УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ
ГЛАВНОГО УПРАВЛЕНИЯ ВНУТРЕННИХ ДЕЛ
МИНСКОГО ГОРОДСКОГО ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

КОНСПЕКТ

ОБ АКТУАЛЬНЫХ СПОСОБАХ И МЕТОДАХ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ И РЕКОМЕНДАЦИЯХ ПО ИХ НЕДОПУЩЕНИЮ

г. Минск
2026

ВВЕДЕНИЕ

Глобальная сеть Интернет стала незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники этим пользуются. Киберпреступность стремительно расширяет свой масштаб, она проникла во все сферы общественной жизни, включая бизнес-структуры, общественную и личную жизнь граждан.

Практически ежегодно в столице наблюдается рост регистрируемых преступлений, совершенных в сфере высоких технологий. Устойчивая тенденция увеличения количества совершаемых киберпреступлений обусловлена активным развитием информационных технологий. Широкое вовлечение процессов, связанных с жизнедеятельностью общества, в интернет-среду объективно изменило вектор противоправных деяний, все более направляя его в киберпространство.

В 2025 году киберпреступления в структуре общей преступности составили более трети (38,0%).

Справочно: 2015 год – 3,8%; 2016 год – 4,3%; 2017 год – 6,5%; 2018 год – 9,1%; 2019 год – 16,3%; 2020 год – 37,4%; 2021 год – 25,6%; 2022 год – 25,2%; 2023 год – 33,7%; 2024 год – 37,6%.

Принятые в 2025 и начале 2026 года всеми заинтересованными предупредительные меры, в части проведения профилактической работы с широким охватом населения, направленной на упреждение совершения киберпреступлений, в целом благоприятно повлияли на состояние криминогенной обстановки в г. Минске в сфере противодействия киберпреступности, что выразилось в снижении к концу 2025 года таких преступных деяний с сохранением указанной тенденции в текущем году.

Несмотря на общее снижение уровня общеуголовной преступности, доля киберпреступлений из всех преступлений, зарегистрированных на территории г. Минска, увеличилась с 38,0% по итогам 2025 года до 41,9% за первый квартал 2026 г.

В сравнении с аналогичным периодом прошлого года в г. Минске отмечается снижение числа учтенных хищений путем модификации компьютерной информации (-16,4%; с 549 до 459) и заведомо ложных сообщений об опасности (- 46,5%; с 43 до 23).

При этом в целом по городу значительно возросло количество вымогательств (+89,6%; с 48 до 91), отмечается рост общего числа учтенных мошенничеств (+4,3%; с 684 до 713), совершенных с использованием информационно-коммуникационных технологий (далее – ИКТ).

Структура зарегистрированных ИКТ-вымогательств выглядит следующим образом:

- Блокировка учетных записей iCloud – 61 (67,0%),

- Угроза разглашения компрометирующих материалов интимного характера – 29 (31,9%),
- Блокировка компьютерной информации – 1 (1,1%).

В структуре киберпреступности, как и прежде, превалируют ИКТ-мошенничества и хищения путем модификации компьютерной информации (53,1% и 35,5% соответственно).

Структура зарегистрированных ИКТ-мошенничеств, как основного вида регистрируемых киберпреступлений, выглядит следующим образом:

- приобретение несуществующих товаров (услуг) на интернет-ресурсах (50,2%; 358 из 713);
- каждое третье преступление (33,5%; 239 из 713) совершается с использованием методов социальной инженерии и вишинга.

По количеству случаев методы распределились следующим образом:

*- РУП «Белпочта» – **87** фактов или 36,4%;*

*- коммунальные предприятия – **81** факт или же 33,9% (Водоканал – 23; замена домофона – 47; Энергосбыт – 10; Мингаз – 1);*

*- имитация деятельности представителей государственных органов и финансовых организаций (ОВД, КГК, КГБ, банковских учреждений, операторов связи) – **40** фактов (16,7%);*

*- социально-профессиональные легенды: учреждения здравоохранения – **17** фактов (7,1%), а также юридические работники организаций – **14** (5,9%).*

- фиктивное инвестирование (10,0%; 71 из 713)
- взлом учетных записей в соцсетях и мессенджерах (1,4%; 10 из 713);
- сообщения/звонки от руководителя (1,1%; 8 из 713);
- мошенничества под видом знакомства (2,1%; 15 из 713).
- ложные выигрыши (1,7%; 12 из 713).

В результате преступных посягательств по линии противодействия киберпреступности по итогам первого квартала 2026 г. в столице пострадало 1 368 лиц (2025 г. – 1 301):

- 813 (59,4%) в результате мошеннических действий;
- 438 (32,1%) хищения путем модификации компьютерной информации;
- 91 (6,6%) вымогательства;
- 26 (1,9%) преступления против компьютерной безопасности.

Проведенный виктимологический анализ позволяет сделать вывод, что доминирующим профилем жертвы от совершаемых киберпреступлений выступает возрастная категория 36-64 лет (более 600 из 1368). Как правило – это социально успешные люди, имеющие стабильный доход, накопления, недвижимость. Именно

материальная беспечность, сформированная привычка доверять «людям в пагонах» или официальным инстанциям, необдуманные действия по указанию «сотрудников безопасности» банка, «юридических работников» организаций делает их главной мишенью для киберпреступников.

Несмотря на высокую технологическую грамотность, жертвами киберпреступников в 474 случаях стали лица возрастной группы 19-35 лет.

Каждый 10 потерпевший – гражданин возраста 65 лет и старше (135 или 9,9%). Основным способом совершения противоправных деяний в отношении данной категории граждан является вишинг посредством звонков по стационарной и сотовой связи, в том числе в мессенджерах, от имени работников коммунальных предприятий и схожее с этим.

АКТУАЛЬНЫЕ СПОСОБЫ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Мошенничества, связанные с приобретением несуществующих товаров (услуг) на интернет-ресурсах

Основная доля мошенничеств, совершаемых в столице, связана с приобретением различных товаров *(цветочная продукция, мобильные телефоны, предметы одежды, шины, мебель, сезонные товары, продукты питания и пр.)* и услуг *(аренда недвижимости, помощь в оформлении виз, туров и т.п.)* в сети Интернет.

Так, в социальной сети «Instagram» злоумышленники создают поддельные (фейковые) аккаунты (страницы) с высокими рейтингами и отзывами покупателей, внушительным количеством подписчиков, где предлагают продажу товара по явно заниженной стоимости. Как правило, продажа интересующего товара предусматривает 100% предоплату (реже частичную), после внесения которой псевдопродавцы перестают выходить на связь с покупателем либо вовсе удаляют аккаунты.

<u>Пример 1:</u> Владимир посредством социальной сети «Instagram» нашел интернет-магазин «@pufs.mebel», специализирующийся на продаже садовых качелей. Для оформления заказа в шапке профиля была размещена ссылка на аккаунт в мессенджере «Telegram». Владимир перешел по ссылке и оформил заказ, произведя при этом полную предоплату за товар и его доставку на предоставленный продавцом номер банковской карты (399 бел.руб.). В связи с тем, что в оговоренный срок садовые качели доставлены не были, Владимир связался с продавцом и потребовал вернуть деньги. Продавец в свою очередь предоставил Владимиру ссылку (фишинговый сайт Приорбанка) для возврата денежных средств. Перейдя по указанной ссылке, Владимир ввел полные

реквизиты своей банковской платежной карты (16-значный номер, срок действия и CVV-код), после чего с нее были похищены все денежные средства.

