**Мошенники в киберпространстве и как им противостоять!**

В настоящее время Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека.   
С одной стороны, это открывает перед гражданами и обществом ряд перспектив, с другой – влечет появление новых рисков и угроз. Так, бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений.

Вопросы цифровой трансформации преступности сегодня являются одними из наиболее злободневных. И от того, насколько эффективно удастся противостоять этому вызову, зависит не только защищенность прав и интересов граждан, но и информационная безопасность общества и государства.

В 2022 году в Брестской области наблюдалась характерная для республики тенденция уменьшения числа зарегистрированных киберпреступлений. Всего в области в 2022 году зарегистрировано 1626киберпреступлений (январь-декабрь 2022 - 1984, -18%). По отношению к аналогичному периоду прошлого года (далее - АППГ) по республике в целом также наблюдается снижение числа зарегистрированных киберпреступлений (с 16446до 14839, -9,8 %).

Как следует из статистических данных, падение количества зарегистрированных киберпреступлений обусловленоснижением количества зарегистрированных хищений путем модификации компьютерной информации (с 1801 до 1385, -23,1 %).

Следует учесть, что абсолютное большинство (1385, 85,2 %) зарегистрированных преступлений составляют хищения путем модификации компьютерной информации, причем 1168 (84,3 %) из них совершено без использования терминальных устройств с использованием методик «вишинга» и «фишинга», что создает объективные проблемы по установлению лиц их совершивших. Из 217 преступлений, совершенных с использованием терминальных устройств, расположенных на территории Республики Беларусь (т.н. «бытовых»), на текущий момент раскрыто 195 (89,9 %).

В 2022 году в Пружанском районе наблюдалась также тенденция уменьшения числа зарегистрированных киберпреступлений. Всего в 2022 году зарегистрировано 42 киберпреступления (2021 - 42, -25%). Установлен подозреваемый по 9 преступлениям(2021 – 14), при удельном весе 21,4%.

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.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;

2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;

3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.

**Помните!** Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.

**Обращаем Ваше внимание**, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.

Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.

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.

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 указанному на банковской карте или официальном сайте номерам;

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;

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 дистанционного банковского обслуживания (Интернет-банкинг, М-банкинг и другие). В такой ситуации немедленно прервите разговор и свяжитесь с Банком;

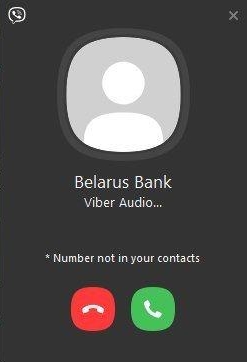
5. Никому и никогда не сообщайте данные своей карточки и всегда держите ее в поле зрения при совершении платежей;

6. Обязательно подключите 3D-secure и смс-оповещение;

7. Используйте только официальный сайт Банка для входа в систему Интернет-банкинга или официальное мобильное приложение;

8. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания, а также для подтверждения платежей;

9. В случае выявления действий по карточке, которые вами не совершались, необходимо оперативно обратится в Банк или самостоятельно заблокировать карточку в системе дистанционного банковского обслуживания.

**Рассмотрим самые распространенные схемы мошенничества сейчас**:

**«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. 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 на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

**У вас просят конфиденциальные данные**

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 (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVС-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» (вы слышите в трубке лёгкий шелест).

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!

**«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 деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

**Ссылка**

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.

**QR-код**

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.

