**ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ.**

В настоящее время сеть Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. С одной стороны, это открывает перед обществом ряд перспектив, с другой - влечет появление новых рисков и угроз. Бурное развитие телекоммуникационных технологий, развитие дистанционных способов совершения преступлений, при которых отсутствует прямой контакт между злоумышленниками и их жертвами, вызванный распространением коронавирусной инфекции Covid-19 переход многих сфер общественных отношений в интернет-пространство, а также недостаточно высокий уровень цифровой безопасности граждан привели 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. При этом универсальных подходов, позволяющих эффективно противодействовать высокотехнологичным преступлениям, не выработано ни одним государством мира.

Причины, повлиявшие на снижение темпов роста киберпреступлений:

*Активная деятельность по пресечению киберпреступлений.*

В этом году пресекалась деятельность действовавших на территории республики «дроп»- и «обнал»-сервисов, а также лиц, занимавшихся обменов похищенных денег с банковских счетов граждан в криптовалюту. Это позволило существенно затруднить злоумышленникам вывод похищенных денег. Последние задержания участников преступных групп, занимающихся «обналом», показали, что подставные банковские карточки регистрируются и обналичиваются приезжими гражданами сопредельных государств.

**Пример 1.** *В результате проведения оперативно-розыскных мероприятий установлены и задержаны участники преступной группы, состоящей из 23 жителей г.Минска, которые с ноября 2020 г. по апрель т.г. осуществили хищение денежных средств путем модификации компьютерной информации у клиентов белорусских банков путем вишинга. Общая сумма материального ущерба составил около 1.450.000 рублей, установлено более 100 потерпевших. В отношении фигурантов возбуждено свыше 100 уголовных дел по ч.2,3- ст.209, ч.2,3,4 ст.212 УК. Получена информация о причастности фигурантов к более 1000 аналогичных преступлений, совершенных на территории республики.*

**Пример 2.** *В конце августа т.г. задержан иностранный гражданин, который в период, с 17 по 28 сентября в составе преступной группы осуществил хищение денежных средств путем модификации компьютерной информации у более 50 граждан Беларуси.*

Активная информационная и профилактическая работа в СМИ, трудовых коллективах и учебных заведениях.

Уровень компьютерной грамотности граждан недостаточно высок и существенно отстает от скорости внедрения тех или иных компьютерных систем в повседневную жизнь. К тому же многие белорусы недостаточно ответственно относятся к защите и безопасности собственной информации и личных данных.

**Какие схемы используют мошенники на** [**Kufar**](https://support.kufar.by/hc/ru)**е**

[**Kufar**](https://support.kufar.by/hc/ru) **—** это самая известная и популярная онлайн-площадка бесплатных объявлений в Беларуси.

**Для продавцов - Предоплата №1**

1. Преступник находит продавца на площадке объявлений, копирует его контактные данные, но на площадке не пишет, - [заблокируют](https://support.kufar.by/hc/ru/articles/360008919837). Ищет номер продавца в мессенджерах, представляется якобы покупателем с Куфара, говорит, что готов купить товар по предоплате.

2. Высылает продавцу ссылку на [поддельную страницу](https://support.kufar.by/hc/ru/articles/360009544877) предоплаты, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги от покупателя.

3. Естественно, никаких денег продавец не получит  - как только он [введет данные](https://support.kufar.by/hc/ru/articles/360003117578) своей карты, преступник получит доступ к его счету.

**Для продавцов - Предоплата №2 (Продвинутая)**

1. Если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка.

2. Чтобы вернуть ошибочно переведенные средства, он предложит перейти на [фишинговый сайт](https://support.kufar.by/hc/ru/articles/360006772838) и ввести данные своей карты.

3. Если продавец это сделает, мошенник повторно спишет деньги.

**Для покупателей. Доставка №1 (Базовая)**

1. Преступник выставляет товар с крайне выгодной ценой.

2. Когда потенциальный покупатель пишет ему, под любым предлогом предлагает перейти  в [мессенджер](https://support.kufar.by/hc/ru/articles/360008919837). Говорит, что на Куфаре неудобно общаться, что в мессенджере можно созвониться и т.п.

