ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ

в рамках профилактической акции
«Декада кибербезопасности»

Минск, ноябрь 2021

Содержание:

Вопрос № 1. Противодействие киберпреступности. Общие сведения

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

Среди факторов, стимулирующих рост киберпреступлений, можно выделить такие, как высокие темпы освоения сети Интернет, вызванный распространением коронавирусной инфекции Covid-19 переход многих сфер общественных отношений в интернет-пространство, развитие дистанционных способов совершения преступлений, при которых отсутствует прямой контакт между злоумышленниками и их жертвами, а также недостаточно высокий уровень цифровой безопасности граждан.

В последние два месяца наблюдается некоторая стабилизация криминогенной обстановки. Так, с начала года зарегистрировано на 17,6% меньше преступлений, чем в аналогичный период прошлого года (13 427; 16 304). Также на 18,8% снизился прирост количества хищений, доля которых в общей киберпреступности составляет 9 из 10 преступлений (так называемые вишинг, фишинг).

Причины, повлиявшие на снижение темпов роста киберпреступлений:

1. *Активная деятельность по пресечению киберпреступлений.*

В этом году пресекалась деятельность действовавших на территории республики «дроп» и «обнал» сервисов, а также лиц, занимавшихся обменом 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 ОРМ установлены и задержаны участники преступной группы, состоящей из 23 жителей г.Минска, которые в период 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 более 100 уголовных дел по ч.2,3 ст.209, ч.2,3,4 ст.212 УК. Получена информация о причастности фигурантов к более чем 1000 аналогичных преступлений, совершенных на территории республики.

Пример 2. В конце августа задержан иностранный гражданин, который в период с 17 по 28 сентября 2021 года в составе преступной группы осуществил хищение денежных средств путем модификации компьютерной информации у более 50 потерпевших граждан Беларуси.

2. Активная информационная и профилактическая работа в СМИ, в трудовых коллективах и учебных заведениях, существенно влияет на снижение количества преступлений данного вида.

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.

В целях реализации Комплексного плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021 – 2022 годы, а также подпункта 1.1 пункта 1 Протокола поручений Министра внутренних дел от 13.04.2021 № 5, с **10 по 20 мая** т.г. в Беларуси проводилась профилактическая акция «Декада кибербезопасности», направленная на совершенствование работы по профилактике киберпреступлений и снижению их числа, повышение уровня цифровой грамотности населения.

В рамках акции реализован комплекс мероприятий по информированию граждан о современных видах киберпреступлений и мерах по противодействию им. В средствах массовой информации за указанный период размещено свыше 80 материалов, проведено около 10 тысяч выступлений в учреждениях образования и трудовых коллективах. Информационно-профилактические материалы размещались в местах массового нахождения граждан, объектах социального назначения и транспортной инфраструктуры.

Вопрос № 2. 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 в результате беспечных действий самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам. Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих 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 хищения средств.

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

От имени банковского сотрудника или представителя правоохранительных органов злоумышленники сообщают жертве, что необходимо осуществить 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 с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы 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, переслав впоследствии реквизиты счета.

Пример 1. В конце октября на «Viber» брестчанину позвонило неустановленное лицо и сообщило, что якобы в Минске неизвестный собирается оформить на его имя кредит. С целью пресечения этих действий он посоветовал открыть на свое имя максимально возможный 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, а полученный кредит переведен через цепочку операций в Россию.

Пример 2. Схожий случай произошел в конце октября в Пинске. Позвонивший на «Viber» местной жительницы неизвестный сообщил, что якобы кто-то пытается получить доступ к ее счету и пытается открыть кредит на ее имя. Якобы для предотвращения этого необходимо взять кредиты на максимально возможные суммы. Женщина выполнила это, а также по настоянию звонящего установила программу удаленного доступа «AnyDesk» и сообщила ему сеансовый пароль. В итоге она лишилась 12 тысяч белорусских рублей.

Пример 3. В середине августа жителю г.Гродно поступил ряд звонков через «Viber» от одного и того же мошенника, который под предлогом выявления недобросовестных банковских работников склонил его к открытию кредита и переводу всей суммы на свой банковский счет. Передав реквизиты, гродненчанин лишился 13 тысяч рублей.

«Фишинг»

Фишинг (от англ. fishing – рыбная ловля, выуживание) – один из видов мошенничества, целью которого является получение доступа к 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 в мессенджерах *(«Viber», «Telegram», «WhatsApp»)*. Он сообщает, что товар его заинтересовал и уже якобы совершил предоплату (зачастую высылается скриншот электронного чека о перечислении средств). Для того чтобы получить данные средства, продавцу необходимо пройти по гиперссылке и ввести данные.

Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных 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 со 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 сайте (практически не отличим от оригинального) пользователю для получения выигрыша предлагается скачать и установить мобильное приложение, привязать к нему бонусную и банковскую карту. Если жертва выполнит это условие – мошенники получат реквизиты и совершат хищение денежных средств.

Вопрос № 3. 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 или 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 просто 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, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

Вопрос № 4. Основные правила цифровой гигиены

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

Не следует сообщать в телефонных разговорах, а также посредством общения в социальных сетях 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 самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка Вам 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.

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., и не

сообщайте сеансовые коды. Через эти приложения мошенники могут получить доступ к мобильному приложению интернет-банкинга на Вашем устройстве и совершить хищение Ваших денежных средств.

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

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

Среди основных – такие, как:

подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов в 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, на 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.

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 данным пользователем (по телефону, лично встретиться) и уточнить, действительно ли он 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!