Профилактика хищений денежных средств граждан с использованием информационно-коммуникационных технологий

Материал подготовлен Гродненским межрайонным отделом Следственного комитета Республики Беларусь

Согласно статистике в текущем (2023) году, как и в прошлом, на территории Гродненской области фиксируется большое количество хищений денежных средств граждан, совершенных с использованием информационно-коммуникационных технологий (далее – ИКТ), большую часть которых составляют хищения путем модификации компьютерной информации (статья (далее – ст.) 212 Уголовного кодекса Республики Беларусь (далее – УК) и мошенничества (ст. 209 УК).

Так, за 8 месяцев текущего года всего в области зарегистрировано **1309** преступлений, совершенных с использованием ИКТ, среди которых **748** хищений путем модификации компьютерной информации, **528** мошенничеств и **33** факта интернет-вымогательства.

Хищение денежных средств путем модификации компьютерной информации злоумышленниками совершается в результате получения доступа к банковскому счету с использованием переданных владельцем счета реквизитов банковской платежной карты, путем доступа к системе «Интернет-банкинг» или мобильному устройству потерпевшего через удаленные программы, а также с использованием похищенной или потерянной банковской платежной карты.

Хищение путем мошенничества совершается в результате использования преступником методов социальной инженерии, когда под видом звонка от сотрудника банковского учреждения или правоохранительных органов гражданина вынуждают добровольно осуществить перевод денежных средств для их сохранения на счете или с целью поимки мошенника, а также в качестве предоплаты за товар в «фейковом» интернет-магазине, за аренду жилья и т.д.

Зафиксированные факты вымогательства в сети Интернет связаны с высказыванием требований перевода денежных средств под угрозой распространения в сети интимных материалов, «попавших» в руки злоумышленнику в ходе доверительной переписки на сайтах знакомств, в социальных сетях, мессенджерах. Доступ к таким материалам злоумышленник также может получить после взлома страниц в социальных сетях и иных аккаунтах.

Схемы и способы, которые используют преступники для хищения денежных средств в сети Интернет

В текущем году, как и ранее, преступниками наиболее часто используется схема так называемого **«вишинга»**, суть которого

заключается в том, чтобы обманным путем заставить человека раскрыть личную или финансовую информацию. Злоумышленники звонят по телефону и, играя определенную роль, к примеру, сотрудника банка, сообщают гражданину, что какое-то лицо оформило на него кредит, либо совершается попытка хищения его денежных средств со счета. В большинстве случаев звонки осуществляются с иностранных номеров. Для отмены кредита, предотвращения хищения денежных средств на счете и поимки виновного предлагается срочно оформить новые кредиты на максимальную сумму платежеспособности, перевести деньги на «безопасный счет» или «защищенную ячейку». Для убедительности к данным звонкам «жертве» также начинают поступать звонки от имени сотрудников правоохранительных органов, подтверждающих наличие проблемы. С целью убеждения в осуществлении перевода денежных средств и участии в мероприятии по выявлению преступника потерпевшему могут также высылаться в мессенджере фотографии служебных удостоверений, злоумышленники инструктируют, как вести себя при оформлении кредита в банке.

В данном случае действуют участники организованных групп. Преступники действуют настолько убедительно, что зачастую потерпевшие осуществляют переводы в течение нескольких дней, имея реальное время подумать над происходящим. Нередко злоумышленники также убеждают граждан устанавливать на мобильный телефон приложения для удаленного доступа к телефону, в ходе чего получают доступ к системе «Интернет-банкинг» и самостоятельно осуществляют хищение денежных средств со счета, в том числе дистанционно оформляя кредиты на граждан.

Второй схемой хищения денежных средств можно выделить функционирование интернет-сайтов, имитирующих различные «**фейковые» интернет-биржи** для заработка денежных средств на торгах. Спам-реклама о данных сайтах широко распространяется в сети Интернет. Доверчивые граждане переходят по ссылке, не проверив историю и отзывы о ресурсе, вступают с так называемыми «представителями биржи» в переписку. Граждан убеждают в высоких доходах, чему способствуют содержащиеся на ресурсе красивые «фейковые» отзывы об эффективности торгов. Убеждают перечислить деньги на предоставленные номера банковских счетов, нередко на криптокошельки. Для убедительности создают «жертвам» личные аккаунты на данных сайтах, где якобы отображаются суммы внесенных денежных средств. А когда человек решает вывести «имеющиеся на счету» и вложенные деньги, начинается «история» о необходимости внесения налога, страховки, компенсации и

т.д., что вынуждает потерпевшего вносить очередные суммы денежных средств.

Третья схема – «**фейковые» интернет-магазины** по продаже товаров (обувь, одежда, мебель и т.д.) в социальной сети **«Инстаграм»**. Страницы с изображением красивых товаров со стоимостью ниже рыночной, с большим числом подписчиков и рядом положительных отзывов не вызывают у будущих жертв сомнения в их подлинности. Желая приобрести тот или иной товар, граждане осуществляют перевод денег в качестве предоплаты за них на подконтрольные злоумышленникам счета.

Четвертая схема – **фишинговые сайты банков, театров и кинотеатров**.

В сети Интернет существует ряд сайтов, имитирующих стартовые страницы системы «Интернет-банкинг». Желая зайти в приложение,

финансового учреждения кроется ссылка на фишинговый сайт, внешне ничем не отличающийся от оригинала, но имеющий иной адрес в браузерной строке. Он может отличаться от правильного адреса всего одним символом. Владелец счета, вводя на таком сайте логин и пароль, предоставляет доступ к своему счету. Через считанные минуты денежные средства переводятся на иной счет.