3. Уговаривает покупателя на предоплату или доставку под любым предлогом: уехал из города, боится встречаться во время эпидемии коронавируса, нет времени.

4. Чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств, которая появилась на Куфаре: если доставки не будет, Куфар автоматически вернет средства на карту.

5. Высылает покупателю ссылку на [поддельную страницу](https://support.kufar.by/hc/ru/articles/360009544877), которая имитирует страницу Куфар Доставки, где нужно ввести данные карты, чтобы совершить предоплату.

6. Как только пользователь вводит данные своей карты, с него списываются деньги, посылка не приходит.

**Для покупателей. Доставка №2 (Продвинутая)**

1. После того, как предыдущая схема полностью реализована, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем.

2. Говорит, что произошла ошибка, товар уже забрали (или передумал подавать), готов вернуть деньги.

3. Высылает ссылку на [поддельную страницу](https://support.kufar.by/hc/ru/articles/360009544877) возврата средств, где покупателю нужно ввести данные своей карты и точную сумму, которую ему должны вернуть.

4. После того, как покупатель повторно вводит данные своей карты, с него повторно списывается та же сумма (если повезет) или все деньги.

**Для покупателей. Доставка №3 (Наглая)**

1. После того, как мошенник реализовал схему Доставка 1.0, он пишет пострадавшему покупателю, представляется службой поддержки Куфара.

2. Говорит, что посылка была не доставлена, извиняется и рассказывает про возможность возврата средств за посылку.

3. Присылает ссылку на [фишинговую страницу](https://support.kufar.by/hc/ru/articles/360006772838), где покупателю нужно вбить данные своей карты и сумму, которая соответствовала сумме предыдущего списания.

4. После того, как покупатель повторно вводит данные своей карты, мошенник повторно крадет деньги с банковского счета.

**Для покупателей. Доставка №4 ( мошенничество с накладными)**

1. Преступник выставляет товар с крайне выгодной ценой.

2. Когда потенциальный покупатель пишет ему, под любым предлогом предлагает перейти  в [мессенджер](https://support.kufar.by/hc/ru/articles/360008919837).

3. Предлагает отправить товар с доставкой. При этом мошенник специально создает ажиотаж вокруг объявления. Он может говорить, что буквально на днях уезжает из города, или что товар готовы купить другие покупатели.

4. Продавец говорит, что можно оплатить товар уже после того, как он его отправит, при этом готов предоставить доказательства.

5. Если покупатель соглашается, в качестве доказательства отправки мошенник высылает ссылку на [поддельную страницу](https://support.kufar.by/hc/ru/articles/360009544877) трекинга посылки или [скан поддельного документа](https://support.kufar.by/hc/ru/articles/360008556817) об оплате. Минимальное знание фотошопа позволяет преступнику сымитировать квиток любой службы доставки, будь то СДЭК, Белпочта или любая другая компания.

6. После того, как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на [фишинговую страницу](https://support.kufar.by/hc/ru/articles/360009544877), где нужно оформить перевод суммы за товар.

7. Как только пользователь вводит данные своей карты, с него списываются деньги, посылка не приходит.

Наиболее актуальные виды киберпреступлений

Одним из самых распространенных киберпреступлений остается хищение денежных средств при помощи модификации компьютерной информации. Причем в большинстве случаев эти преступления становятся возможны из-за беспечности самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

Преступники завладевают реквизитами, необходимыми для осуществлен преступных транзакций, посредством следующих основных способов:

**«Звонок из банка»**

Вишинг (англ, vishing, от voice phishing) - один из методов мошенничества с использованием социальной инженерии, который заключается в выведении злоумышленников жертвы на желаемую модель поведения с целью завладения конфиденциальной информации для последующего хищения средств.

Как правило, для совершения звонка преступники используют один из распространенных мессенджеров, используя функцию подмены номера. Как следствие, у потерпевшего на экране мобильного телефона может отображаться совершенно любой номер телефона, заданный злоумышленником. Также преступники маскируются под логотипом узнаваемых белорусских банко вводя в заблуждение потенциальных жертв.

