МАТЕРИАЛ
для членов информационно-пропагандистских групп
(май 2024 г.)

Профилактика преступлений, связанных с неправомерным завладением реквизитами пластиковых банковских карт и хищением средств с карт-счетов граждан, а также в сфере высоких технологий

Материал подготовлен Управлением Следственного комитета Республики Беларусь по Гродненской области

Состояние преступности в сфере противодействия киберпреступности.

На территории Гродненской области зарегистрировано преступлений в сфере противодействия киберпреступности:

2018 г. – 300 преступлений
2019 г. – 930
2020 г. – 2700
2021 г. – 1814
2022 г. – 1407
2023 г. – **1529** (из которых **1420** – хищения денежных средств: 1096 – совершенных путем модификации компьютерной информации, 301 – путем мошенничества и 23 – путем вымогательства).

За 1 квартал 2024 года в сравнении с аналогичным периодом прошлого года произошел существенный рост по отдельным видам преступлений. В частности, со 178 до 277 (или на 55,6%) возросло количество мошенничеств; с 5 до 18 увеличилось число вымогательств, с 5 до 16 преступлений по незаконному обороту средств платежа и инструментов (ст. 222 УК), с 2 до 7 преступлений, предусмотренных ст. 340 УК (заведомо ложное сообщение об опасности).

Как видно из статистики, как в 2022-2023 годах, так и в текущем году, на территории Гродненской области фиксируется большое количество хищений денежных средств граждан, совершенных с использованием информационно-коммуникационных технологий, большую часть которых составляют именно хищения (путем модификации компьютерной информации (ст. 212 УК) и мошенничества (ст. 209 УК).

Хищение денежных средств **путем модификации компьютерной информации** злоумышленниками совершается в результате получения доступа к банковскому счету с использованием переданных владельцем счета реквизитов банковской карты, путем доступа к системе интернет-банкинг или к мобильному устройству потерпевшего через удаленные

программы, а также с использованием похищенной или потерянной банковской платежной карты.

Хищение **путем мошенничества** совершается в результате использования преступником так называемых методов социальной инженерии, когда потерпевшего вынуждают под видом звонка от сотрудника банковского учреждения или правоохранительных органов 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 Интернете в большей части 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 в иных аккаунтах.

Наиболее распространенные схемы и способы, которые используют преступники для хищения денежных средств в сети Интернет.

1. **«Вишинг» -** метод социальной инженерии, заключающийся в осуществлении телефонных звонков гражданам (как правило в интернет-мессенджерах) от имени работников банковских учреждений, правоохранительных органов, когда злоумышленники сообщают гражданину, что какое-то лицо без ведома оформило на него кредит либо совершается попытка хищения денежных средств со счета.

Для отмены кредита, либо предотвращения хищения денежных средств со счета и поимки виновного необходимо срочно оформить новые кредиты на максимальную сумму платежеспособности, либо перевести деньги на «безопасный счет» или «защищенную ячейку». Для убедительности к данным звонкам «жертве» также начинают поступать звонки от имени работников Нацбанка, сотрудников ОВД и следователей, подтверждающих наличие проблемы, с целью убеждения осуществления переводов денежных средств и участии в мероприятии по выявлению преступника. Потерпевшему могут также высылаться в мессенджере фотографии служебных удостоверений, злоумышленники инструктируют как себя вести при оформлении кредита в банке. В данном случае действуют участники организованных групп. В ряде случаев таким образом мошенники убеждают граждан оформлять кредиты на крупные суммы, осуществить их перевод, в том числе имеющихся на счету денежных средств, на подконтрольные злоумышленникам счета, и похищают их. 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 (вы последнее время, в том числе представляясь работниками компаний сотовой связи), в ходе чего сами получают доступ к телефону и системам интернет-банкинг, и самостоятельно осуществляют хищение денежных средств со счета, в том числе дистанционно оформляя на граждан кредиты.

Примеры преступлений с «вишингом»:

Гродненский МОСК	14.08.2023	ст.212 ч.4	Неустановленное лицо в период времени с 12.15 часов по 16.00 часов 31.07.2023, находясь в неустановленном месте, посредством звонка в мессенджере «Viber» **от имени работника банка склонило** жительницу г.Гродно М. к установке программы **удаленного доступа к мобильному устройству «RustDesk»**, после чего, путем модификации компьютерной информации, похитило с банковского счета денежные средства на общую сумму 44 404 рублей
Ошмянский РОСК	04.08.2023	ст.209 ч.3	Неустановленное лицо, в период в июне 2023 года, совершило звонок жительнице г. Ошмяны Е., представилось сотрудником службы безопасности Национального Банка и **под предлогом аннулирования оформленных злоумышленником на нее кредитов** убедило оформить кредиты в 3-х банках на сумму более 25 000 и перевести на представленные ей номера счетов
Гродненский МОСК	25.08.2023	ст.209 ч.3	Неустановленное лицо 07.08.2023 около 16:00 часов, в ходе звонка в мессенджере «Telegram» и телефонных разговоров от имени работника банка, **под предлогом избежать хищения денежных средств с банковских счетов**, путем обмана убедило жителя г. Гродно А. **перевести** денежные средства в сумме 12 999 рублей на надежный счет посредством банкомата, которыми завладело
Щучинский РОСК	30.04.2024	ст.209 ч.4	Неустановленное лицо в период с 24 по 29.04.2024 в ходе телефонных разговоров в мессенджере «Telegram» путем обмана и злоупотребления доверием **под предлогом изобличения мошенников**, завладело принадлежащими гражданке М., денежными средствами в сумме 74 565 рублей.
Мостовский РОСК	24.04.2024	ст.209 ч.1	Неустановленное лицо 23.04.2024, путем неоднократных звонков на абонентский номер потерпевшего**, путем обмана, под предлогом декларирования принадлежащих потерпевшему денежных средств**, убедило гражданина Б. перевести денежные средства посредством инфокиоска, а также мобильного приложения интернет-банкинга, в результате чего завладело денежными средствами в сумме 7800 рублей.

