УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«Актуальные схемы киберпреступлений и методы борьбы с ними»

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя ваши эмоции.

С клиентом банка посредством телефонного звонка или в социальных сетях связывается мошенник под видом представителя банка или с аккаунта друга, родственника. В ходе звонка или переписки собеседник описывает свою сложную жизненную ситуацию и просит ему материально помочь или «запугивает» ложной информацией о сомнительных операциях с банковской карточкой (наличии заявки на кредит, блокировке счета, мошеннических атаках и др.), представляясь работником банка, и предлагает для сохранения оставшихся денежных средств перевести их на новый счет. Собеседник говорит очень убедительно и, как правило, торопит развивающиеся события.

Сценарии могут быть разными, а итог один: клиент самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли. Поэтому такие случаи не относятся к принципу «нулевой ответственности» банка, так как конфиденциальные данные злоумышленнику сообщили вы сами.

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в банк по номеру, указанному на Вашей банковской карте, официальном сайте либо прийти в офис лично.

Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по номерам, указанным на вашей банковской карте либо официальном сайте финансового учреждения;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было

сообщений от Банка – это повод уточнить ее достоверность и перезвонить в Банк по официальным номерам;

4. Работники банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему Интернет-банкинга. В такой ситуации немедленно прервите разговор и свяжитесь с Банком по официальным номерам.
5. Никому не сообщайте данные своей карточки и всегда держите её в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт для входа в систему Интернет-банкинга или официальное мобильное приложение соответствующего банковского учреждения;
8. Регулярно обновляйте пароли, используемые для входа в систему Интернет-банкинга, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые не совершались ее держателем, необходимо оперативно обратится в Банк по официальным номерам или заблокировать карточку самостоятельно в Интернет/М-банкинге (при наличии такой возможности).

Что бы обезопасить себя и повысить уровень цифровой грамотности, рассмотрим самые распространенные на текущий момент схемы мошенничества:

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber, WhatsApp и Telegram. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка. У мошенников есть возможность звонить с номеров, похожих (реже – полностью совпадающих) на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (зачастую сопровождаемый фразой «Никому не сообщайте!»),

реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить:

- «*Мы звоним с официального номера, проверьте на сайте*».
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные».*
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

Еще один из способов получить доступ к Вашим денежным средствам, используя методы социальной инженерии, побудить клиентов банковских учреждений установить сторонние мобильные приложения для удаленного доступа в мобильное устройство потенциальной жертвы. Для примера, одним из таких приложений является “AnyDesk - удаленное управление” из сервисов Google Play/App Store.

Звонки осуществляются, как правило, на мобильные телефоны из указанных выше мессенджеров. При этом мошенники представляются сотрудниками банка, сообщают о якобы зафиксированных попытках совершения подозрительных операций на внушительные суммы, предлагают подтвердить их легитимность. В ходе разговора, с целью скорейшего вхождения в доверие, опрашивают клиента, задавая вопросы общего характера: «Передавалась ли БПК третьим лицам», «Доставляются ли СМС-оповещения» и т.п. Сообщают о блокировке сомнительных операций и счета клиента. Для повышения степени защищенности Интернет-банкинга и восстановления доступа к счету клиенту настоятельно рекомендуют установить приложение «AnyDesk - удаленное управление» из сервисов Google Play/App Store. В случае согласия пострадавшего, конечно же, оказывают помощь и консультацию в

установке. Установленное приложение позволяет злоумышленникам получить удалённый доступ к вашему устройству.

2. «Потенциальный покупатель»

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети Интернет. По каким-то причинам «покупатель» не может сегодня привезти или перечислить деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в Интернете путем обычного поиска.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

3. «Сообщения в социальных сетях»

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

4. «Розыгрыши/раздачи/опросы от Банка или иных организаций»

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» либо для зачисления денежных средств в честь

юбилейной даты со дня образования того или иного финансового учреждения. Цель опроса — изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение. Однако, по окончанию опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения или ввести персональные данные Вашей карты для зачисления на нее денежных средств.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации, а не ресурс, ссылку на который прислал мошенник или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

5. «Фишинг и новшества в различных платежах»

Дополнительно хотим рассказать о новой мошеннической схеме, которая в текущее время широко распространена на территории Российской Федерации и, к сожалению, может быть актуальна для граждан Республики Беларусь.

Злоумышленниками по электронной почте рассылаются фальшивые уведомления об оплате долгов за жилищно-коммунальные услуги, которые возникли за время самоизоляции. В письмах сообщается о задолженности и просьбой оплатить поддельные квитанции онлайн, либо предоставить сведения об уже совершенной оплате. В случае, если клиент начинал производить оплату и вводить реквизиты карточки на сайте, куда его привели ссылки из письма, мошенники получали доступ к его счету. В случае игнорирования клиентом подобных сообщений, ему звонили от лица управляющей компании и убеждали в наличии «долга по квартплате». При этом мошенники пытались выяснить способы оплаты и реквизиты карточки, по которой проводился платёж, и предлагали совершить «тестовую транзакцию для проверки», а также сообщить им код из SMS.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные. Ведь Ваша безопасность в первую очередь в Ваших руках!