МАТЕРИАЛЫ
для членов информационно-пропагандистских групп
(июль 2026 г.)

О СОСТОЯНИИ ПРЕСТУПНОСТИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В ГРОДНЕНСКОЙ ОБЛАСТИ

Материал подготовлен
Управлением Следственного комитета Республики Беларусь
по Гродненской области

Управлением по противодействию киберпреступности
криминальной милиции УВД Гродненского облисполкома

Несмотря на объективно наблюдаемую картину повышения качества жизни населения, доступности товаров и услуг, вызванную широким распространением информационных технологий, возникают новые риски, вызовы и угрозы. Одним из таких негативных проявлений массовой цифровизации является появление и широкое распространение киберпреступности.

В регионе при общем снижении количества регистрируемых преступлений наблюдается очевидная тенденция увеличения удельного веса киберпреступлений в общей структуре преступности.

Согласно статистике, следственными подразделениями Гродненской области в 2025 году возбуждено более 1970 уголовных дел о киберпреступлениях (рост более чем на 13% в сравнении с 2024 годом). Из них более 97% – преступления о хищении денежных средств, более 200 уголовных дел о тяжких преступлениях (суммы ущерба превысили 250 базовых величин). Удельный вес киберпреступлений в общей массе всех преступлений превысил 31% (почти каждое третье преступление). У граждан области в 2025 году интернет-мошенниками похищено более 8 миллионов рублей.

В первом полугодии 2026 года Следственными подразделениями Гродненской области возбуждено 864 головных дела о совершении киберпреступлений (за аналогичный период 2025 года – 832, рост составил 3,8 %).

Доля киберпреступлений от всех зарегистрированных за январь-июнь 2026 года в УСК по Гродненской области преступлений возросла и составила 31,5% (28,7% - за аналогичный период прошлого года).

В структуре киберпреступности в 2026 году по-прежнему в абсолютном большинстве (97,5%) преобладают преступления против собственности: хищения путем модификации компьютерной информации,

мошенничества и вымогательства, совершенные с использованием информационно-коммуникационных технологий.

При этом за первые шесть месяцев 2026 года по сравнению с аналогичным периодом 2025 года произошло увеличение количества интернет-вымогательств на 34 (с 31 до 65, или +109,7 %), кибермошенничеств на 88 (с 468 до 556, или +18,8 %), уголовных дел, возбужденных по факту блокирования, уничтожения или модификации компьютерной информации на 8 (с 2 до 10, или + 400 %), преступлений о заведомо ложном сообщении об опасности по направлению деятельности противодействие киберпреступности на 1 (с 4 до 5, или +25%), по фактам неправомерного завладения компьютерной информацией на 1 (в 1 полугодии 2025 года уголовные дела о преступлениях, предусмотренных ст.352 УК, не возбуждались).

Между тем, наблюдается снижение хищений путем модификации компьютерной информации на 60 (с 281 до 221, или – 21,3 %), фактов незаконного оборота средств платежа на 6 (с 12 до 6, или – 50 %), несанкционированного доступа к компьютерной информации и оборота вредоносных компьютерных программ на 1 (в 1 полугодии 2026 года уголовные дела о преступлениях, предусмотренных ст.ст.349 и 354 УК, не возбуждались).

Согласно статистике, в 1 полугодии 2026 года установлены подозреваемые лица в совершении 329 киберпреступлений (в 1 полугодии 2025 года – 222). Удельный вес раскрываемости вырос на 9,1%, с 25,4% до 34,5%. За период с января по июнь 2026 года предварительное расследование окончено по 103 уголовным делам (против 115 за аналогичный период 2025 года), принимались решения о приостановлении предварительного следствия по ч.1 ст.246 УПК по 822 уголовным делам (759).

Психологический портрет жертвы телефонных мошенников

Это собирательный образ, объединяющий людей определенных психологических характеристик и жизненных обстоятельств, делающих их более уязвимыми. В основе лежит, доверчивость, подкрепленная наивностью.

