**Предупредить легче, чем найти злоумышленников…**

Последние несколько десятилетий в Беларуси, как, впрочем, и во всем мире, отмечается бурный рост компьютерных технологий. Практически все трудоспособное население страны, так или иначе, вовлечено в активности, связанные с вычислительными ресурсами, чаще всего происходящими в сети Интернет. На этом фоне отмечается и значительный рост преступлений с ними связанных, львиную долю которых составляют хищения с использованием компьютерной техники.

Прогнозируется, что развитие IT-отрасли и финансово-кредитной сферы, будут способствовать сохранению тенденции увеличения числа киберпреступлений.

Одним из основных приемов мошенничества является осуществление мошенниками звонков с использованием подмены номера (IP-телефония), что в свою очередь позволяет использовать номера, которые похожи на номера банков с официальных сайтов. Нередко для осуществления звонков используется мессенджер «Viber» с изображением логотипа банковского учреждения. Потенциальной жертве мошенники представляются сотрудниками банковского учреждения, сообщают о попытках совершения подозрительных операций по счету, предлагают подтвердить их легитимность, сообщив реквизиты платежных карточек (номер, срок действия карточки, СVV/CVC-код), СМС-кодами, направляемыми от имени банковского учреждения.

**Что важно знать если:**

1. **Поступают звонки с анонимного номера или номера схожего   
   с номером банка.**

Сотрудники банка не вправе выяснять в ходе телефонной беседы конфиденциальные сведения о клиенте (полный номер банковской платежной карты, срок ее действия, CVV-код, личный номер паспорта клиента, содержание СМС-сообщений от банка, и т.п.).

1. **Собеседник просит скачать какие-либо приложения   
   из магазина приложений для мобильных устройств “PlayMarket”   
   или “AppStore”.**

Сотрудники банка никогда не просят устанавливать какие-либо приложения, так как программы, предлагаемые для скачивания «лжебанкирами», являются программами удаленного доступа и управления компьютерами и другими устройствами под управлением Windows, MacOS, Linux, а также Androidи iOs

1. **СМС якобы от банка приходит в новую переписку.**

Не спешите переходить по ссылкам в сообщениях, предоставленных якобы банком.

1. **Собеседник не может ответить на простые вопросы,   
   при условии того, что настоящий сотрудник банка видит наэкране компьютера всю информацию о клиенте, которая есть в базе банка.**

Если собеседник не готов ответить на простой вопрос, например, назвать остаток по карте или последнюю операцию, то вероятно это мошенник.

1. **Собеседник спрашивает данные карты или СМС-код.**

Смс-код — один из главных паролей. Сотрудники банка никогда его не спросят, так же как и CVV на обратной стороне карты.

1. **Вам обещают выгоду без усилий.**

Чтобы завлечь жертву, мошенники обещают солидный доход быстро и без усилий: суперприбыльную работу, беспроигрышные конкурсы, курсы, которые сделают всех богатыми. Но мошенники могут взять предоплату за обучение и пропадут. Или посулят приз и выманят у вас данные карты якобы для перевода выигрыша.

1. **Собеседник торопит вас или пытается переубедить.**

Сотрудник банка никогда не будет настаивать или торопить клиента.

1. **Ошибки в сообщении.**

У банка есть бдительные редакторы, а вот мошенники пишут   
с ошибками. Не дайте неграмотному преступнику вас обмануть.

1. **Имя отправителя написано неправильно.**

Мошенники регистрируют адреса, похожие на названия банков. Тут срабатывает особенность восприятия: мы считываем смысл слов даже, если буквы в них перепутаны. Когда приходит такое СМС, вас должно насторожить ещё и то, что сообщение оказалось в новой переписке.

**ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ:**

Если вы хотите убедиться в надёжности собеседника, спросите его имя, а после перезвоните в банк по официальному номеру и попросите переключить на человека, который вам звонил.

Если не уверены в собеседнике, попросите его назвать номер карты или остаток на счёте.

Не паникуйте, если вам сообщают о блокировке счета. Позвоните в банк по номеру, указанному на сайте или на карте.

Не обращайте внимание на обещания лёгких денег или выгоды без усилий.

Если собеседник торопит вас или спрашивает смс-код, то вы говорите с мошенником!

Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.

Вторая распространенная разновидность мошенничества - получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2код) – путем направления пользователю в мессенджерах либо по электронной почте от имен известных брендов ссылки на сайт, внешне не отличимый от официального. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, а также реквизиты банковской платежной карты, что позволяет в дальнейшем мошеннику получить доступ к аккаунтам и банковским счетам.

В последнее время распространены факты использования для мошенничества торговой площадки [Kufar.by](http://kufar.by/). На данный момент известно 6 типичных схем, направленных как на продавцов, так и на покупателей товаров.

**Возможные схемы обмана**

Преступник находит продавца на официальной площадке объявлений, ищет номер продавца в мессенджерах или пишет в соцсетях, представляясь якобы покупателем с Куфара и сообщает что уже совершил предоплату, после чего высылает ссылку на поддельную страницу, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги. Среди данных, которые просит злоумышленник: номер карты, имя держателя, срок действия, CVV-код на оборотной стороне карты. Иногда просит предоставить СМС-код подтверждения платежа, ссылаясь на то, что перевел предоплату и хочет убедиться, что она поступила на счет продавца.

Если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка. Чтобы вернуть ошибочно переведенные средства, он предложит перейти на фишинговый сайт и снова ввести данные своей карты.

В итоге продавец лишается своих средств…

**Рекомендации:**

К любым операциям, производимым с использованием Вашей банковской карты, относится максимально внимательно и осторожно. Терять бдительность никогда нельзя.

Для оплаты покупок в Интернете **завести отдельную карту**  
и не хранить на ней много денег.

**Если Вам прислали ссылку** на почтовый ящик, в мессенджер или SMS-сообщением, то, независимо от того кто прислал, даже если это Ваш друг, знакомый, государственный орган или организация, с которой Вы постоянно ведете переписку, или абсолютно незнакомый человек, прежде чем ее открывать, следует особенно внимательно проверить доменное имя. При возникновении малейшего сомнения, что ссылка ведет не на официальный ресурс, ее необходимо проверить. Сделать это можно отыскав в интернете официальный сайт и сверив домен, либо проверив информацию о дате регистрации домена (у фишинговых обычно от нескольких дней до нескольких месяцев) на интернет-ресурсе <https://hb.by/whois.aspx> или подобные ему (например: <https://whois.net>, <https://whois.domaintools.com>) в поле «CreationDate».

Преступность в сфере противодействия киберпреступности характеризуется высокой степенью латентности, в результате чего реальное количество киберинцидентов существенно выше. Однако во всех случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Поэтому ПОМНИТЕ, основной проблемой является наша БЕСПЕЧНОСТЬ. Не стесняйтесь быть бдительными сохраняя свои деньги…

Первый заместитель начальника

ОВД Калинковичского райисполкома

– начальник криминальной милиции В.А.Карасев