# К сведению граждан пожилого возраста!

# ОСТОРОЖНО МОШЕННИКИ!

Злоумышленники не оставляют попыток **обмануть** доверчивых граждан - в последнее время все чаще звонят по Viber якобы от имени банка. Их легенды бывают убедительными, и некоторые люди сообщают мошенникам данные карточек.

**- Как мошенники чаще всего обманывают белорусов в интернете по телефону, когда пытаются украсть деньги?**

- Наиболее часто мошенники используют для выманивания денег технологии социальной инженерии. Это психологическое манипулирование людьми для побуждения их на какие-то определенные действия или разглашение конфиденциальной информации. Самые распространенные для нашей страны - вишинг (с использованием телефонной связи), фишинг (поддельные сайты, на первый взгляд идентичные оригиналу), взлом социальных сетей и рассылка сообщений от чужого имени с просьбой выслать деньги.

**Цель одна** - хищение денежных средств.

**- Какие предлоги используют злоумышленники, которые, используя телефонную связь, выманивают у людей конфиденциальную информацию?**

- Вишинг-мошенники могут представляться сотрудниками банка, работниками госучреждений или, например, покупателями, которые звонят по объявлению о продаже, размещенному на виртуальных торговых площадках или в социальных сетях. Для этого используются различные схемы: возможность устранить проблему с неожиданно списанными деньгами, сообщение о якобы оформленном кредите, отмена "ошибочно" выполненного перевода на карточку жертвы, история о преступниках, которые пытаются незаконно использовать карточку, угроза блокировки карточки и др. И, конечно же, по их словам, избежать всех этих неприятностей можно только сообщив "сотруднику" персональные данные - реквизиты банковской платежной карточки, сеансовые одноразовые коды, которые приходят в СМС-сообщениях на телефоны, логины и пароли и др.

Для убедительности и правдоподобия мошенники пользуются профессиональной терминологией, говорят быстро и уверенно, при разговоре слышен офисный шум, имитирующий работу кол-центра. При этом зачастую они давят на эмоции людей, уверяя, что случится что-то непоправимое, торопят и запугивают. В большинстве случаев номера телефонов звонящих могут быть скрыты либо принадлежать операторам связи других государств. Мошенники могут также использовать специальные программы, изменяющие номера телефонов, с которых идут звонки, тогда они определяются как официальные номера, указанные на сайте банка. Они также используют официальные логотипы банков и других учреждений. Зачастую для звонков используется Viber.

**Помните:** сотрудники банков никогда не используют Viber для звонков клиентам. Банк никогда не будет запрашивать пароли и другие секретные данные. Сотрудник банка при звонке клиенту заранее должен знать все необходимые сведения.

**- Что делать, если человеку звонят с номера банка и просят предоставить конфиденциальную информацию?**

- Уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и наберите официальный номер банка. Но даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. *Наберите номер кол-центра банка вручную. Телефон банка можно найти на обратной стороне банковской платежной карточки или на официальном сайте банка.*

**- А если мошенникам все же удалось получить реквизиты карточки?**

- Если реквизиты банковской платежной карточки стали известны третьим лицам (реквизиты скомпрометированы), ее необходимо срочно заблокировать. Это можно сделать несколькими способами: позвонить в кол-центр обслуживающего банка, воспользоваться возможностями мобильного, интернет- или СМС-банкинга, обратиться лично в отделение банка.

**- Что делать, если деньги все-таки украли?**

- При наличии несанкционированного списания денежных средств со счета карточки, независимо от размера нанесенного ущерба, нужно как можно скорее обратиться в правоохранительные органы. Любые сведения о злоумышленниках помогут раскрыть преступление.

**Давайте еще раз назовем правила безопасности, которые помогут людям защитить деньги на счетах от телефонных мошенников.**

Это простые правила, выполнять которые не составит труда.

**Первое** - ни под каким предлогом никому не сообщать личные данные (ФИО, паспортные данные), реквизиты самой банковской платежной карточки (номер банковской платежной карточки, срок ее действия) и секретную информацию (CVC/CVV-код на оборотной стороне карточки, коды из СМС-сообщений, ПИН-код). Подключите услугу дополнительной безопасности 3D-Secure (добавочное подтверждение операций, совершаемых в интернете).

**Не доверяйте** слепо СМС-сообщениям. Не спешите переходить по ссылкам из сообщений "от банка". Присматривайтесь к написанию имени сайта и наличию у браузера отметки, что сайт безопасен. В любой непонятной ситуации звоните в банк по официальному номеру и уточняйте информацию. Полезно также подключить услугу СМС-оповещения, которая позволит получать уведомления о совершенных операциях и мгновенно узнавать о неправомерных действиях, а значит, и своевременно реагировать на угрозу.

# «Помощь» в оформлении кредита

Как это выглядит: **в социальных сетях нередко можно встретить предложения о помощи в оформлении и получении кредита.** Например, мошенник может представиться сотрудником банка, у которого есть возможность «поправить» систему так, чтобы она вас одобрила. В дальнейшем мошенники выманивают паспортные данные, номер мобильного телефона и код из SMS-сообщения. На имя физического лица оформляется онлайн-кредит, однако денежные средства ему не передаются – мошенники используют их по своему усмотрению.

Кроме того, существует множество организаций, которые выступают посредниками между банком и клиентом (кредитные брокеры). Они предлагают свои услуги и в Интернете: помощь в оформлении кредита, подбор оптимального кредитного продукта и т.д. Такие компании рассчитывают на процент от суммы оформленного вами кредита, что непосредственно будет указано в договоре. Главное, в случае использования такой услуги отличить легальных брокеров от недобросовестных, так называемых «черных» брокеров, которые используют нечестные, и даже противоправные методы (например, внесение в заявку несоответствующих действительности сведений о доходе,  оформление через девайс клиента якобы  от имени клиента кредита на более крупную сумму, или кредитов, в целях увеличения суммы гонорара). Даже в случае отказа по заявке от банка, такие «специалисты» возвращать деньги за свои услуги не будут, так как в подписанном вами договоре будет указано, что вы платите за «информационные» услуги.

**Что делать:** обращаться за кредитом только лично.