы найти слабые места человека, а также полагаются на слабые цифровые навыки людей и желание быстро получить «выигрыш».

С другой стороны, получая доступ к электронной почте пользователей, мошенники могут отправлять сообщения друзьям человека, призывая их открыть ссылку или вложение, которое все же оказывается вирусом, и, соответственно, ваша электронная почта со всем ее содержимым становится доступной для мошенников. Обычно это короткие и лаконичные тексты: «Открой это, здесь ты выглядишь смешно!» или «Посмотри, какую твою фотографию я нашел в интернете!». Все это попытки мошенничества, поэтому следует быть очень бдительными и критичными при оценке любой информации, которую вы получаете, даже от близких людей», – указывает **Павел Мицкевич**.

Если вы ввели данные на мошенническом сайте:

- Смените пароль на реальном сайте (почтовый сервис или учетная запись в социальной сети), который был подделан мошенниками. Если вы используете один и тот же пароль для нескольких учетных записей, измените и их. Эксперты по безопасности не рекомендуют использовать один и тот же пароль более одного раза. Также желательно использовать двухфакторную аутентификацию, когда используется как пароль, так и другой фактор или дополнительный шаг, например, путем отправки кода на смартфон пользователя. Двухфакторная аутентификация в настоящее время считается одним из самых безопасных подходов к защите вашей информации в интернете.
- Если вы ввели данные платежной карты, немедленно обратитесь в банк, чтобы заблокировать карту.
- Убедитесь, что вы не стали жертвой кражи идентификационных данных. Во-первых, настройте входящие уведомления об изменении на счете или проверяйте выписку по счету как можно чаще, чтобы как можно быстрее обнаружить подозрительные транзакции. Сообщите об инциденте в кредитные бюро, предупредив о том, что ваши данные могут быть использованы, и попросив их сообщать об изменениях в вашей кредитной истории.

Большая часть нынешних киберпреступлений носит транснациональный характер, и Государственная полиция для поддержки расследований сотрудничает с правоохранительными органами других стран. Хотя расследования в рамках международных уголовных дел сложны и требуют много времени, есть случаи, когда благодаря быстрому сообщению в соответствующие органы жертвы возвращают свои деньги.

«Шансы на возвращение денег пропорциональны времени, в течение которого жертва обратилась в банк, и скорости, с которой он или она написали заявление в полицию. Важно сразу же сообщить в банк, следующий шаг – обратиться с заявлением в полицию. К нам активно поступают жалобы не только от жертв, уже потерявших свои деньги, но и от жителей, сообщающих о подозрительной активности в интернете. Это помогает своевременно оценивать ситуацию в сфере кибербезопасности и принимать превентивные меры», – указывает **Дмитрий Хоменко, заместитель начальника Управления по предотвращению экономических преступлений Государственной полиции.**

Заявление в Государственную полицию можно отправить в электронном виде на портале Latvija.lv, подтвердив электронной подписью, отправить на электронную почту pasts@vp.gov.lv, подать лично или отправить по почте в ближайшее отделение Государственной полиции. Предупреждение о различных подозрительных действиях в интернете отправляйте для рассмотрения в полицию через мобильное приложение Mana Drošība.

Дополнительная информация:
Сабине Спурке
Эл.почта: sabine.spurke@financelatvia.eu
Т. +371 20604166
Руководитель по коммуникации Ассоциация финансовой отрасли