2. **Фейковые интернет-магазины** по продаже товаров в социальных сетях. Наиболее часто в последнее время встречаются именно **в социальной сети «Инстаграм».** Злоумышленники создают фейковые аккаунты по продаже одежды, обуви, предметов мебели и интерьера, наполняют их тематических контентом из свободных источников сети Интернет с фотографиями якобы реализуемого товара, рядом положительных отзывов, и с доступными ценами ниже рыночных, вступают в переписку в различных мессенджерах, предлагая внести за товар предоплату либо аванс путем перечисления на банковский счет. Для получения денежных средств при этом, как правило, используются банковские карт-счета подставных лиц.

Аналогичные объявления о продаже товара могут размещаться на веб-сайтах, в сообществах или путем рассылки в мессенджерах, а также на сайтах аренды надвижимости под предлогом внесения предоплаты за аренду квартиры.

Нередко злоумышленники используют и известные площадки с объявлениями о продаже товара или предоставления услуг, в частности торговую площадку «Куфар», сайт продажи автомобилей «av.by», выступая там «продавцами» и убеждая граждан перечислять предоплату за товар/услугу. Обман происходит по следующим схемам: 1) **внесения предоплаты за продаваемый товар**, 2) **завладение реквизитами банковской карты под предлогом оплаты товара** посредством предоставления фишинговой ссылки и хищение средств с использованием полученных реквизитов БПК.

Примеры преступлений с «фейковыми магазинами» и «фейковыми продавцами»:

Гродненский МОСК	05.05.2024	ст.209 ч.1	Неустановленное лицо, 01.05.2024 находясь в неустановленном месте, **используя аккаунт «drilloviy_market» в социальной сети «Instagram»**, под предлогом продажи одежды, завладело денежными средствами жителя г. Гродно Ш. на сумму 260 рублей.
Новогрудский РОСК	04.05.2024	ст.209 ч.1	Неустановленное лицо, находясь в неустановленном месте, 04.05.2024 путем обмана, посредством переписки **в социальной сети «Instagram», под предлогом продажи цветов**, склонило жителя г. Новогрудка к переводу денежных средств в размере 140 рублей на подконтрольный злоумышленнику банковский счёт, которыми завладело
Гродненский МОСК	02.05.2024	ст.209 ч.1	Неустановленное лицо, в период с 22 по 24.04.2024, находясь в неустановленном месте, **используя аккаунт в соцсети «Instagram» «apple_market_by»**, под предлогом продажи мобильного телефона, завладело денежными средствами гражданина Б. сумму 450 рублей.

Лидский РОСК	30.04.2024	ст.209 ч.1	Неустановленное лицо, находясь в неустановленном месте, **в ходе переписки в социальной сети «Instagram»**, 24.04.2024 часов, путем обмана, под предлогом продажи гражданину Ж. кухонного комбайна, склонило последнего к переводу денежных средств в размере 200 рублей на подконтрольный злоумышленнику банковский счет
Гродненский МОСК	06.05.2024	ст.209 ч.4	Неустановленное лицо, в период с 18 по 23.04.2024, находясь в неустановленном месте, посредством переписки в мессенджере «WhatsApp» с директором одного из ООО, **под предлогом продажи промышленных станков на интернет-платформе «Куфар»**, путем обмана завладело денежными средствами, принадлежащими на сумму **168 771** рублей.
Зельвенский РОСК	02.04.2024	ст.212 ч.1	Неустановленное лицо, 01.04.2024, находясь в неустановленном месте, под предлогом заполнения информации об адресе, с целью дальнейшей отправки заказанного товара, принудило П., **перейти по отправленной ссылке и ввести данные о** принадлежащей ему БПК, после чего завладев реквизитами указанной банковской карты похитило 682 рубля.

3.**Веб-сайты**, имитирующие различные **трейдинговые платформы** для заработка денежных средств на торгах. Спам реклама о данных сайтах распространяется повсюду в сети Интернет. Доверчивые граждане переходят по ссылке, не проверив историю и отзывы ресурса, 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 перечислять 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 «имеющие на счету» и вложенные деньги, начинается «история» о необходимости внесения налога, страховки, компенсации и т.д., вынуждая потерпевшего вносить очередные суммы денег средств

Гродненский МОСК	06.05.2024	ст.209 ч.3	Неустановленное лицо в период с 10.02.2024 по 29.03.2024, находясь в неустановленном месте, посредством переписки в мессенджере «Телеграмм» с гражданином П., **под предлогом заработка на платформе «stockmarkt.net»,** путем обмана, завладело его денежными средствами в сумме более 20 000 рублей.