Жертвы склонны верить людям на слово, не подвергая сомнению полученную информацию, особенно если она исходит от представителя авторитетной организации (банк, правоохранительные органы). Они легче поддаются эмоциональному давлению.

Эмоциональное состояние, в котором пребывает человек играет свою роль. Стресс, тревога, страх потерять деньги или навредить близким – все эти чувства дезориентируют и ослабляют способность критически

оценивать ситуацию. Мошенники умело используют эти состояния, создавая ощущение срочности и паники, вынуждая жертву действовать импульсивно, при этом её внимание рассеяно, а эмоциональная устойчивость снижена.

Немаловажным фактором является одиночество и потребность во внимании. Пожилые люди, живущие одни, особенно уязвимы проявлениям внимания, даже если они исходят от незнакомцев.

Импульсивность и склонность к азарту могут способствовать попаданию в ловушку мошенников. Обещания легкой наживы, выигрыша в лотерею могут затмить разум и заставить человека действовать необдуманно, не проверяя достоверность информации.

Важно отметить, что жертвами становятся не только люди с низким уровнем образования или интеллекта. Напротив, успешные и образованные личности также попадаются в сети мошенников. Поскольку их уверенность в собственных знаниях приводит к переоценке своей способности распознать обман.

Любой человек, независимо от возраста, образования или социального статуса, может стать жертвой телефонного мошенничества. Психологический портрет лишь указывает на факторы, повышающие уязвимость к подобным манипуляциям. Поэтому важно постоянно повышать свою осведомленность и быть в курсе последних тенденций в сфере телефонного мошенничества.

Мошенники постоянно совершенствуют свои методы обмана, используя последние технологические достижения и психологические приемы. Чтобы обмануть своих жертв в ход идут убедительные легенды, запугивание, срочность и обещание невероятной выгоды.

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

1. **ТЕЛЕФОННЫЕ ЗВОНКИ В МЕССЕНДЖЕРАХ и реже по обычной связи от имени работников банков, сотрудников правоохранительных органов, работников операторов сотовой связи и иных организаций** (мошенниками в ходе звонков сообщается)**:**

по счету гражданина зафиксированы **преступные финансовые операции**, поэтому будет проведен обыск и возбуждено уголовное дело, чтобы этого избежать, необходимо «задекларировать» все имеющиеся средства путем перевода на специальный счет или передать курьеру;

банковский **счет «в руках» злоумышленников** и необходимо перевести деньги на «безопасный счет»;

мошенники **оформили кредиты** на гражданина и для противодействия (аннулирования) владельцу счета нужно самому оформить новые кредиты и перевести деньги на другие счета;

потерпевший участвует в некой **спецоперации** по поимке преступников либо недобросовестных работников банка, поэтому необходимо выполнять нужные действия;

звонок от имени родственников, **якобы попавших в ДТП** и для смягчения ответственности надо перевести деньги либо передать их курьеру.

Все чаще схема со звонками приобретает гибридный характер.

Поступает первый звонок от имени работников «Водоканала», «Энергосбыта», «Белпочты», «домофонного сервиса», «Инспекции по электросвязи», операторов сотовой связи.

Мошенниками сообщается:

будет производиться замена счетчиков или чипов для домофона;

поступило заказное письмо;

необходимо продлить договор на услугу доступа в Интернет или сотовой связи и др.

Настаивают – НУЖНО СООБЩИТЬ КОД из поступившего SMS или паспортные данные.

Затем поступают второй и последующие звонки от имени работников Нацбанка, сотрудников правоохранительных органов (КГБ, ДФР, УСК, КГК и др.)

Мошенниками сообщается:

что накануне это звонили злоумышленники, которым Вы сообщили личные или финансовые данные, с использованием которых на Вас оформлены кредиты либо банковский счет используется для переводов денежных средств на террористическую деятельность, либо банковский счет скомпрометирован и будут похищены деньги.

Поступают угрозы:

«Будет возбуждено уголовное дело, будет проведен обыск, имеющиеся наличные деньги будут изъяты».