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

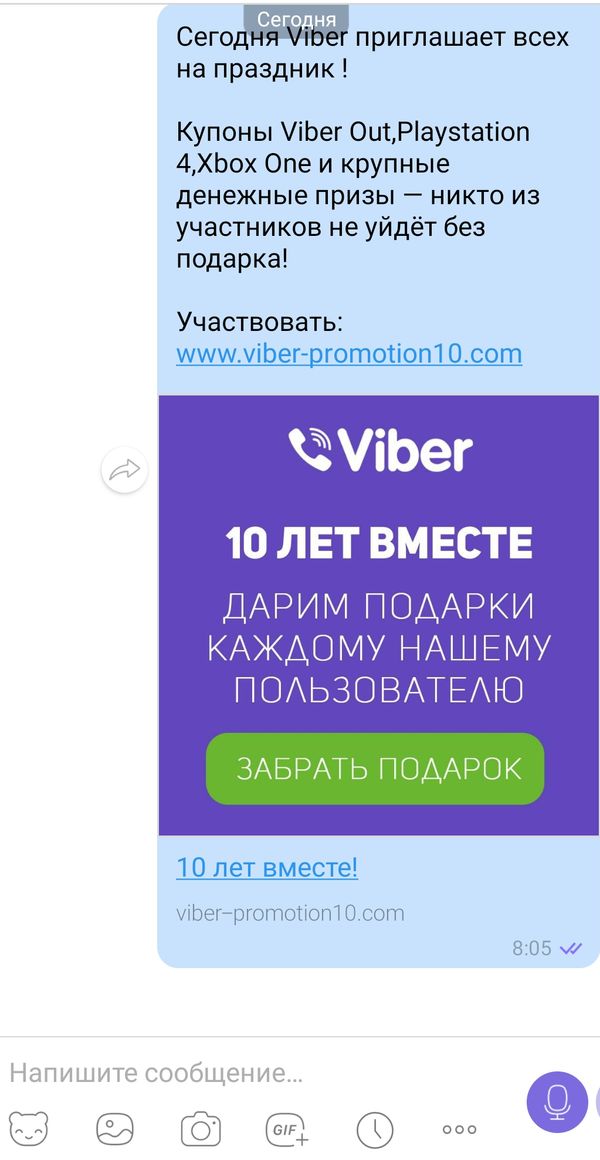
**«Сообщения в социальных сетях»**

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.

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

«**Розыгрыши/раздачи/опросы от Банка или иных организаций»**

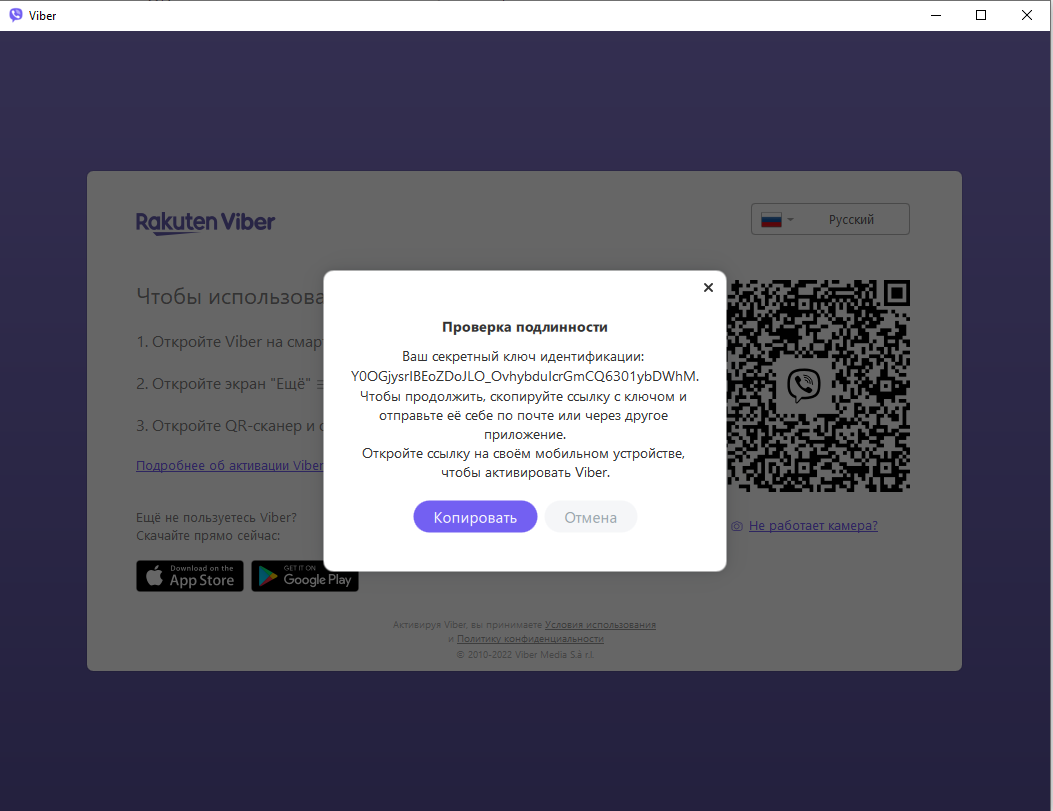
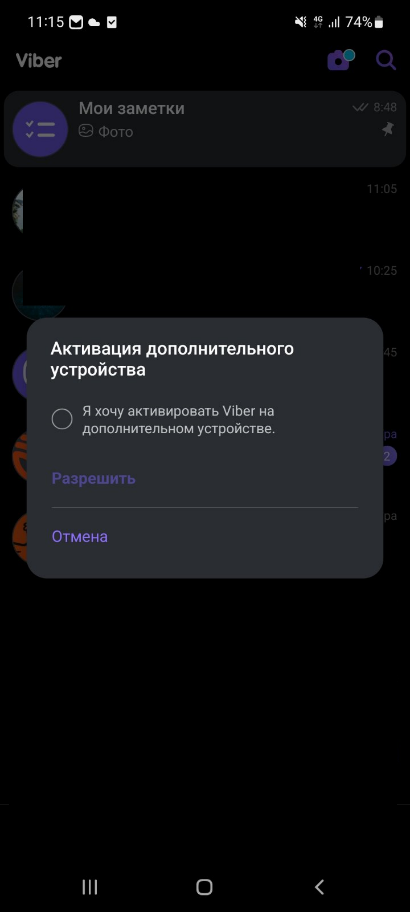
Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.

Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего –ввести данные Вашей банковской карты.

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 или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

**«Взлом» учётной записи мессенджера «Viber»**

Получение доступа к учётным записям пользователей мессенджера «Viber» возможно посредством использования десктопного приложения данного мессенджера (далее – ПО), установленного на ПЭВМ. После осуществления установки данного ПО, пользователю предлагается осуществить копирование данных с мобильного устройства, где установлено мобильное приложение «Viber» на ПЭВМ. Осуществление указанных действий возможно путём сканирования QR-кода камерой мобильного устройства или создания ссылки активатора, создаваемой путём выбора пункта «Не работает камера?». Сформированную ссылку злоумышленник рассылает посредством любых источников передачи данных. После осуществления перехода по указанной ссылке, пользователь мессенджера «Viber» получает системное уведомление содержащие в себе текст согласия на активацию учетной записи мессенджера «Viber» на другом устройстве. Когда пользователь разрешает данное действие, учётная запись копируется на устройство, посредством которого была сгенерирована вышеуказанная ссылка. Одновременно с этим, пользователю мобильного устройства показывается информационное окно с кнопкой «Синхронизация», посредством которой (при её нажатии) будет осуществлена синхронизация контактов и сообщений между мобильным устройством и ПЭВМ на котором дополнительно активирован «Viber». После производства вышеуказанных действий злоумышленник получает доступ к использованию учётной записи мессенджера «Viber» пользователя, прошедшего по ссылке.

**Важно!** Не переходите по подозрительным ссылкам. Обращайте внимание на действия, которые вам предлагает осуществить приложение.

**Сайты знакомств**

С каждым днем мошенники придумывают все больше новых уловок, с целью «легкого заработка» на наших доверчивых гражданах. Вот одна из них. Мошенники регистрируют вымышленные анкеты на различных сайтах знакомств и, представившись девушкой, вступают в переписку с доверчивыми мужчинами. После непродолжительной переписки на сайте знакомств злоумышленник предлагает продолжить общение в интернет-мессенджере (обычно «Telegram»). В процессе общения следует предложение сходить в кинотеатр, драмтеатр и др. Для приобретения или бронирования билетов злоумышленник в мессенджере отправляет фишинговую (поддельную) ссылку, переходя по которой для приобретения соответствующих билетов необходимо ввести реквизиты банковской платежной карты. Мошенники подкупают интерес тем, что идет очень редкое представление, поэтому билеты могут раскупить.

Введя реквизиты своей банковской карты, мужчина теряет все свои денежные средства, находящиеся на лицевом счете, к которому выпущена указанная карта.

**Важно!** Не вводите реквизиты своей банковской карты на сайтах, на которые перешли по ссылкам незнакомцев. Помните, что визуально подмену заметить сложно. Мошеннические страницы могут быть как две капли воды похожи на официальные сайты торговых площадок или служб доставки.