От имени банковского сотрудника или представителя правоохранительных органов злоумышленники сообщают жертве, что необходимо осуществит какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами банковской платежной карты, преступники осуществляют хищение денежных средств банковского счета потерпевшего.

В последнее время наиболее актуальная схема - побуждение жертв, открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переела впоследствии реквизиты счета.

**Пример 1.** *В конце октября на «Viber» брестчанину позвонил неизвестный и сообщил, что якобы в Минске неизвестный собирается оформить на его имя кредит. С целы пресечения этих действий он посоветовал открыть на свое имя максимально возможны кредит: мужчина открыл кредит на 7,5 тысяч рублей. Также по рекомендации звонящего установил программу удаленного доступа «AnyDesk» и сообщил сеансовый пароль, затем отправил фотографии своего паспорта и реквизиты банковской платежной карты. Вскоре потерпевший обнаружил, что с его основного счета похищены около 800 рублей, полученный кредит переведен через цепочку операций в Россию.*

**Пример 2.** *В конце октября в Пинске местной жительницы на «Viber» позвонил неизвестный и сообщил, что якобы кто-то пытается открыть кредит на ее имя. По его словам, для предотвращения этого необходимо взять кредиты на максимально возможные сумы. Женщина сделала то, что ей предложил неизвестный, а также по его настоянию установил программу удаленного доступа «AnyDesk» и сообщила сеансовый пароль. В итоге жертва лишилась 12 тысяч белорусских рублей.*

**«Фишинг»**

Фишинг (от англ, fishing - рыбная ловля, выуэ/сивание) - один из видов мошенничества, целью которого является получение доступа конфиденциальным данным пользователей (логинам и паролям) и последующего хищения денежных средств.

Наиболее часто данная преступная схема реализовывает в отношении клиентов торговых интернет-площадок. Выступая в роли покупателя, злоумышленник находит продавца товара и вступает с ним в переписку мессенджерах («Viber», «Telegram», «WhatsApp»). Он сообщает, что товар его заинтересовал и уже якобы совершил предоплату (зачастую высылаете скриншот электронного чека о перечислении средств). Для того, чтобы получит данные средства, продавцу якобы необходимо пройти по гиперссылке и ввести данные.

Невнимательный интернет-пользователь может и не заметить подмены так как подобные страницы визуально схожи с оформлением сайтов известны: сервисов (Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.) Адрес поддельной веб-страницы также может напоминать реальный (kufar-dostavka.by, erip-online.com, belarusbank24.xyz, cdek-zakaz.info и др.).

Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

**Пример 1.** *Жительница Бресткой области на торговой интернет-площадке разместила объявление о продаже туфлей. Вскоре в мессенджере «Viber» ей поступило сообщение от неизвестного абонента, который сообщил о желании приобрести товар. Затем он прислал ссылку «https://evropochta.pay-get.by», пояснив, что женщине необходимо ввести реквизиты своей банковской платежной карты для последующего перевода денег за туфли. Она прошла по ссылке, ввела требуемую информацию, и вскоре с ее счета преступник похитил 2 тысячи рублей.*

**Пример 2.** *Борисовчанка через торговую интернет-площадку пыталась продать ставшую ненужную в хозяйстве вещь. Покупатель нашелся быстро: он долго расспрашивал о состоянии вещи и ее потребительских свойствах. Затем отправил женщине ссылку на фишинговый сайт, где нужно ввести данные ее банковской карты для зачисления платежа. Оплаты за товар не поступило, а с счета потерпевшей было списано почти 2 тысяч рублей.*

В последнее время участились случаи создания фишинговых сайтов ориентированных под запросы пользователей в поисковых системах. Граждане попадают на них прямо из Google и Yandex после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска и не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации. В результате введенные данные отправляются преступнику, а не банку.

Также приобрела популярность мошенническая схема, связанная с проведением якобы «рекламных акций» от имени известных в Беларуси торговых брэндов. После прохождения опроса на поддельном сайт (практически не отличимом от оригинального) пользователю для получения выигрыша предлагалось скачать и установить мобильное приложение, привязав к нему бонусную и банковскую карту. Если жертва выполняла это условие - мошенники получали реквизиты для хищения денежных средств.