Пример 2: Татьяна и Олег в мессенджере "Telegram" в группе "FlattyBy" нашли объявление о сдаче в аренду квартиры в г. Минске. Молодые люди списались с лицом, разместившим указанное объявление, и договорились об аренде квартиры. «Арендодатель» сообщил о необходимости внесения залога в размере 300 бел.рублей. Олег совершил перевод денежных средств в размере 300 бел.рублей на предоставленный ему номер БПК. В последующем неизвестное лицо заблокировало Олега в мессенджере "Telegram", а объявление о сдаче квартиры в аренду было удалено.

Пример 3: в социальной сети «Instagram» 40-летний Денис нашел аккаунт с туристическими услугами. Он связался с менеджером, который предложил «горящий тур» в Египет по выгодной цене. Денис согласился, после чего представитель турагентства сообщил, что вылет на отдых запланирован через несколько дней, поэтому необходимо внести 100% предоплату. Мужчина перевел 8500 белорусских рублей на предоставленный счет, после чего с ним перестали выходить на связь и удалили переписку.

Что должно **насторожить** покупателя, если он приобретает товары или услуги онлайн?

- подозрительно низкие цены на товар или услугу;
- 100% предоплата;
- требование продавца ввести паспортные данные или полные реквизиты БПК;
- предложение перейти по ссылке.

! Рекомендации:

1. не совершайте покупки в магазинах из социальных сетей, если у вас требуют полную предоплату;
2. не переходите по подозрительным ссылкам и не вводите личные данные и реквизиты БПК;
3. заведите отдельную банковскую платежную карту для оплаты товаров и услуг в сети Интернет и переводите на нее сумму равную сумме покупки;
4. выбирайте надежных и проверенных продавцов.

ВНИМАНИЕ! Проверить ссылку или имя аккаунта на предмет мошенничества можно с помощью Telegram-бота @SCAMBY_BOT.


Привет! Я бот ScamBY!
Найду свет в темноте, подсвечу опасность!
Проверка сайтов
Проверка Instagram
Проверка Telegram
Проверка TikTok
Отправь ссылку или имя аккаунта –
проверю ресурс на мошенничество!
БЕЛАРУСЬ
Попробуй прямо сейчас!
Проверь ресурс
с ScamBY!
@SCAMBY_BOT

Звонки от имени представителей правоохранительных органов, банковских учреждений, сотовых компаний, работников коммунальных и телекоммуникационных предприятий, медицинских организаций и т.п. (вишинг)

Злоумышленник звонит на стационарный телефон, представляется сотрудником сотовой компании (МТС, А1, Life), работником коммунальных (Мингаз, Минскэнерго, Энергосбыт и пр.) или телекоммуникационных предприятий (Белтелеком), медицинских организаций и в разговоре сообщает о необходимости дистанционного продления (перезаключения) договора на оказание услуг, замены устаревшего оборудования, оперативной сверки показателей счетчиков, приглашает на диспансеризацию либо указывает на необходимость обновить данные амбулаторной карты и т.д. При этом для верификации и удобства требует предоставить персональные данные (идентификационный номер паспорта, номер мобильного телефона, иные личные данные), а также просит сообщить поступивший по смс-сообщению код подтверждения. В это время параллельно на мобильный телефон жертвы (как правило посредством мессенджера «Viber» либо «Telegram») поступает звонок якобы от сотрудника правоохранительных органов или банка, который сообщает, что в данный момент по стационарному телефону жертва общается с мошенниками и что разговор необходимо прервать. После этого «псевдоправоохранитель» действует по стандартной мошеннической схеме и сообщает, что:

- на имя потерпевшего оформили кредиты;
- с расчетных счетов потерпевшего осуществляется финансирование террористической деятельности либо военных действий в Украине;
- необходимо оказать помощь правоохранительным органам в поимке аферистов;
- в связи с тем, что в отношении потерпевшего возбуждено уголовное дело и у него в ближайшее время по месту жительства будет проведен обыск, необходимо срочно обезопасить накопленные денежные средства, для чего осуществить их декларирование либо перевод на специальный «безопасный» счет;
- оказать содействие другим жертвам мошенников, которые в силу возраста или физических особенностей не могут самостоятельно обратиться в банк для зачисления наличных денежных средств на безопасный счет.

После всего услышанного жертва испытывает эмоциональный шок. Ведь сложно поверить, что это все четко спланированная мошенническая схема. Потерпевшие, идя на поводу аферистов, следуют их инструкциям

и добросовестно исполняют все, что те от них требуют, даже продают собственное жилье и вырученные деньги также переводят на предоставленные злоумышленниками счета.

Необходимо отметить, что мошенники до такой степени втираются в доверие жертв, что при попытках ИСТИННЫХ сотрудников милиции или работников банковских учреждений их образумить, чаще всего игнорируют все разумные доводы.

<u>Пример 1:</u> В начале мая 60-летнему Николаю Анатольевичу на домашний телефон позвонила женщина, которая представилась сотрудницей «Энергосбыта» и сообщила о необходимости замены счетчиков. Пожилого мужчину данный факт не смутил, так как около 1 месяца назад он оставлял заявку на замену счетчиков.

Сотрудница «Энергосбыта» попросила предоставить идентификационный номер паспорта, а также код, полученный по смс-сообщению, якобы для подтверждения заявки. После окончания разговора с указанной сотрудницей, Николаю Анатольевичу на мобильный телефон посредством мессенджера «Viber» с белорусского мобильного номера телефона позвонил ранее неизвестный мужчина, который представился подполковником юстиции Князевым Виталием Владимировичем из управления Следственного комитета Республики Беларусь и в ходе разговора пояснил, что у них сработала специальная система по предупреждению мошеннических звонков с неизвестных номеров. В ходе диалога Князев В.В. пояснил, что пожилой минчанин стал жертвой мошенников, которые по личному номеру паспорта через подставных лиц берут кредиты. Также Князев В.В. пояснил, что с потенциальным потерпевшим должен связаться специалист из Национального Банка Республики Беларусь. После окончания звонка от Князева В.В., посредством мессенджера «Viber» позвонил неизвестный мужчина, который представился как Исаев Игорь Леонидович - специалист Национального Банка, и пояснил, что в настоящее время участились случаи мошенничества в Республике Беларусь, а именно после предоставления личных данных происходит взятие кредитов, снятие пенсий по предоставленным данным. В ходе беседы Исаев И.Л. разговаривал очень четко, ссылался на нормативно-правовые акты Республики Беларусь, в связи с чем каких-либо сомнений у Николая Анатольевича по данному поводу не возникло. В процессе разговора Исаев И.Л. пояснил, что все банковские карточки Николая Анатольевича решением Национального Банка будут заблокированы, и все денежные средства пропадут. Также Исаев И.Л. указал, что зафиксированы попытки получения кредитов в различных банках столицы. Для того, чтобы вычислить мошенников, нужно взять контрольные кредиты, и в последующем сделать перевод по их погашению. Николай Анатольевич снял последние денежные средства, которые у него имелись, после чего направился в банковские учреждения, где оформил договоры на кредиты. При оформлении указанных кредитов сотрудники банков интересовались, для каких целей ему нужны денежные средства и не находится ли он под влиянием третьих лиц,

а также предупреждали о мошенниках, на что тот пояснил, что денежные средства нужны на личные нужды.

Получив кредитные средства, Николай Анатольевич перевел их на реквизиты банковской карты, которые указал ему Исаев И.Л.

Необходимо отметить, что при осуществлении потерпевшим переводов, представители банков уточняли, куда, кому и с какой целью Николай Анатольевич переводил деньги, разъясняя ему, что он действует нелогично и, скорее всего, находится под чьим-то влиянием, то есть мошенников.

