

РИГА

22 марта 2021 года

## 8 советов, как не попасться на наживку финансовых мошенников

В течение последнего года финансовые мошенники все чаще использовали различные методы для получения данных доступа к банковским счетам жителей с целью мошенничества. Они звонят, пишут и вторгаются в нашу повседневную жизнь с четким планом: заставить врасплох, использовать растерянность и получить деньги или персональные данные. Вот почему Ассоциация финансовой отрасли составила 8 ключевых советов, как не попасться на приманки мошенников.



### КОНТРОЛЬНЫЙ СПИСОК БЕЗОПАСНОСТИ

Чаще всего на крючок мошенников попадают из-за любопытства и спешки. Прежде чем перечислить кому-то деньги, ввести коды Smart-ID, данные электронной подписи или другие личные данные, остановитесь, сделайте вдох и **ОТВЕЬТЕ НА 7 ВОПРОСОВ:**

 <p>ДОВЕРЯЕТЕ ЛИ ВЫ ОТПРАВИТЕЛЮ?</p>	Не кликайте на указанные интернет-ссылки, если номер телефона или электронный адрес отправителя кажется подозрительным!	 <p>ПРОСИЛИ ЛИ ВАС НАЗВАТЬ БАНКОВСКИЙ ПАРОЛЬ, КОДЫ SMART-ID, ДАННЫЕ ЭЛЕКТРОННОЙ ПОДПИСИ ИЛИ ДРУГУЮ ЛИЧНУЮ ИНФОРМАЦИЮ?</p>	Банк никогда не будет звонить и писать клиентам, чтобы попросить поделиться паролями или другими личными данными. Не разглашайте эту информацию, она защищает ваши деньги и цифровую идентичность!
 <p>ГОВОРЯТ ЛИ С ВАМИ НАХОРОШЕМ ЛАТЫШСКОМ ЯЗЫКЕ?</p>	Мошенники чаще всего ведут общение на русском языке, реже на английском, а на латышском языке еще не научились говорить свободно.	 <p>ОБРАЩАЮТСЯ ЛИ К ВАМ ОСОБО НАСТОЙЧИВО, ДАЖЕ АГРЕССИВНО?</p>	Мошенники пользуются психологическими приемами, чтобы найти слабые места человека. Сразу же прекратите разговор! Заблокируйте номер телефона, так как мошенники часто звонят повторно!
 <p>СОГЛАШАЛИСЬ ЛИ ВЫ НА УЧАСТИЕ?</p>	Если вы не принимали участия в конкурсе, но вам обещают огромный выигрыш, это мошенничество.	 <p>ПРИЗЫВАЮТ ЛИ ВАС ИНСТАЛЛИРОВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ</p>	Работники банка или инвестиционного предприятия никогда не попросят установить дополнительное программное обеспечение, чтобы делать инвестиции. С помощью него мошенники подключаются к вашему устройству, получают данные платежных карт и крадут деньги.
 <p>ПОЛУЧАЛИ ЛИ ВЫ МИСТИЧЕСКИЙ СЧЕТ?</p>	Если вы не пользовались услугой, за которую вам выставлен счет, это мошенничество.		

Если у вас возникли подозрения, что вы столкнулись с мошенничеством, прервите звонок, позвоните в свой банк и убедитесь, что ваши средства защищены от мошенничества!