Мошенники требуют:

все наличные сбережения «ЗАДЕКЛАРИРОВАТЬ» путем перевода по предоставленным реквизитам счета либо передать курьеру;

все наличные сбережения «ПРЕДОСТАВИТЬ ДЛЯ ПРОВЕРКИ» путем передачи курьеру;

участвовать в спецоперации, частью которой является оформление кредитов в банках и перевод денежных средств по предоставленным реквизитам либо их передача курьеру;

предоставить доступ к карт-счету (сообщить все реквизиты банковской карты и коды из SMS, либо логин и пароль в интернет-банк) для перевода денег на «безопасный» счет;

по предоставленной ссылке установить на телефон программу удаленного доступа для просмотра всей информации на телефоне.

Примеры по уголовным делам:

В конце января 2026 года жительнице Гродно позвонили на домашний телефон от имени работника Водоканала и под предлогом замены счетчиков попросили паспортные данные. Затем в Вайбере и Телеграм от имени сотрудников Департамента Финансовых расследований и КГБ сообщили, что на женщину мошенниками оформлены кредиты, будет возбуждено уголовное дело, проведен обыск и для погашения кредитов ей нужно оформить другие кредиты, а полученные деньги перевести на предоставленные реквизиты счетов. Под влиянием лжесотрудников потерпевшая оформила кредиты в 3-х банках и перевела аферистам более 41 тысячи рублей.

В середине февраля 2026 года женщине из Мостовского района позвонили от имени работника Электросетей и под видом замены счетчика попросили код из SMS. Затем от имени правоохранителей сообщили, что на имя женщины мошенниками открыт банковский счет, посредством которого осуществляются переводы денежных средств для спонсирования терроризма. Грозили обыском и изъятием всех денег. Указали на необходимость декларирования имеющихся сбережений. Находясь под влиянием аферистов, женщина открыла банковский счет, зачислила на него все деньги, после чего предоставила лжесотрудникам доступ к интернет-банку, сообщив пароль и коды из SMS. И как итог потеряла без малого 18 тысяч рублей, которые злоумышленники перевели на подконтрольные им счета.

В конце января 2026 года жительнице Гродно позвонили на мобильный телефон от имени домофонного сервиса и под предлогом замены чипов домофона попросили код из SMS. Затем в Вайбере от имени правоохранителей сообщили, что по счету зафиксированы операции по финансированию терроризма, запугали обыском и изъятием всех денег. В итоге убедили женщину в необходимости декларирования денежных средств. Под влиянием лжесотрудников потерпевшая передала прибывшему курьеру 10 тысяч Евро сбережений.

Что НУЖНО ЗНАТЬ про звонки от мошенников:

банковский счет **априори** в безопасности (если никакие личные данные гражданином не предоставлялись и не вводились на неизвестных ресурсах, особенно по предложению звонящих лиц, в том числе не устанавливались какие-либо программы);

работники банка, сотрудники правоохранительных органов **не будут просить личные данные**, **коды** из СМС, просить совершать какие-либо действия со счетом, **не звонят в мессенджерах**;

работники банка **САМОСТОЯТЕЛЬНО** при подозрениях **заблокируют** счет/аннулируют кредит и т.п.

При таких просьбах в ходе звонка – необходимо взять паузу (обдумать происходящее: со счетом же ничего не совершал, карту не терял), **не передавать никаких данных и не совершать никаких действий**;

ПРИ ЛЮБЫХ ПРОСЬБАХ ПРЕДОСТАВИТЬ ЛИЧНЫЕ ЛИБО ФИНАНСОВЫЕ ДАННЫЕ – **завершить разговор** и перезвонить в свой банк либо в ОВД.

Кроме этого, потерпевшему звонящим также могут высылаться в мессенджере фотографии служебных удостоверений, злоумышленники инструктируют как себя вести при оформлении кредита в банке. Преступники действуют настолько убедительно, что зачастую потерпевшие осуществляют переводы в течение нескольких дней, имея реальное время подумать над происходящим. Очень часто происходят инсценировки с несколькими лицами (звонящими).