Гродненский МОСК	30.04.2024	ст.209 ч.1	Неустановленное лицо 13.03.2024, находясь в неустановленном месте, **под предлогом заработка на фейковом сайте ОАО «Беларуськалий»**, путем обмана, в ходе переписки и звонков в приложении «Skype» с гражданином В., завладело принадлежащими ему денежными средствами на сумму 500 рублей.

4. Фишинговые сайты банков, театров и кинотеатров.

В сети Интернет существует ряд сайтов, имитирующих главные веб-страницы банковских учреждений и страницы интернет-банкинга. Желая зайти в приложение, граждане ищут страницу интернет-банкинга своего банка путем поискового запроса в браузере, что делать нельзя. Нередко в первых результатах поиска за названием аббревиатуры финансового учреждения кроется ссылка на фишинговый сайт, внешне ничем не отличающийся от оригинала (по наполнению, цвету, разделам и т.д.), но имеющий иной адрес в адресной строчке браузера. Отличаться он может даже одним символом от правильного адреса. Вводя на таком сайте логин и пароль владелец счета предоставляет доступ к интернет-банкингу, а это полный доступ к счету. Через считанные минуты денежные средства переводятся злоумышленником на иной счет.

Аналогично в интернете распространяются ссылки на поддельные сайты **театров и кинотеатров**. Для покупки билетов необходимо ввести реквизиты БПК и код подтверждения из СМС. Далее происходит хищение денежных средств с карт-счета с использованием реквизитов карты. Нередко покупке билетов предшествует переписка со случайным собеседником в социальной сети, мессенджере, на сайте знакомств.

ГМОСК	07.01.2024	ст.212 ч.1	Неустановленное лицо 07.01.2024, находясь в неустановленном месте, **завладев посредством фишингового сайта «mtbbank-by.com»** реквизитами доступа к интернет-банкингу жителя г. Гродно Л., похитило с карт-счета последнего денежные средства в сумме 386 рублей.
ГМОСК	31.07.2023	ст.212 ч.1	Неустановленное, находясь в неустановленном месте, 19.07.2023 около 18.22 часов, в ходе переписки в мессенджере «Telegram» с жителем г. Гродно А., 1998 г.р. договорилось **о походе в театр**, после чего для покупки билетов **предоставило жителю г. Гродно А. ссылку фишингового сайта**, посредством которой завладело реквизитами банковской карты и похитило с карт-счета 609 рублей.
ГМОСК	20.03.2024	ст.212 ч.1	Неустановленное лицо, 19.03.2024, находясь в неустановленном месте, с использованием сети «Интернет», **под предлогом совместной покупки билетов в театр** на сайте «theater.by-63.shop», завладело реквизитами банковских платежных карт гражданина М., и с их использованием похитило с карт-счетов денежные средства в сумме 4 799 рублей

5. Иные способы (менее распространенные)

– завладение деньгами в виде предоплаты по объявлениям об **аренде жилья**,

– завладение деньгами в ходе переводов денежных средств в социальной сети или в мессенджере обратившемуся в переписке «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:

- ни под каким предлогом **никому не сообщать полные** реквизиты банковской платежной карты, в частности 3 цифры с оборотной стороны карты, коды из SMS, паспортные данные, логин и пароль от интернет-банка. 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 карты нужны лишь для подтверждения расходной операции;

- не переходить по подозрительным ссылкам

При поступлении звонков от имени работников банковских учреждений (правоохранительных органов) 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. Сотрудники банков и правоохранительных органов не требуют оформления кредитов, в ходе телефонных разговоров участии в поимке злоумышленников, предоставления паспортных и иных личных данных, реквизитов БПК, кодов из СМС, осуществления переводов денежных средств на иные счета;

- в случае малейшего подозрения на несанкционированные действия со счетом сотрудники банка самостоятельно заблокируют операцию и/или банковский счет.

При желании заработать в сети Интернет, необходимо помнить:

- ряд фейковых сайтов в сети Интернет позиционируют себя биржами/трейдинговыми платформами, коими не являются, нет никаких 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 заработка в сети Интернет нужны 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 – максимально высокий риск потери средств;

- фотографии имеющихся товаров на множестве разных фонов (в разных помещениях) – один из признаков фейкового магазина, данные фото 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 не использовать основную банковскую карту, а оформить виртуальную и перед совершением покупки переводить на нее необходимую сумму;

При осуществлении доступа к системе интернет-банкинг помните:

- нельзя искать сайт интернет-банка путем поискового запроса в браузере. Адрес сайта банка (страницы интернет-банкинга) нужно знать и вводить «вручную» в адресной строке. А лучше добавить в список закладок браузера, или использовать мобильное приложение.

Общаясь в социальных сетях, 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).