Наряду с этим, потерпевшему по мобильной связи звонил участковый инспектор милиции и расспрашивал, кому тот делал переводы. Во время разговора с участковым Николай Анатольевич «плавал» и понимал, что все то, что ему описывает НАСТОЯЩИЙ сотрудник милиции в качестве преступной схемы, аналогичным способом происходит и с ним сейчас. В тот момент Николай Анатольевич начал осознавать, что свои кредитные деньги он перевел мошенникам, однако участковому не сказал правду, обманув его, что распоряжается деньгами по своему усмотрению и попросил впредь его не беспокоить.

Не желая быть обманутым со стороны якобы спецслужб, 60-летний мужчина решил позвонить Исаеву И.Л. и сообщить о своих предположениях об участии в противоправных действиях, однако Исаев И.Л. уверил его, чтобы тот ни от кого не брал трубки, кроме него, Князева В.В., а также Сафронова Кирилла Алексеевича, который, в последующем, позвонил по видеосвязи и представился начальником Следственного отдела и руководителем Князева В.В. Сафронов К.А. разъяснял потерпевшему, что все деньги по кредиту ему вернут. При этом Сафронов К.А. был одет в форменное обмундирование, в связи с чем каких-либо сомнений у Николая Анатольевича снова не возникло.

Далее в ходе телефонной беседы Исаев И.Л. сообщил, что Николаю Анатольевичу нужно будет ехать в Москву, чтобы помочь в специальной операции по выявлению мошенников.

Так, по указанию Исаева И.Л., с использованием кодового слова, озвученного им же, мужчина забрал крупную сумму денежных средств у двух минчанок (75 и 45 лет), которые передали ему денежные средства в целлофановых пакетах. Далее по указанию Исаева И.Л., Николай Анатольевич приобрел билет на поезд до Москвы.

По приезду в г. Москва Николай Анатольевич заселился в гостиницу «Канна» и проживал там на протяжении суток. На следующий день ему позвонил Исаев И.Л., который сообщил, что тот должен встретиться с его коллегой. Далее, по прибытию в указанное Исаевым И.Л. место, к Николаю Анатольевичу подошел молодой человек 28-30 лет неопрятного внешнего вида. Николай Анатольевич передал ему денежные средства, после чего вернулся обратно в гостиницу. По возвращению в гостиницу Исаев И.Л., Князев В.В. и Сафронов К.А. перестали выходить на связь.

По возвращению в г. Минск к Николаю Анатольевичу по месту жительства прибыли сотрудники столичной милиции, которые сопроводили

его в ближайшее РУВД. И только в РУВД Николай Анатольевич окончательно убедился, что с ним до этого общались мошенники.

При беседе с сотрудниками милиции Николай Анатольевич пояснял, что неоднократно слышал в новостях и телепередачах о преступных схемах мошенников, более того помочь разобраться в ситуации ему пыталась и супруга, но Николай Анатольевич решил игнорировать все ее доводы, полагая, что он сам знает, как лучше поступить, и в итоге стал жертвой аферистов и соучастником преступления.

Пример 2: Татьяне в мессенджере «Telegram» от пользователя «Виктория Николаевна» поступило сообщение от девушки, которая представилась медсестрой из поликлиники и сообщила, что обнуляется медицинская карта и необходимо уточнить рост, после чего задала несколько вопросов касаемо аллергии, а также об актуальности абонентского номера телефона. Далее псевдомедсестра попросила сообщить код, который поступил Татьяне по смс-сообщению, и прекратила разговор. Через несколько минут Татьяне на мобильный телефон поступил звонок от незнакомого мужчины, который представился сотрудникам «МТБанк» и пояснил, что только что она общалась с мошенником и ввиду того, что предоставила данные о себе и сообщила смс-код, на ее имя оформлен кредит. Далее с женщиной в мессенджере «Telegram» связался якобы сотрудник Национального банка Республики Беларусь с именем «@Koltsov9887» и сообщил о том, что необходимо взять все имеющие у Татьяны денежные средства и положить их на свой счет в ЗАО «Альфа-Банк» якобы для их дальнейшего декларирования, что та и сделала. Так, Татьяна осуществила зачисление наличных денежных средств в размере 4 240 бел. руб. на свою БПК, эмитированную ЗАО «Альфа-Банк», после чего по указанию мошенников осуществила ряд переводов денежных средств на различные якобы безопасные счета на общую сумму 4 100 бел. руб. Далее Татьяне пояснили, что необходимо дождаться следующего дня, чтобы закрыть ранее оформленный на ее имя кредит. Через некоторое время Татьяна обдумала произошедшее и поняла, что попалась на уловку мошенников, после чего обратилась в милицию.

Нередки случаи, когда злоумышленник просит установить на мобильный телефон программу удаленного доступа, завуалировать под приложение интернет-банкинга и иное, после чего, получив доступ к устройству, кибераферист оформляет онлайн-кредит на имя потерпевшего без его ведома.

Кроме того, мошенники могут действовать по следующей схеме обмана: гражданину поступает звонок от «специалиста компании оператора сотовой связи (A1, МТС, Life) с использованием различных мессенджеров (Viber, Telegram, WhatsApp). В ходе телефонного разговора злоумышленник под предлогом обновления официального приложения, продления договора обслуживания и т.п., отправляет ссылку для скачивания вредоносного файла (формата «.apk»).

После скачивания и запуска указанного файла, производится установка приложения удаленного доступа внешне схожего с официальным приложением оператора сотовой связи. Установленное приложение обладает функциональными возможностями, предоставляющими доступ злоумышленнику к функциям мобильного телефона, в том числе камере, микрофону, файлам, хранящимся на устройстве, списку контактов, смс-сообщениям и др. Полученные сведения могут быть использованы для совершения хищения денежных средств с банковских счетов и иных противоправных действий в отношении владельца мобильного телефона (завладение информацией и иное).

! Рекомендации:

1. ни под какими предлогами не сообщайте посторонним паспортные данные, не предоставляйте информацию о реквизитах банковской карты (номере, сроке ее действия, ПИН-коде, CVV2/CVC2 коде) или одноразовые коды, поступившие на мобильный телефон по смс-сообщению, даже если звонят лица, представляющиеся сотрудниками правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работниками коммунальных служб или телекоммуникационных компаний;
2. не оформляйте кредиты по указанию третьих лиц;
3. не проводите через банкоматы и иные устройства самообслуживания (включая систему дистанционного банковского обслуживания) никакие операции под психологическим давлением или по инструкциям, полученным по телефону или мессенджерам;
4. не устанавливайте на мобильный телефон приложения по просьбе третьих лиц, даже если они настоятельно этого требуют;
5. не становитесь курьером мошенников путем собирания денежных средств у других граждан, попавших в неприятную жизненную ситуацию;
6. при поступлении ЛЮБОГО сомнительного звонка, незамедлительно завершите разговор и обратитесь в милицию.

ПОМНИТЕ! Сотрудники правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работники государственных организаций и предприятий, коммунальных служб или телекоммуникационных компаний НИКОГДА не выясняют ваши персональный данные по телефону!

Для оформления заявок на оказание услуг по телефону, указание идентификационного номера паспорта либо реквизитов банковской пластиковой карты НЕ ТРЕБУЕТСЯ!

Инвестирование
(трейдинг и другие способы легкого заработка в сети Интернет)

Особо актуальная на сегодняшний день схема обмана под предлогом дополнительного заработка, связанного с инвестициями или трейдингом («финансовые эксперты» обещают высокий доход).

Посты и рекламные баннеры в сети Интернет (соцсетях) часто обещают быстрый и очень высокий доход. Их цель – завлечь людей на мошеннические сайты, где якобы можно инвестировать деньги в ценные бумаги и получить прибыли больше, чем на других площадках.