2. ФЕЙКОВЫЕ ИНТЕРНЕТ-БИРЖИ и участие в ФЕЙКОВЫХ ИНВЕСТ-ПРОЕКТАХ («БелТрансГАЗ», «Газпром», «Государственная программа» и т.п.) Схемы отмечаются **большим ущербом**.

Спам реклама о фейковых проектах (сайтах) распространяется повсюду в сети Интернет, особенно в социальных сетях. После перехода по ссылке так называемые «представители» биржи вступают в переписку в мессенджере. Граждан убеждают в высоких доходах, чему способствуют содержащиеся на ресурсе красивые фейковые отзывы об эффективности заработка. Для убедительности мошенники создают «жертвам» личные аккаунты на сайте биржи (платформы), где якобы отображаются суммы внесенных денежных средств. Когда человек решает вывести «имеющиеся на счете» вложенные деньги, начинается «история» о необходимости внесения налога, страховки, компенсации и т.д., вынуждая потерпевшего вносить очередные суммы денег. При этом «жертве» вначале могут дать заработать около 100 рублей для создания видимости успешности проекта.

Примеры по уголовным делам:

В период с 21.10.2025 по 19.01.2026 неустановленные лица путем использования сайта фейковой биржи «silent-point.com», аккаунтов в мессенджере «Telegram» @akim777invest, @Reshetov_AI, @Manager_Fin1, @MaksimBelov1989 и звонков с абонентских номеров +79236708186, +48226022655, +441517008736, под предлогом инвестиций на бирже, путём обмана совершило хищение денежных средств жительницы Волковыска на сумму более 39000 рублей, которые последняя перевела на предоставленные в ходе переписки подконтрольные неустановленному лицу банковские счета.

В период с 20.11.2025 по 13.01.2026 неустановленные лица посредством переписки и звонков в мессенджере «Телеграм» с аккаунта @Dmytrkuznts с абонентским номером +79030841519, @maria_23254, @Andreevich_, @yuriiklimov18, под предлогом инвестирования денежных средств в сфере криптовалюты, путем обмана завладело денежными средствами жительницы Гродно, 2000 г.р. в общей сумме 28724 рублей, которые последняя самостоятельно перевела на неустановленный криптокошелек.

Правовое регулирование криптовалютных операций в Республике Беларусь

Операции по покупке и продаже криптовалюты за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) разрешены только в криптобиржах (оператор обмена криптовалют), являющихся резидентами Парка высоких технологий. Совершение операций по купле (продаже) криптовалюты на иных криптобиржах и у физических лиц является незаконным и запрещается. Порядок осуществления сделок с криптовалютой определен Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367

«Об обращении цифровых знаков (токенов)», за нарушение которого предусмотрена административная ответственность частью 3 статьи 13.3 Кодекса Республики Беларусь об административных правонарушениях, предусматривающей штраф с конфискацией всей суммы дохода.

В последнее время мошенники обещают «новый токен» или быстрый заработок. Для участия предлагают пройти «верификацию» – пополнить депозит настоящей криптовалютой. Результат: деньги навсегда уходят аферистам.

Кто такие дропы?

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных

лиц, так называемых «дропов». Часто промежуточных счетов бывает более десятка.

В нашей стране открыть банковский счет может гражданин с 14 лет, с разрешения законных представителей, то есть даже несовершеннолетние могут открыть банковские счета. Этим и пользуются преступники. Находясь за границей, злоумышленники подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет интернет-банкинга, а также предоставить разовый СМС-код.

Поиск дропов

Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда, или людей для разгрузки товаров, или людей на вакансию «тайный покупатель», или заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Надо знать, что статьей 222 Уголовного кодекса предусмотрена уголовная ответственность за распространение из корыстных побуждений, находящихся в незаконном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или виртуальным кошелькам. За предоставление своих личных данных для использования в мошеннических схемах предусмотрена административная ответственность по статье 12.35 Кодекса Республики Беларусь об административных правонарушениях.