**NEPOPADI.LV**

- 1. Не разглашайте пароль банка и коды Smart-ID, как бы сильно у вас их ни просили. Не вводите коды, если не вы сами инициировали действие, для подтверждения которого эти данные необходимы. Эта информация защищает ваши деньги и идентичность в цифровой среде!** *«В настоящее время активизировались мошенники, которые звонят и запрашивают данные банковской карты и интернет-банка, часто представляясь представителем банка или компании-разработчика приложения Smart-ID. Они используют технологии, при помощи которых можно подделать номер телефона или название компании, отображаемых на экране. Поэтому будьте внимательны и помните самый важный критерий для таких звонков: банк никогда сам не позвонит вам, чтобы узнать данные вашей платежной карты, номер пользователя интернет-банка или чтобы попросить ввести коды Smart-ID»*, – рассказывает **Вадим Фролов, руководитель управления клиентского сервиса Swedbank.**
- 2. Не поддавайтесь спешке, агрессии и прочим психологическим приемам мошенников!** В таких случаях немедленно завершите разговор. Всегда будьте осторожны, отвечая на звонки от неизвестных абонентов.
- 3. Если разговор или предложение звучат подозрительно и вызывают сомнения, завершите разговор и позвоните на официальный номер телефона вашего банка.** Объясните ситуацию сотруднику банка, он скажет вам, был ли звонок попыткой мошенничества, и объяснит, что делать. Например, одним из подозрительных моментов является то, что звонящий **не говорит по-латышски**, хотя представляется как **сотрудник организации или учреждения, представленного в Латвии.**
- 4. Если вы получили неожиданное электронное письмо, убедитесь, кто его настоящий отправитель.** Часто сначала кажется, что сообщение пришло из банка, но, когда мы видим, что скрыто под <адресом>, мы понимаем, что это подделка. *«Часто используемая мошенническая приманка – это призыв обновить ваши данные. Цель этой схемы – убедить вас поделиться ценной информацией, такой как данные банковской карты, для якобы подтверждения вашей идентичности и обновления информации. Такие электронные письма сделаны так, чтобы создать впечатление, что они были отправлены из учреждения, которому вы доверяете (банки, Служба государственных доходов и т.д.). Следовательно, всегда необходимо проверить, соответствует ли адрес электронной почты отправителя организации, из которой якобы было отправлено письмо, нет ли в нем лишних цифр или букв. То же самое относится и к ссылкам на веб-сайты в электронной почте. Необходимо убедиться, что они связаны с организацией, от имени которой было отправлено письмо. Если письмо кажется подозрительным, удалите его и сообщите о попытке мошенничества. Не открывайте подозрительные файлы, потому что даже антивирусные программы часто не могут определить новое вредоносное содержание»*, – указывает **Оскарс Блумбергс, руководитель по информационной безопасности банка SEB.**
- 5. Изучите прикрепленную веб-ссылку, прежде чем нажимать на нее.** Не переходите по интернет-ссылке, указанной в электронном письме или текстовом сообщении, если вы не доверяете отправителю! *«Помните, что банк*

*никогда не будет посылать ссылку на интернет-банк через SMS. Также при вводе кодов доступа в интернет-банке обращайтесь внимание на адрес сайта. Например, если это не <>.seb.lv, <>.swedbank.lv или другой адрес официального сайта вашего банка, на такой странице вводить коды доступа нельзя», – подчеркивает Оскар Блумбергс.*

6. **Если предлагаются инвестиции с нулевым риском и огромной прибылью, это приманка мошенников.** Недаром говорят, что бесплатный сыр бывает только в мышеловке. Чем выше обещанная прибыль, тем выше риск. Самый простой способ убедиться в подлинности предложения – поискать в Google информацию о соответствующей компании и инвестициях. *«Я определенно рекомендую заглянуть на сайт Комиссии рынка финансов и капитала Латвии, где можно найти лицензированных поставщиков инвестиционных услуг», – говорит Вадим Фролов.*
7. **Регулярно проверяйте исходящие платежи со своего счета!** Настройте уведомления об изменениях на счете или проверяйте выписку по счету как можно чаще, чтобы как можно скорее обнаружить подозрительные транзакции. Таким образом, вас нельзя будет поразить вводящей в заблуждение информацией об активности на вашем счете, потому что вы будете хорошо информированы.
8. **Не отвечайте на запросы об установке программного обеспечения на свои смарт-устройства.** Сотрудники банка или инвестиционной компании **никогда не попросят вас установить на ваши смарт-устройства дополнительное программное обеспечение**, которое поможет вам инвестировать. С их помощью мошенники получают доступ к устройству и выманивают деньги.

И все же, если вы поддались давлению и допускаете возможность того, что раскрыли свои данные интернет-банку мошеннику, немедленно свяжитесь с банком! Всегда сообщайте о подозрениях в полицию, даже если вы не стали жертвой мошенников! А если вас обманули, подайте заявление в ближайшее отделение Государственной полиции или в электронном виде на портале Latvija.lv. Для проверки отправляйте предупреждение о различных подозрительных действиях в интернете в полицию на мобильное приложение Mana Drošība.

**Дополнительная информация:**

Сабине Спурке

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

Т. +371 20604166

Руководитель по коммуникации

Ассоциация финансовой отрасли