Иногда такие сообщения (посты) появляются на страницах, которые мошенники специально создают под видом обычных пользователей. Также злоумышленники заводят фейковые аккаунты реально существующих банков или известных финансовых экспертов, и размещают публикации от их имени.

Часто для обмана злоумышленники создают сайты, которые сложно отличить от настоящих сайтов банков и брокерских компаний. А еще выкладывают посты в соцсетях от имени вымышленных людей или выступают под видом компетентных экономистов, рекламируя подозрительные инструменты с высоким доходом.

Как правило, мошенники предлагают повышенную доходность. Обычные вклады в рублях приносят 10-15% годовых. Мошенники же обещают, как минимум 20-30%, а иногда и больше – это может быть и 70%, и 250% в год.

Но важно помнить: высокая доходность связана с большими рисками и гарантировать ее невозможно. Для мошенников же достоверность цифр значения не имеет, главное – зацепить внимание человека и заставить его зарегистрироваться на сайте.

Затем они просят якобы «пополнить свой счет», а по факту – перевести деньги, чаще всего на карту физического лица или электронный кошелек.

После регистрации мошенники «прикрепляют» к обманутому пользователю так называемого «финансового эксперта», который якобы должен советовать активы к покупке и помогать инвестировать. На самом деле его задача – убедить человека вложить как можно больше денег. «Эксперт» будет говорить, что торговля идет хорошо и Вы получаете прибыль, но растущие цифры на сайте ничего не значат: деньги не попадают на биржу, а мошенники могут имитировать любой доход.

Фейковый рост депозита внушает доверие, это побуждает отправить мошенникам еще больше денег. Иногда, чтобы им доверяли, мошенники переводят жертве небольшую сумму под видом прибыли с биржи. Так они

пытаются показать, что их схема заработка работает и нужно вкладывать еще.

Вернуть свои деньги практически невозможно. Если отказаться от новых переводов или сказать, что денег нет, мошенники будут давить: говорить, что нужно брать кредит, продавать телефон, автомобиль, недвижимость, ведь сейчас есть уникальная возможность заработать и все вложения окупятся. А если человек решит настоять на выводе денег, его попросят оплатить комиссию.

Интернет-мошенники – хорошие психологи, которые знают, как вызвать интерес, расположить собеседника к себе и убедить человека расстаться с собственными сбережениями.

Пример 1: Полина в мессенджере «Telegram» обнаружила пользователя «@confidential_inf8», который рассказал о возможностях дополнительного заработка путем оформления ставок на спортивные события. Со слов злоумышленника, он обладал информацией о «покупных» матчах и играх, в виду чего гарантировал стабильный заработок через ставки. Будучи введенной в заблуждение, Полина в вышеуказанный период времени под предлогом оплаты налогов и страховых взносов для вывода выигрыша осуществила неоднократные пополнения предоставленных злоумышленником счетов на сумму не менее чем 19 186 бел.рублей. Однако вывести выигрыш не удалось.

Пример 2: 48-летний Алексей в ноябре 2025 года в сети Интернет нашел предложение о дополнительном заработке путем вложения в инвестиции. В последующем в период с ноября 2025 г. по январь 2026 г. Алексей со своей БПК осуществлял переводы денежных средств на БПК, реквизиты которых были ему предоставлены, после чего совершал под руководством "менеджера" сделки. После каждого перевода денежных средств со своих БПК, Алексей видел, что баланс его счета на бирже также пополняется, ввиду чего спокойно продолжал совершать сделки. После середины января мужчина решил вывести с лицевого счета на бирже около 18 тысяч долларов США, однако ему поступило сообщение с просьбой внести дополнительный платеж в сумме 2 348 долларов США «для фиксации курса обмена», путем перевода на криптокошелек. Заявитель понял, что общение с ним вели мошенники. Здесь необходимо отметить, что для совершения вышеописанных сделок Алексей взял в банке кредит на сумму 9 500 бел.рублей, а также некоторую сумму денежных средств брал в долг у знакомых. Таким образом, сумма ущерба составила порядка 86 000 бел.рублей.

Не единичны случаи, когда жертвы такого рода мошенничеств пытаются самостоятельно вернуть похищенные денежные средства посредством поиска «юридической помощи» в сети Интернет.

Пример: Николай, вложивший в 2025 году в фейковую торговую биржу порядка 5 тысяч евро, в социальной сети «Instagram» нашел компанию, которая оказывает юридические услуги по возврату похищенных денежных средств

(криптовалюты). Так, за «запуск процедуры возврата» и под иными «весомыми» предлогами Николай перевел указанной компании 1 800 долларов США. Само собой деньги минчанину так и не вернули ни в первом, ни во втором случае.

! Рекомендации:

1. не верьте обещаниям легкого заработка в интернете. Прежде чем вкладывать деньги в какие-либо проекты, проверьте достоверность предложения поиском в браузере или по телефонам организаций, размещенным на их сайтах;
2. ведите переписку и совершайте сделки только на официальных биржах.

Взлом аккаунта (учетной записи)

Не теряют своей актуальности мошенничества, сопряженные с несанкционированным доступом (взломом) к учетным записям в различных социальных сетях и мессенджерах (Одноклассники, ВКонтакте, INSTAGRAM, Telegram, Viber и пр.) и последующей рассылкой сообщений с просьбой перевода денежных средств в долг либо оказания материальной помощи на лечение.

Пример: Максиму в мессенджере «Telegram» пришло сообщение с учетной записи его девушки Веры о необходимости перевода 150 бел.рублей для осуществления ею выкупа покупок с маркетплейса «Wildberries». Ничего не заподозрив, Максим осуществил перевод денежных средств на указанные в сообщении от Веры реквизиты БПК. Спустя 10 минут молодому человеку позвонила его девушка и сообщила, что ее учетную запись в мессенджере «Telegram» взломали и стали рассылать сообщения различного содержания всем ее контактам, после чего Максим понял, что отправил денежные средства мошенникам, и обратился в милицию.

! Рекомендации:

1. для обеспечения безопасности своих аккаунтов необходимо устанавливать сложные пароли и двухэтапную аутентификацию;
2. не переходить по ссылкам из различных сообщений, поступивших даже от родных и знакомых людей;
3. при поступлении подобного рода сообщений созвонитесь с человеком, который просит у вас финансовой помощи, для удостоверения правдивости происходящего.

Звонки от имени руководителей организаций

В 2024 году появилась новая схема мошенничества, которая остается актуальной и в настоящее время (схема «Fake boss»). Для реализации такой

схемы злоумышленники предварительно изучают чаты трудовых коллективов в мессенджерах и социальных сетях, собирают информацию об организациях и руководителях, создают учетные записи от их имени. В последующем с помощью поддельного (фейкового) аккаунта руководителя преступники вступают в переписку с подчиненными и, используя авторитет начальника и доверие к нему, дают определенные указания либо разъяснения.

Чаще всего лжеруководитель требует оказать содействие правоохранительным органам в проверке на предмет причастности к финансированию террористической деятельности либо под предлогом одалживания денежных средств (сообщения могут быть как текстовыми, так и голосовыми).

Пример 1: Кристине в мессенджере «Telegram» поступило сообщение от пользователя, аккаунт которого был внешне похож на аккаунт главврача поликлиники, где она работает. В сообщении говорилось о том, что с ней в скором времени в мессенджере «Telegram» свяжется куратор из КГБ. Через некоторое время Кристине поступило сообщение от пользователя, который представился как «Смирнов Андрей». Последний сообщил, что на имя Кристины был оформлен кредит, денежные средства из которого были отправлены в Украину и для того, чтобы избежать проблем, женщине необходимо перевести оставшиеся у нее денежные средства на безопасный счет. Ей были предоставлены реквизиты, на которые она в последующем осуществила денежный перевод в размере 3 500 бел.рублей. Далее при общении с коллегами Кристина узнала, что главврач имеет другой аккаунт в мессенджере «Telegram», после чего поняла, что все это время она общалась с мошенниками.