Имеются факты, когда в преступную деятельность вовлекались несовершеннолетние.

<u>Что НУЖНО ЗНАТЬ про рекламу быстро заработать:</u>

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 указанной деятельности нужные большие познания и опыт работы с официальными известными интернет-ресурсами, абсолютное большинство таких ресурсов и реклама на них в социальных сетях – ФЕЙК!

Кроме этого, в сети Интернет распространяется много фейковых ресурсов, рекламирующих услуги от имени юристов, юридических и других организаций, агентств и фондов в оказании помощи по возврату переведенных средств мошенникам и лжеброкерам, когда злоумышленники вновь попросят перевести денежные средства за сои услуги, предоставить реквизиты счета и так далее. Известны случаи, когда таким образом граждане дважды теряли своим деньги.

3. Третья схема – **фейковые интернет-магазины** по **продаже товаров** (одежда, обувь, мебель, качели, цветы, морепродукты и т.д.) и **предоставлении услуг**, в частности в социальной сети **INSTAGRAM и группах Telegram** (наиболее частые случаи)

Мошенники создают страницы (аккаунтов) с изображением красивых товаров по привлекательным ценам, «накручивают» большое число подписчиков для создания видимости реального магазина. Обязательное условие – ПОЛНАЯ ПРЕДОПЛАТА путем перевода на подконтрольные злоумышленникам счета.

<u>Что НУЖНО ЗНАТЬ при покупках в сети Интернет:</u>

ранее неизвестные интернет-магазины, работающие только по предоплате и предлагающие товары стоимостью ниже рыночной – 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 (известные маркетплейсы);

при онлайн-покупках рекомендуется ИСКЛЮЧИТЬ ПРЕДОПЛАТУ и НЕ ИСПОЛЬЗОВАТЬ основную банковскую карту, а оформить

виртуальную и перед совершением покупки переводить на нее необходимую сумму.

4. Четвертая схема – ФИШИНГ

фишинговые сайты банков (интернет-банкинг, акции по выплате бонусов и вознаграждений за прохождение опросов и др.);

фишинговые СЕРВИСЫ служб доставки или оплаты (от имени компаний «CDEK», «Европочта», «Белпочта» и др.);

фишинговые объявления о сдаче жилья в аренду с получением предоплаты путем ввода данных банковских карт.

ЦЕЛЬ злоумышленников – получить полные реквизиты банковской карты и коды из SMS, либо логин и пароль в интернет-банк. Заполучив эти данные, злоумышленник переводит все деньги на свои счета.

В сети Интернет появляется ряд фейковых сайтов, имитирующих официальные сайты банковских учреждений или стартовые страницы интернет-банкинга. Желая зайти в свой личный кабинет, граждане ищут страницу интернет-банкинга своего банка путем поискового запроса в браузере. Нередко в первых результатах поиска за названием аббревиатуры финансового учреждения кроется ссылка на фишинговый сайт, внешне ничем не отличающийся от оригинала, но имеющий иной адрес в адресной строчке. 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 злоумышленниками на иной счет.

Нередко пользователи сети могут наткнуться на различные фейковые рекламные акции белорусских банков или организаций, размещенные на неофициальных веб-сайтах. Как правило, для получения вознаграждения, там необходимо ввести реквизиты банковской карты, трехзначный номер и поступивший код из SMS, но вместо выигрыша происходит списание всех денежных средств со счета.

Стоит помнить, что фишинговые ссылки могут быть предоставлены и на сайтах покупки/продажи товаров с предоставлением форм для ввода реквизитов банковской карты и кода из SMS, якобы для получения денежных средств (например, на торговой платформе «Куфар»). Чтобы обмануть покупателей и продавцов, мошенники также создают и поддельные сайты, предлагая товары по слишком низким ценам, в том числе утверждая, что товар конфискованный, используя фальшивые отзывы для повышения доверия.