Иные способы совершения киберпреступлений

Свободный доступ к банковской карте

В ряде случаев причиной хищений с банковских счетов становятся не хитрые схемы мошенников, а банальная утеря карты, оставление ее в легкодоступном месте или передача иным лицам для осуществления разовых платежей. Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому хранилищу преступник получает беспрепятственный доступ к банковскому счету его владельца.

Риск остаться без заработанных денежных средств также увеличивает хранение PIN-кода рядом с картой (например, записанным на бумажке в кошельке или на самой банковской карте).

*Покупка с предоплатой*

Наиболее простой, но от этого не менее работающей формой интернет- мошенничества, является размещение преступниками объявлений о продаже каких-либо товаров по бросовым ценам. Но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

*Шантаж*

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети — это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.

*Онлайн-игры*

Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты банковских платежных карт для покупки игровых преимуществ, коллекционные предметы, которые игроки также нередко приобретают з реальные деньги.

Основные правила цифровой гигиены

**Никогда, никому и ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и банковских карг, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов.**

Также не следует сообщать в телефонных разговорах и при общении соцсетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и сами? позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты. Сообщите о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка не звонил.

В том случае, если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и банк это заметит, то его сотрудники сперва инициативно заблокируют банковскую платежную карту затем сообщат Вам причину принятого решения (ничего не уточняя) и пригласят посетить банк с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты.

Учтите: сотрудники банков никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»).

**В настоящее время просто необходимо наличие второй банковской платежной карты, не привязанной к основному банковскому счету (например, зарплатному).**

Этой картой рассчитывайтесь в сети Интернет, заранее пополняя ее на необходимую сумму. В таком случае Вы сможете обезопасить свой основной банковский счет.

Многие банки предлагают своим клиентам услугу выпуска «виртуальной карты». Процесс ее открытия не требует посещения клиентом банка и представляет собой достаточно быстрый процесс. В итоге Вы станете обладателем электронного аналога банковской карты, посредством которой сможете рассчитываться за услуги в сети Интернет без риска скомпрометировать основной банковский счет. Просто перед оплатой пополните ее необходимой суммой с основной карты - и никаких проблем!

**Ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам!**

Никогда не устанавливайте по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer» и др. Не сообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернет-банкинга на Вашем устройстве и совершить хищение денежных средств.

**Каждый владелец банковских платежных карт может настроит собственный алгоритм безопасности при их использовании.**

Для обеспечения сохранности денежных средств, размещенных н банковских счетах, каждый держатель карточки посредством систем дистанционного банковского обслуживания может установить индивидуальны ограничения (лимиты/запреты).

Среди основных - следующие:

подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов сети Интернет);

установление банком-эмитентом ограничение на проведение расходных операций (максимальная сумма и количество операций в определенный период времени);

возможность самостоятельно устанавливать ограничения (на проведение операций в сети Интернет, на совершение операций в конкретной стране, н совершение отдельных видов операций).

**Для доступа к системам дистанционного банковского обслуживания и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора.**

Рекомендуется составлять комбинации паролей не менее чем из 12 знаков (цифры, буквы и символы в разном регистре). Создавайте уникальные пароли для каждого сервиса в отдельности. Стоит воздержаться от паролей, составленных из дат рождения, имен, фамилий - то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей). Также следует регулярно менять пароли, чем чаще - тем лучше. Пользуйтесь только проверенным менеджерам паролей!

**При поступлении в социальных сетях сообщений от лиц, состоящих в** **категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек - не следует сразу же отвечать на подобные сообщения!**

Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться с этим человеком (по телефону, лично встретиться) и уточнить, действительно ли oн нуждается в помощи.

**В целях защиты устройств необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систем.**

Установить антивирусную программу следует не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

Обязательно расскажите об этих основных правилах «цифровой гигиены» своим родственникам, близким, знакомым и друзьям, ведь в силу возраста или недостаточного уровня финансовой грамотности они могут быть особенно уязвимы для действий киберпреступников!

*Материал подготовлен*

*Хотимским РОВД*