Пример 2: в конце января 2026 года с ведущим инженером одного из государственных научных учреждений посредством мессенджера «Telegram» связалось неизвестное лицо, которое представилось ее директором и предупредило, что ей будет звонить сотрудник КГБ. После этого женщине в указанном мессенджере от неизвестного лица, подписанного как «Владимир Колесников», поступил звонок, в ходе которого неизвестный мужчина представился сотрудником КГБ и пояснил, что банковские счета последней используются для финансирования экстремистских организаций, в связи с чем, во избежание ареста правоохранительными органами, женщине необходимо перевести денежные средства на «безопасный» счет. В последующем потерпевшая перевела на предоставленные аферистом реквизиты денежные средства в размере 2 550 бел.рублей.

! Рекомендации:

1. при поступлении подобного рода сообщений (звонков), необходимо убедиться в достоверности аккаунта и номера телефона, а также связаться с руководителем по стационарной связи либо иным возможным способом.

Знакомства в Интернете

Знакомства в мессенджерах или социальных сетях все чаще заменяют реальные встречи. Однако стоит внимательно относится к знакомствам в интернет-пространстве, так как за красивым снимком профиля может скрываться мошенник.

Пример 1: Валентина в социальной сети «TikTok» познакомилась с мужчиной по имени «Михаэль». Общение продолжилось в мессенджере «Telegram». В канун 8 Марта Михаэль сообщил женщине, что отправил ей посылку, в которой содержались различные вещи, драгоценности и денежные средства.

Через некоторое время на электронную почту женщины поступило сообщение от ранее неизвестного пользователя, зарегистрированного под именем «Christopher Erica», который сообщил, что необходимо оплатить денежные средства за доставку посылки, и указал реквизиты банковского счета. Данную информацию также продублировал Михаэль в мессенджере «Telegram». По инструкции данного пользователя женщина направилась в банковское учреждение, где через кассу осуществила перевод денежных средств в размере 4 200 бел.рублей на предоставленный ей счет.

Через несколько дней от Михаэля пришло сообщение о необходимости оплаты «растаможки» посылки. Валентина через банковское учреждение осуществила еще 2 перевода денежных средств в размере 8 200 и 8 300 бел.рублей.

В последующем Михаэль сообщил, что денежные средства не поступили ему на счет. Женщина пыталась как-то решить данный вопрос в переписке, а также предложила встречу, однако Михаэль написал, что банк обманывает и денежные средства никуда не направил, и от личной встречи отказался. Валентина осознала, что стала жертвой мошенника.

! Рекомендации:

1. тщательно изучайте аккаунт собеседника;
2. как можно лучше узнайте нового знакомого;
3. созванивайтесь по мобильному телефону и/или по видеосвязи;
4. не ведитесь на просьбы оказать материальную помощь, тем более не отправляйте деньги на «посылки», «госпошлины», «лечение» и прочее незнакомым вам людям;
5. ни под какими предлогами не переходите по подозрительным ссылкам, отправленным вам собеседником, и не вводите личные данные и тем более реквизиты банковской платежной карты.

Фишинг

Фишинг – вид интернет-мошенничества, это когда мошенники создают фейковые (поддельные) сайты или присылают письма и сообщения, чтобы украсть у пользователя пароли, деньги или другую личную информацию.

Как понять, что сайт – фейк (поддельный)?

- внимательно посмотрите на адрес в браузере – если есть странные буквы, цифры или что-то лишнее это плохой знак;
- убедитесь, что в адресе есть https: и значок замка – это значит, что интернет-соединение защищено;
- если сайт оформлен с ошибками в тексте или странными картинками, это должно насторожить;
- если сайт настойчиво требует срочно ввести пароли, данные карты или другую личную информацию – будьте осторожны.

Пример 1: в начале марта т.г. Павел в социальной сети «Instagram» обнаружил аккаунт по продаже цветов «flowersloves.by». Перейдя в данный профиль и изучив ассортимент, мужчина решил сделать заказ. В связи с тем, что указанный магазин затребовал 100% предоплату товара, Павел со своей банковской карты перечислил 150 бел.рублей на предоставленные продавцом реквизиты. В ходе дальнейшего общения продавец сообщил о необходимости оплаты доставки, после чего поступила ссылка для ее оформления. Перейдя по данной ссылке, Павел ввел реквизиты своей банковской карты и коды из СМС-сообщений, после чего с его БПК было списано 125 бел.рублей.

Пример 2: Петр решил на месяц снять квартиру. Так, на сайте «Domovita.by» он нашел объявление о сдаче в найм жилья в г. Борисове. В объявлении был указан контакт для связи в мессенджере «Viber». В ходе переписки девушка, которая представилась Дианой, попросила внести предоплату в размере 500 бел.рублей, для чего предоставила номер БПК, на которую Петр перевел указанную сумму. Однако позже она написала, что квартира уже сдана и предложила вернуть Петру деньги, для чего предоставила соответствующую ссылку (https://alfabank-by.dostavka10.info/receiving/176749185). Петр перешел по указанной ссылке, ввел реквизиты своей БПК, а также код из СМС-сообщения. После этого с его БПК было списано 885 бел.рублей.

Пример 3: Леонид разместил объявление о продаже аэрогриля на торговой площадке «Kufar». Так, в мессенджере «Viber» с ним связался псевдопокупатель, который пояснил, что желает приобрести аэрогриль и оформить курьерскую доставку «Европочты». Далее Леониду была отправлена ссылка «evropochta.by-id715.bond» якобы для получения денежного перевода за продаваемый им аэрогриль, по которой он перешел, ввел реквизиты своей БПК, а также код, полученный по смс-сообщению. В результате с его БПК было списано 830 белорусских рублей.

! Рекомендации:

1. будьте осторожны с тем, что читаете и на что кликаете (нажимаете) в Интернете;
2. не переходите по ссылкам, которые вызывают сомнения;
3. не вводите персональные данные, реквизиты БПК, а также различные смс-коды на подозрительных сайтах.

Кибервымогательства

Все вымогательства, совершенные с использованием информационно-коммуникационных технологий, можно разделить на **три основных вида**:

1. Связаны с **блокированием, модификацией или уничтожением компьютерной информации**. При этом в подавляющем большинстве случаев отмечается блокирование мобильных устройств Apple посредством входа на них в предоставленную злоумышленниками под благовидными предлогами учетную запись iCloud, что в последующем позволяет удаленно включить «режим утери» (тем самым заблокировать устройство) либо стереть данные.

Следует отметить, что ранее большая часть предлогов заключалась в онлайн-знакомстве потерпевших с мошенником, представляющимся лицом противоположного пола, у которого сломался телефон и ему необходимо **оказать помощь в загрузке каких-либо файлов из облачного хранилища iCloud**.

В настоящий момент вектор сместился на рекламу **бесплатных игр** или приложений в социальной сети TikTok, для установки которых необходимо зайти в предоставленный мошенником аккаунт Apple. Потерпевшими в таких случаях выступают подростки, являющиеся активными пользователями указанной социальной сети, наиболее уязвимая категория граждан.

Также остается актуальным предлог о **трудоустройстве**, для чего злоумышленники предоставляют соискателю для входа якобы корпоративный аккаунт Apple.

2. Связаны с **угрозой распространения личной информации потерпевших либо иных сведений, которые последние желали сохранить в тайне**, преимущественно – фотографий и видеозаписей интимного характера, а также иные личные сведения, которые в большинстве случаев потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером для знакомства противоположного пола.