Граждане, заинтересовавшиеся объявлениями о продаже товаров по низким ценам, теряют бдительность, вступают в переписку со злоумышленниками, которые представляются продавцами Интернет-магазинов. В ходе переписки, желая получить товар по выгодной цене в

кратчайшие сроки, доверчивые граждане, никак не убеждаясь в добропорядочности продавца, переводят на указанные им счета денежные средства. После этого общение с покупателем прекращается, товар никто не высылает.

Мошенники обманывают граждан на торговых площадках и под видом покупателей. Например, девушка выставила товар на продажу на «Куфар». Через некоторое время ей пишет «покупатель»: «Оплачу сразу, оформлю доставку, вот ссылка». Ссылка выглядит очень похоже на сервис доставки CDEK (может быть Белпочта, Европочта) только вместо «by» - «.shop». Девушка вводит данные карты по предложенной форме, включая CVV-код и код из смс-сообщения, после этого мошенники списывают все денежные средства с карты.

Нередки случаи, когда после получения злоумышленником денежного перевода в виде предоплаты (например, в INSTAGRAM), с целью дальнейшего хищения он под видом возврата средств или оплаты доставки (например, товар закончился, либо надо оплатить доставку) убеждает потерпевшего перейти по предоставленной ссылке и в форму на интернет-странице ввести реквизиты банковской карты якобы для получения средств обратно или оплаты доставки.

Завладев реквизитами карты и кодами из SMS, мошенник, с их использованием похищает денежные средства с карт-счета путем перевода на свои счета.

Что нужно знать про ФИШИНГ:

При осуществлении доступа к системе интернет-банкинг НЕЛЬЗЯ искать сайт банка путем поискового запроса в браузере и переходить по интернет-ссылке. Адрес сайта нужно знать и вводить «вручную» в адресной строке. Лучше использовать мобильное приложение, скачанное из официального источника.

Акции от имени банков о выплате средств за прохождение анкетирования или опроса – ФЕЙК!

Не вводите личные или финансовые реквизиты после перехода по неизвестным ссылкам от незнакомцев

Для получения денег на карту НЕ НУЖНЫ 3 цифры с обратной стороны карты и коды из SMS (это данные для списания средств!!!)

5. Пятая схема – ИНТЕРНЕТ-ВЫМОГАТЕЛЬСТВО

Знакомства в социальных сетях.

Мошенники создают фальшивые профили в приложениях для знакомств или в социальных сетях, используя украденные фотографии

привлекательных людей. Долгое время поддерживают отношения с потенциальной жертвой, чтобы в конечном итоге попросить деньги (под предлогом болезни, проблем с визой, оплаты посылки и т.д.).

В ходе доверительного общения в сети Интернет (например, с парнем от имени девушки в мессенджере или социальной сети) злоумышленник получает интимные материалы, после чего за неразглашение их требует перевода денежных средств.

При аналогичных переписках с «обратной стороны сети» пользователь просит на Айфоне авторизоваться потерпевшего в чужой учетной записи iCloud по предоставленным реквизитам, после чего, зная пароль, удаленного блокирует телефон и требует деньги за разблокировку.

НУЖНО ЗНАТЬ:

за «аватаркой» друга или случайного знакомого может скрываться преступник, не стоит распространять в сети личные материалы или финансовые данные;

никогда не входите по просьбе случайных знакомых в учетную запрись iCloud или иные.

6. Шестая схема – «ФЕЙК-БОСС»

Злоумышленники изучают средства обмена сообщениями (данные участников переписки, содержание сообщений в чатах, группах, каналах и личных переписках (VIBER, TELEGRAM) в различных мессенджерах и социальных сетях, используемых работниками для коммуникации, определяют учетные записи руководителей, создают копии их учетных записей и вступают в личную переписку с иными участниками таких чатов.