Аналогично в Интернете распространяются ссылки на поддельные сайты **театров и кинотеатров**. Для покупки билетов необходимо ввести реквизиты банковской платежной карточки и код подтверждения из «службы коротких сообщений» (далее – СМС). Далее происходит хищение денежных средств с карт-счета с использованием реквизитов банковской платежной карты. Нередко покупке билетов предшествует переписка со случайным собеседником в социальной сети, мессенджере, на сайте знакомств.

Пятая схема – торговые площадки с объявлениями о продаже товара, в частности, торговой площадки «Куфар». Обман происходит по следующим схемам: предоплата за продаваемый товар; завладение реквизитами банковской платежной карты под предлогом оплаты товара; хищение путем использования реквизитов банковской платежной карты.

Реже используются **иные** способы хищения денежных средств – завладение деньгами в виде предоплаты по объявлениям об **аренде жилья**, переводы денежных средств обратившемуся в переписке в социальной сети или мессенджере «другу» с просьбой **одолжить денежные средства** или переводы в качестве **пожертвований** на «фейковые» объявления, **завладение интимными** материалами с последующем вымогательством денежных средств за неразглашение информации.

Рекомендации гражданам, чтобы не стать жертвой преступников и не потерять свои денежные средства:

Ни под каким предлогом **никому не сообщать** полные реквизиты банковской платежной карты, в частности, три цифры с оборотной стороны карты, коды из СМС, паспортные данные, логин и пароль для входа в систему «Интернет-банкинг». Не хранить их в открытом доступе, не пересылать в социальных сетях и мессенджерах. Данные реквизиты являются ключами к банковскому счету. Три цифры с оборотной стороны банковской платежной карты нужны лишь для подтверждения расходной операции.

Не следует переходить по подозрительным ссылкам в электронном письме, сообщении и т.д. Если уже открыта потенциально опасная ссылка, ни в коем случае не вводить конфиденциальную информацию.

При поступлении звонков от имени работников банковских учреждений следует знать:

Работники банка не звонят в мессенджерах и не просят устанавливать программы для доступа к телефону.

Сотрудники банка могут лишь уточнить, действительно ли держателем карт-счета совершалась определенная расходная операция по счету, и не требуют оформления кредитов, участия в поимке злоумышленников, предоставления паспортных и иных личных данных, реквизитов банковской платежной карты, кодов из СМС, осуществления переводов денежных средств на иные счета.

В случае подозрения на несанкционированные действия со счетом сотрудники банка самостоятельно заблокируют операцию.

При желании заработать на бирже, необходимо помнить:

Ряд «фейковых» сайтов в сети Интернет позиционируют себя биржами, коими не являются; нет полных гарантий в заработке и исключении потери денежных средств. Такие сайты могут быть созданы за считанное время из любой точки мира, найти их владельцев крайне затруднительно.

Абсолютное большинство таких сайтов имеют в Интернете крайне отрицательные отзывы, которые легко найти путем поисковых запросов в сети.

«Фейковые» биржи, как правило, созданы (зарегистрированы) не более года назад, а то и месяцы до начала функционирования, что легко проверить в сети Интернет.

Для торговли на бирже необходимы большие познания и опыт работы с официальными известными интернет-ресурсами.

При посещении аккаунтов интернет-магазинов, в частности, в сети **«Инстаграм», следует знать:**

Ранее неизвестные интернет-магазины, работающие только по предоплате и предлагающие товары стоимостью ниже рыночной, исключительно с положительными отзывами, – высокий риск потери денежных средств.

Фотографии имеющихся товаров на множестве разных фонов (в разных помещениях) – один из признаков «фейкового» магазина, данные фотографий скачаны в сети Интернет.

Подобные «фейковые» аккаунты легко создаются в считанные часы, отзывы и подписки искусственно накручиваются, их владельцы могут находиться в любой точке мира, что усложняет их установление.

Более безопасно осуществлять покупки в интернет-магазинах на известных и проверенных интернет-площадках (известных брендов).

При онлайн-покупках рекомендуется использовать виртуальную платежную карту, а не основную банковскую платежную карту (перед совершением покупки необходимую денежную сумму переводить с основной банковской платежной карты на виртуальную платежную карту).

При осуществлении доступа к системе «Интернет-банкинг» помните: нельзя искать сайт интернет-банка (системы «Интернет-банкинг») путем поискового запроса в браузере. Адрес сайта банка (страницы системы «Интернет-банкинг») нужно знать и вводить «вручную» в адресной строке, лучше добавить в список закладок браузера или использовать мобильное приложение.

Общаясь в социальных сетях, на сайтах знакомств, путем переписки в мессенджерах, следует помнить, что за «аватаркой» друга или знакомого может скрываться иное лицо, пытающееся завладеть денежными средствами или личными данными.

При необходимости финансовых перечислений следует удостовериться в личности собеседника с использованием других каналов связи (личная встреча, телефонный звонок, звонок посредством интернет-мессенджера).

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но всем гражданам в любой ситуации следует не терять бдительность, обдуманно относиться ко всему происходящему в сети Интернет. Ведь зачастую излишняя доверчивость и неосмотрительность самих граждан способствует совершению вышеуказанных преступлений.