3. Связаны с **угрозой применения насилия**. В данных случаях угроза поступала после того, как потерпевшие пытались дозвониться (либо вели переписку) по абонентским номерам, указанным в анкетах девушек, размещенных на интернет-ресурсах по оказанию сексуальных услуг.

ВЫМОГАТЕЛЬСТВА, СОПРЯЖЕННЫЕ С БЛОКИРОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ APPLE

Прежде всего следует отметить, что механизм блокирования мобильных устройств Apple потерпевших реализуется не путем взлома операционной системы iOS (iPadOS, macOS, watchOS – в зависимости от устройств), а посредством методов социальной инженерии с использованием доверчивости граждан.

Примечание: в дальнейшем для понятности в качестве устройства будет говориться о мобильном телефоне iPhone. Но данная схема актуальна для любого устройства Apple: Mac Book, iPad и др.

Так, злоумышленники под различными благовидным предлогами вынуждают собеседника выйти из своего аккаунта Apple (iCloud) и войти на iPhone в мошеннический аккаунт, для чего предоставляют логин (адрес электронного почтового ящика) и пароль. С этого момента мобильный телефон жертвы «в руках» вымогателя. Он изменяет пароль от учетной записи, знание которого требуется для выхода из нее, после чего удаленно через облачный сервис iCloud активирует функцию «Найти iPhone», переводя таким образом устройство в режим пропажи, и полностью блокирует его.

Далее потерпевшему приходит сообщение (либо выводится на заблокированном экране), что телефон заблокирован, а для его разблокировки необходимо заплатить деньги. Также зачастую предоставляется контакт в Telegram лица, способного решить этот вопрос (как правило, это и есть злоумышленник, заблокировавший телефон). Характерно, что даже при выполнении требования вымогателя, разблокировка устройства в подавляющем большинстве случаев не осуществляется.

Существует несколько основных предлогов, вынуждающих потерпевших войти на своих устройствах в мошеннический аккаунт Apple.

Предлог 1. Реклама бесплатных игр и приложений в социальных сетях и мессенджерах.

Злоумышленники осуществляют размещение рекламы (чаще всего видеоролик в TikTok либо в Telegram), в которой указывается бесплатный способ скачать на iPhone то или иное приложение (AyuGram, Telegram Premium, позволяющие читать удаленные сообщения, забирать «звезды»,

скрывать статус «онлайн» и т.д.), игру («PUBG Mobile», «Standoff2» и др.) либо мод, получить на свой баланс игровую валюту.

Для установки данных приложений злоумышленники предлагают жертве войти на телефоне в предоставленный ими аккаунт Apple (iCloud). Потерпевшими в таких случаях выступают подростки, являющиеся активными пользователями социальных сетей – наиболее уязвимая категория граждан.

Предлог 2. «Сломался телефон». Оказание помощи с файлами из облачного хранилища iCloud.

В данном случае первоначальная коммуникация злоумышленника и жертвы происходит в приложениях либо сайтах для знакомств (Mamba, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица противоположного пола, желающего познакомиться. Затем «новый знакомый» переводит общение в мессенджер, где под различными предлогами (например, сломался телефон и необходимо очень срочно скачать какие-либо файлы: курсовую работу или иные важные документы) вынуждает потерпевшего зайти в чужую учетную запись Apple на своем iPhone. При этом для большей убедительности присылает заранее заготовленные фотографии разбитого телефона, голосовые сообщения и видеозаписи.

Получив согласие, злоумышленник высылает логин и пароль, а после входа потерпевшего в учетную запись, меняет пароль и включает режим пропажи.

Предлог 3. Трудоустройство.

Злоумышленник осуществляет размещение рекламы в сети Интернет о поиск сотрудника на вакансию, как правило, связанную с тестированием мобильных приложений для устройств Apple. После удачного «прохождения собеседования» жертве предоставляется логин и пароль для входа в якобы корпоративный аккаунт Apple, который должен использоваться для работы либо загрузки необходимых приложений.

После входа соискателя на своем iPhone в предоставленную учетную запись Apple, он оказывается в ловушке. Затем происходят события, аналогичные описанным выше.

Предлог 4. Переход по фишинговой ссылке.

В некоторых случаях «интернет-знакомый» вместо убеждения жертвы войти на своем телефоне в мошеннический аккаунт Apple, может сбросить ссылку для скачивания приложения либо входа в облачное хранилище iCloud, где будет предложено ввести логин и пароль от учетной записи Apple уже со стороны потерпевшего. Данная ссылка будет являться фишинговой (поддельной). Введя авторизационные данные своей учетной

записи, они сразу же станут известны вымогателю. После смены пароля последний не только заблокирует устройство жертвы, но и получит доступ к его личным данным (фотографии, файлы, заметки, геопозиция, почта и др.), которые синхронизированы в облачном хранилище.

ВАЖНО!

Работники сервисных центров не оказывают услуги по восстановлению устройств Apple либо учетных записей iCloud, заблокированных мошенниками. Разблокировать такое устройство возможно только путем обращения в службу технической поддержки компании Apple, приложив документы, подтверждающие законность его приобретения.

Для этого потерпевший должен обратиться в службу поддержки Apple посредством сервиса Request Activation Lock Support [https://al-support.apple.com/#/al/agreement] и предоставить:

IMEI устройства;

доказательства покупки устройства (чек, коробка с IMEI, гарантийный талон);

доказательства его «легального» использования потерпевшим (учетная запись Apple потерпевшего, привязанные банковские платежные карточки, телефонные номера и почтовые ящики);

обстоятельства противоправного входа (путем введения в заблуждение) в мошеннический Apple ID.

Процесс восстановления через службу поддержки занимает от нескольких дней до недели, при этом устройство может быть сброшено до заводских настроек (все данные удалятся).

Запомните! Настройки iPhone не для игр!

1. никогда и не под каким предлогом не входите на своем мобильном устройстве в чужую учетную запись Apple, даже если вас об этом просит друг и тем более – незнакомый человек из интернета;
2. никому не сообщайте ваши логин и пароль от аккаунта Apple;
3. не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком;
4. не вводите на посторонних сайтах свои логин и пароль от аккаунта Apple iCloud.

! Совет родителям, чьи дети используют мобильные устройства Apple.

Для того, чтобы ваш ребенок не смог осуществить ввод логина и пароля предоставленных злоумышленником, достаточно установить родительский контроль. Он никак не ограничивает действия ребенка в функционале мобильного устройства, лишь запрещает выйти из учетной записи Apple, а также воспользоваться платежными средствами.

ВЫМОГАТЕЛЬСТВА, СВЯЗАННЫЕ С УГРОЗОЙ РАСПРОСТРАНЕНИЯ ЛИЧНОЙ ИНФОРМАЦИИ ПОТЕРПЕВШИХ ЛИБО ИНЫХ СВЕДЕНИЙ, КОТОРЫЕ ПОСЛЕДНИЕ ЖЕЛАЛИ СОХРАНИТЬ В ТАЙНЕ

При данном виде вымогательств в подавляющем большинстве случаев объектом преступления являются фотографии и видеозаписи интимного характера потерпевшего, переписка на сексуальную тему либо иная компрометирующая информация.

Первоначальная коммуникация злоумышленника и жертвы происходит в приложениях либо сайтах для знакомств (Mamba, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица, противоположного пола, желающего познакомиться. Затем общение довольно быстро приобретает сексуальный подтекст. «Новый знакомый» предлагает обменяться интимными фотографиями. При этом для большей убедительности присылает заранее заготовленные якобы свои фотографии либо видео в обнаженном виде.