В ходе переписки, выдавая себя ЗА РУКОВОДИТЕЛЯ, злоумышленник сообщает вымышленные сведения о том, что работником интересовались сотрудники правоохранительных органов (называет данные этих «сотрудников») и настаивает на сохранении конфиденциальности факта общения. Указанный психологический прием в ряде случаев снижает уровень критической оценки гражданином последующих действий преступников, обеспечивая беспрекословное выполнение поступающих от них указаний.

Далее гражданину поступают звонки посредством мессенджеров или телефонной связи от якобы сотрудников правоохранительных органов, а также банковских учреждений, в некоторых случаях с демонстрацией посредством мессенджеров фотографии поддельных служебных удостоверений. В ходе беседы псевдосотрудники убеждают в необходимости совершения определенных действий, в том числе по

перечислению денежных средств под различными мошенническими предлогами.

НУЖНО ЗНАТЬ:

при поступлении подобных сообщений в мессенджерах проверять принадлежность соответствующей учетной записи тому лицу, именем которого учетная запись названа и (или) фотоизображение которого присутствует в профиле – сверить абонентский номер (МЕССЕНЖЕР ПРОИНФОРМИРУЕТ, что номер собеседника не записан в вашей телефонной книге), связаться с владельцем учетной записи по иным каналам связи;

никому не сообщать реквизиты банковских карт, аутентификационные данные для доступа к банковским счетам, содержание sms-сообщений, поступивших на личные абонентские номера, выполнять инструкции;

в случае осуществления несанкционированного доступа к учетной записи интернет-мессенджера или социальной сети принимать незамедлительные меры по уведомлению о случившемся граждан, общение с которыми осуществлялось в указанном интернет-мессенджере или социальной сети, с целью предупреждения о возможных попытках осуществления в отношении них преступных действий;

незамедлительно информировать о выявленных попытках руководство организации (предприятия) для принятия мер по упреждению подобных действий и правоохранительные органы для реагирования.

Также (реже) в Гродненской области фиксируются иные схемы киберпреступлений:

оплата на сомнительных сайтах услуг оформления виз для выезда в другие страны;

предоплата на аренду «жилья» после поиска объявлений в сети Интернет.

Чтобы создать привлекательное объявление о сдаче жилья мошенники используют фотографии, найденные в интернете, а также используют привлекательные цены, чтобы привлечь внимание. Прежде чем показать квартиры, всегда просят предоплату. Личная встреча с арендодателем и осмотр жилья перед оплатой позволят не остаться без жилья и денег. Некоторые мошенники утверждают, что не могут встретиться с потенциальными арендаторами по различным причинам (например, находятся в другом городе).

хищение средств под видом оплаты выигрыша в сети Интернет;

перевод денег «возлюбленному», представляющемуся женщинам в переписке в мессенджере «военным», «врачом», «умирающим миллионером», «актером», попавшему в сложную ситуацию, требующую оплаты расходов для приезда в Республику Беларусь, растаможивания «ценного подарка» и т.п. (например, известен факт общения от имени актера Киану Ривза);

завладение деньгами путем фейковых объявлений о помощи больным людям (благотворительность);

хищение путем просьб об одолжении денежных средств в социальной сети или в мессенджере обратившемуся в переписке «другу».

ВАЖНО ЗНАТЬ:

ряд сайтов либо аккаунтов могут быть фейковыми, они создаются в любой точке мира, нельзя решать любые финансовые вопросы в сети Интернет, обстоятельства уточнять личным звонком или при встрече; нельзя сообщать личные и финансовые данные; переходить по неизвестным ссылкам и сайтам, когда потребуется ввод личных данных и реквизитов (паспортные данные, реквизиты БПК, коды из СМС, логины и пароли к ученым записям, скачивание программ, подтверждение запроса на подключение аккаунта на второе устройство и т.д.)

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но всем гражданам в любой ситуации следует не терять бдительность, обдуманно относится ко всему происходящему в сети Интернет. Необходимо мыслить критически и не принимать поспешных решений. Посоветуйтесь с членами семьи или друзьями. Ведь в большинстве случаев излишняя доверчивость и неосмотрительность самих граждан способствует совершению вышеуказанных преступлений.

