Безопасность денег – в собственных руках.

Как распознать попытки мошенничества и как действовать, столкнувшись с ними? Знайте, распознавайте и не попадайтесь!

Мошенники чаще всего звонят!

Если раньше мошеннические предложения чаще всего появлялись в электронной почте, то теперь популярнее стали телефонные звонки.
Ни в коем случае не разглашайте данные о себе! Не вводите и не называйте коды доступа к своему интернет-банку и не подтверждайте с помощью Smart-ID / калькулятора кодов действия, не инициированные вами. Если все же вы разгласили данные, незамедлительно свяжитесь со своим банком, чтобы по возможности быстрее заблокировать доступ и защитить свои деньги.

Номер телефона – не признак для распознавания!

Мошенники могут звонить и с зарубежного номера, и с поддельного латвийского номера. Они могут выдавать себя за представителей банка.
Чем раньше вы закончите такой разговор, тем меньше риск разгласить какие-то важные данные. Мошенники отлично умеют вытягивать информацию во время разговора.

Предприятия могут получать поддельные электронные письма деловых партнеров!

Мошенники могут использовать поддельную электронную почту, с которой письма отправляются вроде бы от деловых партнеров, или же чтобы вытянуть информацию (если нажмете на включенные в электронное письмо ссылки на сайты), или же чтобы выманивать деньги через фальшивые счета.
Обращайте внимание на то, с какого адреса отправлено электронное письмо. Кроме того, проверяйте, какой адрес скрывается за включенными в текст ссылками на сайты. Ни в коем случае не позволяйте инсталлировать программатуру с таких сайтов и не вводите в них персональные данные.

Упоминание персональных данных – не повод доверять!

Упоминание персональных данных – не повод доверять!
Сильная сторона мошенников – торопить, упоминать ваши данные и уговаривать. Мошенник по доступной в интернете или полученной преступным путем информации может знать ваши имя, фамилию, телефонный номер и даже персональный код или номер платежной карты.
Если имеются хоть малейшие сомнения в идентичности звонящего, положите трубку и лично свяжитесь со своим банком или другим предприятием, за представителя которого выдает себя звонящий, чтобы убедиться в том, какова на самом деле ситуация.

Подозрительные электронные письма от руководителя предприятия

Мошенники могут отправлять поддельные электронные письма, выдавая себя за руководителя предприятия или другого члена руководящей команды и призывая сделать перечисления или разгласить информацию.
Если получаете нетипичную просьбу руководителя или же если она предусматривает перечисления денег или разглашение конфиденциальной информации, лучше лишний раз убедиться в том, что руководитель действительно отправил такое электронное письмо. Обратите также внимание на правописание отправителя электронного письма и на используемые стиль и грамматику.

Код Smart-ID приравнивается к э-подписи!

Операция, подтвержденная Smart-ID или калькулятором кодов, приравнивается к э-подписи – любая операция, которая подтверждена Smart-ID или калькулятором кодов, практически исключает возможность ее исправить.
В приложении Smart-ID перед подтверждением операции видна именно та информация, которая подтверждается. Никогда не подтверждайте операции, в целях которых вы не уверены! Лучше несколько раз проверить, чем подтвердить, не глядя.

Берегите данные!

Очень тщательно надо относиться к вводу данных и на мало известных, и на крупных и широко известных платформах, например, в соцсетях. Нередко данные о человеке доступны публично. Кроме того, их можно получить у поставщиков услуг при слабой защите данных. Возможно, данные украдены у самого пользователя.
Делайте покупки только в известных интернет-магазинах и обращайте максимальное внимание на то, на каких сайтах регистрируетесь и какие данные там просят ввести. Всегда ли они необходимы для обеспечения услуги? Чтобы беречь свои устройства и носители данных, установите надежные пароли и не открывайте подозрительные документы/приложения.

Угроза вымогательства!

Мошенники могут угрожать утечкой данных, заставляя сотрудника принимать нерациональные решения. Они пугают тем, что не подлежащая публикации информация может подвергнуться утечке, и тем самым стараются выманить деньги или уговорить установить мошенническую программатуру. Таким образом мошенники действительно могут получить доступ к данным, которые зашифруют или сделают недоступными, запросив оплату за их разблокирование.
Не поддавайтесь угрозам, даже если они кажутся настоящими – проверьте их достоверность. Если мошенники имитируют одного из коллег, не стесняйтесь связаться с этим коллегой и выяснить правду. Кроме того, проинформируйте коллег из службы безопасности (если таковая имеется).

Просят обновить данные?

Под призывом подтвердить свою идентичность и обновить данные доступа может скрываться мошенническая схема, цель которой – убедить поделиться ценной информацией, например, данными банковской карты. Подобные электронные письма обычно делаются похожими на официальные извещения из банка или других учреждений.
Проверьте, включен ли в адрес электронной почты отправителя правильный адрес домашней страницы, не вклинилась ли туда лишняя цифра или буква. Если электронное письмо кажется подозрительным, удалите его и сообщите о попытке мошенничества. Избегайте открытия подозрительных приложений – даже антивирусные программы зачастую не могут идентифицировать атаки.

Несколько рекомендаций

- Не торопитесь, убедитесь в достоверности упомянутых фактов
- Проверяйте реквизиты получаемых счетов – мошенники могут использовать реальные реквизиты, в которые вводят свой номер банковского счета
- Не открывайте сайты, где просят ввести данные или установить программатуру
- Международные предложения по электронной почте – это обычно попытка мошенничества
- Не используйте пиратскую программатуру, она зачастую служить основанием для шантажа и вымогательства
- Установите дневные и месячные лимиты перечислений, соответствующие хозяйственной деятельности вашего предприятия

Swedbank