В случае, если жертва «повелась» на данное предложение и сбросила свои интимные фотографии или видео, злоумышленник их сохраняет. При этом отправление самоуничтожающихся сообщений не поможет, так как экран всегда можно сфотографировать другим устройством. Одновременно с этим вымогатель собирает информацию о жертве в сети Интернет: находит страницы в социальных сетях, анализирует данные из открытых источников, узнает круг друзей и родственников, место работы. Затем злоумышленник сообщает, что распространит имеющиеся у него интимные фотографии потерпевшего среди его друзей и знакомых либо выложит их в открытый доступ, если ему не заплатать за их нераспространение.

Если же в ходе интернет-переписки вымогателю не удалось получить интимные изображения жертвы, он может изготовить их с помощью различных фоторедакторов, используя фотографии собеседника из его социальных сетей. Также злоумышленник может угрожать оглаской состоявшейся переписки на сексуальные темы, дополнительно сообщив, что является несовершеннолетним, таким образом намекая о возможности привлечения жертвы за «совращение малолетнего».

В некоторых случаях «интернет-знакомый» может сбросить фишинговую ссылку, например, для просмотра фото в облачном хранилище либо его видео на различных стриминговых сервисах. Перейдя по ссылке и введя свои данные (как правило, абонентский номер и полученный код-подтверждение) злоумышленник получает доступ к мессенджеру жертвы и его социальным сетям. В таком случае вымогатель получает доступ ко всем контактам и перепискам потерпевшего, а при

наличии в них интимных фото или видео (например, при общении с другими девушками) либо иной компрометирующей информации, использует ее по вышеописанному принципу. В данном случае ситуация усугубляется тем, что злоумышленник видит все реальные контакты жертвы, а также может использовать ее личные учетные записи для совершения иных мошеннических действий (просить одолжить деньги, перевести средства на благотворительный сбор и т.д.).

! Рекомендации:

1. никогда не отправляйте свои интимные фотографии и видео незнакомцам из интернета;
2. не оставляйте в сети Интернет о себе личную информацию и не делитесь с ней с незнакомцами;
3. скройте данные о себе в настройках конфиденциальности в социальных сетях и мессенджерах;
4. не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком;
5. не вводите на посторонних сайтах свои личные данные и коды из сообщений.

ТАКЖЕ СЛЕДУЕТ ПОМНИТЬ, что изготовление и распространение порнографических материалов или предметов порнографического характера влечет за собой привлечение к уголовной ответственности по ст.343 Уголовного кодекса Республики Беларусь с применением наказания вплоть до двух лет лишения свободы.

ВЫМОГАТЕЛЬСТВА, СВЯЗАННЫЕ СУГРОЗОЙ ПРИМЕНЕНИЯ НАСИЛИЯ, ПОСЛЕ ПОСЕЩЕНИЯ САЙТОВ ПО ОКАЗАНИЮ СЕКСУАЛЬНЫХ УСЛУГ

Злоумышленники на различных сайтах по оказанию сексуальных услуг размещают анкеты девушек, в которых зачастую в качестве контактного указывают абонентский номер белорусского оператора мобильной связи.

Потерпевшие, находясь в поисках подобных услуг, безрезультатно пытаются дозвониться по указанному в анкете абонентскому номеру (трубку никто не снимает).

В последующем, как правило на следующий день, потерпевшим поступает телефонный звонок, в ходе которого лицо с выраженным кавказским акцентом в голосе сообщает, что по причине звонка произошло «блокирование» (либо иные причины), ввиду чего «девушки не могут работать». В ходе звонка злоумышленник предлагает решить вопрос «тихо-мирно», пополнив баланс, тем самым ее разблокировать.

В дальнейшем происходит давление в сторону жертвы и склонение к переводу все больших сумм денежных средств под различными предлогами, в том числе высказываются угрозы жизни и здоровью потерпевшего либо его близких родственников.

В последующем общение переводится в мессенджер, куда сбрасываются реквизиты, на которые необходимо перечислить денежные средств (как правило, p2p переводы). Туда же потерпевшие сбрасывают электронные чеки как подтверждение о переводе денежных средств.

В некоторых случаях на звонки или сообщения потерпевших при посещении интернет-сайтов отвечает якобы девушка и договаривается о встрече, для чего требует предоплаты в качестве гарантии. В действительности никакой девушки не существует, а злоумышленники просто имитируют женский голос. После совершения данной мошеннической схемы также следуют звонки по вышеописанному принципу.

СЛЕДУЕТ ПОМНИТЬ! Реклама услуг сексуального характера в Республике Беларусь запрещена. Отказ от подобного досуга не только убережет ваше здоровье, но и деньги.

ВЫМОГАТЕЛЬСТВА, СВЯЗАНЫЕ С ШИФРОВАНИЕМ ФАЙЛОВОЙ СИСТЕМЫ НА СЕРВЕРАХ ПРЕДПРИЯТИЙ

Мошенническая схема шифрования файлов на серверах предприятий, известная как атака с использованием программ вымогателей (шифровальщиков), является одной из наиболее опасных киберугроз для бизнеса. Злоумышленники проникают в сеть, чтобы зашифровать критически важные данные и потребовать выкуп за их восстановление.

Как происходит **атака**? Современные атаки шифровальщиков – это не автоматический вирус, а хорошо спланированная операция, управляемая людьми. Ее можно разделить на несколько **этапов**:

1. Проникновение в сеть. Начальный доступ злоумышленники получают различными способами:

фишинг: массовые или целевые рассылки писем сотрудникам.

Например, письмо может маскироваться под накладную от «1С:Предприятие» с вложенным архивом, внутри которого находится вредоносный файл;

атака на удаленный доступ: взлом слабозащищенных точек входа, таких как RDP (протокол удаленного рабочего стола), VPN или серверы с уязвимостями;

использование легитимного ПО: злоумышленники могут применять легальные программы для мониторинга (например, Mipko Employee

Monitor), чтобы оставаться незамеченными и изучать активность сотрудников, перехватывать нажатия клавиш и буфер обмена.

2. Закрепление и разведка. Попав внутрь, злоумышленники не начинают шифрование сразу. Они изучают сеть, ищут ценные данные, повышают свои привилегии, получают доступ к контроллерам домена и, что самое важное, находят и стараются вывести из строя резервные копии. Этот этап может длиться неделями.

3. Подготовка к финальной атаке. Перед запуском шифровальщика преступники часто крадут конфиденциальные данные. Это делается для двойного шантажа: они угрожают не только навсегда заблокировать файлы, но и опубликовать украденную информацию в Интернете.

4. Запуск шифрования. В назначенный момент на всех ключевых серверах и рабочих станциях запускается вредоносная программа. Она начинает массово шифровать документы (Office, PDF, базы данных, исходный код и т.д.), часто переименовывая их и оставляя в каждой папке файл с требованием выкупа. Современные шифровальщики также уничтожают теневые копии томов (VSS) и отключают средства восстановления системы, чтобы у жертвы не осталось простых путей отката.

Как защититься от шифровальщиков? Защита должна быть многоуровневой и строиться на принципе («доверяй, но проверяй», а также на готовности к тому, что атака может произойти в любой момент.

Технические меры защиты инфраструктуры:

✓ Неприкасаемые резервные копии (правило 3-2-1). Это самый главный пункт. У вас должно быть как минимум три копии данных, на двух разных носителях, и одна копия обязательно должна храниться вне основной инфраструктуры (офлайн), чтобы злоумышленники не могли до нее добраться. В облачных средах стоит использовать неизменяемые (immutable) резервные копии, которые нельзя изменить или удалить даже при компрометации учетной записи администратора.

✓ Принцип минимальных привилегий. У сотрудников должен быть доступ ровно к тем данным, которые необходимы для работы, и не больше. Административные учетные записи должны использоваться только для выполнения конкретных задач.