ФОРМЫ соучастия граждан в преступной деятельности мошенников:

«работа» курьером: у обманутых граждан забрать/передать/перечислить деньги);

продажа мошенникам банковских карт и их реквизитов (логин и пароль к интернет-банку), которые используются для вывода похищенных средств.

Пример по делу «курьера»:

«Обманули и подставили: пенсионерка из Гродно поверила мошенникам и оказалась под следствием».

Гродненским межрайонным отделом Следственного комитета устанавливаются обстоятельства мошенничества, совершенного в особо крупном размере.

По данным следствия, в конце декабря прошлого года на домашний телефон 80-летней жительницы Гродно позвонил якобы «сотрудник Следственного комитета». С первых минут разговора он шокировал пенсионерку ложной информацией: на её имя оформлен кредит, по которому проведены сомнительные операции, часть из них – это переводы на финансирование экстремистской деятельности.

Злоумышленник убедил женщину, что за эти действия ей грозит уголовная ответственность, и заявил о необходимости срочно получить в Москве справку, подтверждающую её непричастность. При этом он не называл ни конкретных должностных лиц, ни адресов государственных учреждений, где можно получить такой документ.

Испуганная возможными последствиями, пенсионерка без возражений выполняла все указания мошенников. Одним из «поручений» было забрать «документы» у двух жителей областного центра, которые якобы оказались в аналогичной ситуации, и отвезти их в Москву.

В тот же день женщина, передвигаясь на такси, поехала по указанным адресам, где её действительно ждали люди. Однако передавали они ей вовсе не документы, а денежные средства. Продолжая следовать инструкциям требовательного собеседника, жительница Гродно села в маршрутное такси, чтобы доехать до Минска. По пути транспорт остановили сотрудники ГАИ, которые обнаружили в её личных вещах более 84 тысяч рублей.

На допросе женщина пояснила, что мошенники говорили с ней настолько убедительно, что у неё не возникло ни малейших сомнений в их искренности. О том, что незнакомые люди будут передавать ей деньги вместо документов, её никто не предупреждал.

Гродненским межрайонным отделом Следственного комитета возбуждено уголовное дело по ч.4 ст.209 (мошенничество, совершенное в особо крупном размере) Уголовного кодекса Республики Беларусь.

Окончательная правовая оценка действиям фигурантки будет дана по результатам расследования.

Ответственность «курьера» за соучастие в преступлении – статья 209 Уголовного кодекса (максимальное наказание – до 12 лет лишения свободы со штрафом)

За продажу личной банковской карты либо реквизитов доступа к своему карт-счету – статья 12.35. КоАП (штраф от 20 до 50 базовых величин, общественные работы или арест)

За продажу чужих банковских карт либо реквизитов доступа к чужим карт-счетам) – статья 222 Уголовного кодекса (максимальное наказание до 10 лет лишения свободы).

ЛЮБЫЕ ДЕЙСТВИЯ В ИНТЕРНЕТЕ НАВСЕГДА ОСТАВЛЯЮТ ЦИФРОВОЙ ОТПЕЧАТОК (СЛЕДЫ), ПО КОТОРОМУ УСТАНАВЛИВАЮТ ВИНОВНОЕ ЛИЦО

ВСЯ ВЫЛОЖЕННАЯ В ИНТЕРНЕТ ЛИЧНАЯ и ФИНАНСОВАЯ ИНФОРМАЦИЯ МОЖЕТ БЫТЬ ИСПОЛЬЗОВАНА ПРОТИВ ВАС (ЦИФРОВОЕ ДОСЬЕ)

Telegram-канал Следственного комитета, в котором публикуются актуальные схемы, используемые кибермошенниками и другая информация о противодействии киберпреступлениям:

Еженедельно по пятницам в эфире «Радио Гродно» в 17:50 отделом цифрового развития предварительного следствия УСК по Гродненской области жителям региона доводится актуальная информация о зафиксированных схемах киберпреступлений за неделю.