✓ Многофакторная аутентификация (MFA). Обязательно включите NIFA везде, где это возможно: для доступа к почте, VPN, облачным сервисам и, конечно, к консолям администрирования серверов.

✓ Сегментация сети. Критически важные серверы (файловые, резервного копирования, базы данных) должны находиться в отдельных виртуальных сетях (VLAN) с жесткими правилами доступа. Это не даст атаке с зараженного компьютера бухгалтера быстро перекинуться на все хранилища.

✓ Обновление ПО и политики запуска. Своевременно устанавливайте обновления безопасности. Используйте белые списки приложений (AppLocker, WDAC), чтобы запретить запуск неподписанных или неразрешенных программ, включая неизвестные шифровальщики.

! ЧТО НЕ НАДО ДЕЛАТЬ РАБОТНИКАМ ПРЕДПРИЯТИЙ? ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ.

Самая совершенная защита может рухнуть из-за одной ошибки сотрудника. Поэтому персоналу **категорически нельзя:**

- переходить по подозрительным ссылкам и открывать вложения в письмах от незнакомцев, даже если они выглядят как документы от контрагентов или госорганов;
- использовать слабые пароли (типа «password123», «Qwerty» или «1С») и записывать их на стикерах, приклеенных к монитору;
- подключать к рабочим компьютерам личные или найденные USB-накопители, которые могут быть заражены;
- игнорировать необычное поведение компьютера (резкое замедление, невозможность открыть файлы, появление странных файлов с требованием выкупа). В такой ситуации нужно немедленно отключить компьютер от сети и сообщить в IT-отдел;
- передавать логины и пароли коллегам по телефону или в мессенджерах.

! ЧТО ДЕЛАТЬ, ЕСЛИ ФАЙЛЫ УЖЕ ЗАШИФРОВАНЫ?

Если беда все-таки случилась, главное правило – не паниковать и не платить выкуп. Платеж не гарантирует возврат данных и лишь финансирует дальнейшие атаки преступников.

План действий должен выглядеть следующим образом:

1. Изолировать зараженные системы. Немедленно отключите зараженные компьютеры и серверы от сети (физически выдерните сетевой кабель). Это может остановить распространение шифрования на другие устройства;
2. Сообщить о проблеме. Немедленно уведомите руководство и отдел информационной безопасности. Если в компании есть регламент по реагированию на инциденты, следуйте ему.
3. Оценить ущерб и начать восстановление. Вместе со специалистами определите, какие системы затронуты. Если у вас есть чистые, не затронутые атакой резервные копии, можно начинать процесс восстановления. Для этого потребуется полностью переустановить ОС на зараженных машинах и только после этого восстанавливать данные.
4. Обратиться в милицию. Это не просто рекомендация, а важный шаг для официальной фиксации преступления. Представитель компании (руководитель или ответственный за информационную безопасность)

должен написать заявление. Необходимо предоставить любые материалы, которые могут помочь расследованию: переписку с вымогателями (если она была), IP-адреса, образцы зашифрованных файлов (для последующей передачи экспертам) и файлов с требованиями.

СЛЕДУЕТ ПОМНИТЬ! Атаки шифровальщиков – это вопрос не «если», а «когда». Поэтому ключ к информационной безопасности предприятия – надежные изолированные бэкапы, обученные сотрудники и отработанный план действий на случай инцидента.

Сваттинг
(заведомо ложное сообщение об опасности)

Сваттинг – заведомо ложный вызов милиции, аварийно-спасательных служб путем фальшивых сообщений о минировании, убийствах, захвате заложников и т.п. от имени другого лица.

Этот термин происходит от названия штурмовой группы «SWAT» (Special weapons and tactics) – специализированной полицейской единицы в США и многих других странах. Если есть угроза, при которой необходимо вмешательство этой единицы, последствиями иногда становится эвакуация учреждений образования, административных учреждений, крупных торговых объектов. В западных странах «сваттинг» расценивается как разновидность терроризма, поскольку его используют для запугивания и создания риска получения телесных повреждений или даже смерти.

Сваттинг в первую очередь свойственен среде, где люди (чаще всего молодые) объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о заминировании какого-либо объекта.

В последние годы сваттинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Жертвами хулиганов становятся как обычные люди, так и знаменитости.

В Республике Беларусь за последние пять лет возросло количество случаев поступления сообщений на электронную почту о ложном минировании объектов. Подобные «шалости» дорого обходятся государству, а для виновных чреваты весьма нешуточными последствиями.

За совершение указанных действий грозит наказания в виде лишения свободы сроком до пяти лет, а в случае повторного совершения, либо группой лиц по предварительному сговору, либо повлекшее причинение

ущерба в крупном размере, либо повлекшее иные тяжкие последствия, до семи лет лишения свободы.

Незаконный оборот платежных инструментов, средств платежа и их реквизитов

В 2022-2024 году (реже в настоящее время) чаще в молодежной среде, отмечался рост количества преступлений, связанных с продажей реквизитов платежных инструментов (банковских платежных карт, логинов и паролей к системе дистанционного банковского обслуживания).

Организаторами преступных групп, совершающими киберпреступления, все активнее в противоправную деятельность вовлекается молодежь, для совершения действий, предусмотренных статьей 222 Уголовного кодекса Республики Беларусь (незаконный оборот платежных инструментов, средств платежа и их реквизитов).

Зачастую подростки находят объявления в Интернете (мессенджерах), где им предлагают оформить на свое имя банковскую карту и продать ее реквизиты, тем самым предоставив доступ к банковским счетам, «привязанным» к карте, либо электронным кошелькам (как правило «заработок» за такие действия составляет от 50 рублей за реквизиты одной БПК). В дальнейшем, реквизиты этих платежных инструментов используются при совершении преступных сделок.

Вступившим в силу Законом Республики Беларусь от 17 февраля 2025 г. №61-З «Об изменении кодексов по вопросам уголовной ответственности» дифференцируется ответственность за незаконный оборот платежных инструментов (ст. 222 УК РБ и ст. 12.35 КоАП). Так, за распространение чужих (находящихся в незаконном владении) реквизитов банковских платежных карточек сохраняется уголовная ответственность. Такие же действия в отношении собственных (находящихся в законном владении) реквизитов банковских платежных карточек будут влечь административную ответственность.

Операции с криптовалютой

Беларусь развивающаяся страна и граждане активнее пользуются цифровыми технологиями.

Порядок осуществления сделок с криптовалютой в настоящее время определен Указом Президента Республики Беларусь от 17 сентября 2024 г. №367 «Об обращении цифровых знаков (токенов)» (далее – Указ №367).

Указом №367 установлена обязанность для физических лиц совершать операции по покупке-продаже криптовалюты за денежные

средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий, а также перечислять (переводить) денежные средства со своих банковских счетов, электронных кошельков исключительно указанным резидентам ПВТ. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается.

Указ №367 не вводит запрет в отношении операций по переводу криптовалюты на зарубежные торговые площадки и не ограничивает возможность использования физическими лицами таких площадок для совершения операций обмена (например, обмен криптовалюты одного вида на криптовалюту другого вида, торги криптовалютой), не связанных с непосредственным вводом или выводом денежных средств.

Таким образом, в настоящее время в Беларуси действуют следующие нормы:

Разрешено покупать токены (криптовалюту) за денежные средства только на белорусских криптобиржах, являющихся резидентами Парка высоких технологий; обменивать токены на другие токены на любых криптоплатформах без ограничений, например, обменивать Bitcoin на Ethereum.

Запрещено покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах.

УПК КМ ГУВД Мингорисполкома