Следственный комитет Республики Беларусь
Управление по г. Минску
Ленинский районный отдел
ул. Физкультурная, 31
220028, г. Минск
тел.: (017) 369-05-87
факс: (017) 369-05-86
03.04.2023 № 2/15-2443

Администрацию Ленинского района г. Минска, учреждения здравоохранения, организации и предприятия Ленинского района г. Минска
(согласно списку рассылки)

Об отдельных вопросах противодействия преступлениям, совершаемым с использованием возможностей глобальной сети Интернет и преступлениям против собственности

В современном мире наблюдается активное внедрение и совершенствование электронных информационных систем, а также автоматизация множества процессов. В настоящее время сложно выделить сферу общественной деятельности, в которой бы не применялись информационные технологии.

Внедрение современных технологий в различные сферы происходит непрерывно. Процессы информатизации, направленные на улучшение качества жизни, приобрели глобальный характер. На необходимость активного использования информационных технологий во всех сферах жизнедеятельности общества обращает внимание и Глава государства.

На протяжении последних шести лет фиксируется существенный рост преступлений в сфере высоких технологий, в том числе связанных с хищением денежных средств посредством использования возможностей глобальной компьютерной сети Интернет, а также информационно-коммуникационных технологий.

Справочно: в 2022 году следственными подразделениями столицы возбуждено 5 380 уголовных дел о преступлениях в сфере высоких технологий. Территориальным подразделением Следственного комитета Ленинского района г. Минска за 2022-2023 года возбуждено более 750 уголовных дел данной категории. Результаты показали, что большинство противоправных деяний совершается путем использования социальной инженерии: «вишинг» и «фишинг» (более 91% от общего количества возбужденных уголовных дел).

Увеличение количества преступлений в IT-сфере происходит наряду с ростом количества абонентов сети Интернет, доли населения, использующей информационные технологии при проведении финансовых операций.

Интернет-банкинг и платежные сервисы постепенно завоевывают статус основных платформ для заказа банковских и иных услуг, осуществления денежных переводов и управления расчетными счетами. Для доступа к системе виртуального банкинга и платежным сервисам

Администрация Ленинского района г. Минска
ПОСТУПИЛО
«03» 04 2023
Входящий № Г93

клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте учреждения.

Справочно: в настоящее время более 85 % населения пользуется интернетом, а согласно аналитическим данным Национального банка в настоящее время число банковских платежных карт, находящихся в обращении в Республике Беларусь, превышает 15,2 млн. Доля безналичных операций в 2022 году составила 63,8 % от всех совершенных платежей в белорусских рублях.

Современные методы оплаты в глобальной компьютерной сети Интернет позволяют совершать платежи путем введения в компьютерную систему сведений о банковской платежной карте (далее – БПК): номере, сроке действия, владельце, коде безопасности – CVC (как правило, трехзначный код на оборотной стороне карты), данных из sms-сообщений, а при завладении персональными данными клиента (ФИО, идентификационный номер паспорта и др.) – позволяют открывать и использовать счета в платежных сервисах с использованием межбанковской системы идентификации.

Механизмы завладения указанной информацией и совершения хищений денежных средств со счетов клиентов платежных сервисов и банковских учреждений разнообразны.

Данные обстоятельства позволяют злоумышленникам, обладая необходимой электронно-цифровой информацией, совершать платежи в сети Интернет и пользоваться счетами без ведома их владельцев.

В настоящее время можно выделить следующие основные методы социальной инженерии, используемые злоумышленниками для совершения противоправных действий:

«вишинг» (осуществление звонков под видом сотрудников банков, правоохранительных органов и других учреждений, организаций). Как правило, злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, а также осуществляет звонки с использованием различных мессенджеров.

«фишинг» – несанкционированный доступ к конфиденциальной информации с использованием подменных Интернет-ресурсов (максимально схожего по внешним признакам и доменному имени с оригиналом) где необходимо ввести личные данные, либо путем интернет/смс-рассылки, содержащей вредоносное программное обеспечение.

Успех вышеуказанных методов напрямую зависит от способности злоумышленников манипулировать человеческими чувствами (страхом, любопытством, симпатией, тщеславием и жадностью). Рассматриваемые преступления совершаются, как правило, в составе групп, участники которых, зачастую, лично не знакомы друг с другом.

Анализ деятельности злоумышленников на территории Республики Беларусь показал, что в период с 2022 по 2023 год идет рост противоправных деяний в IT-сфере совершаемых с использованием фишинговых ссылок, а также увеличилось количество преступлений по сравнению с прошлым годом, когда потерпевшие отзывались на «уловки» преступников и, будучи обманутыми, сами осуществляли переводы денежных средств на счета с реквизитами, указанными злоумышленниками.

Наиболее часто злоумышленниками использовались фишинговые ссылки со следующими доменными именами: «kufar.dostavka-by.com», «kufar.by-transfer.ca», «kufar.by-getdostavka.com», «kufar.items-by.com», «autolight.order-by.com», «kufar.by-ordering.com», «evropochta.by-c.ca», «wwv-kufar.by» и «evropocgta.deliver-by.online» с использованием которых совершено более 450 преступлений.

Следует отметить, что все чаще жертвами киберпреступников становятся граждане в возрасте от 16 до 35 лет, что прежде всего обусловлено увеличением количества преступлений в IT-сфере, предусмотренных ст. 209 УК (на 45 % больше по сравнению с аналогичным периодом прошлого года), когда потерпевшие сами осуществляли переводы денежных средств на счета с реквизитами, указанными злоумышленниками.

При совершении указанных преступлений злоумышленники создают поддельные интернет-магазины, учетные записи различных торговых марок в мессенджерах и социальных сетях (Instagram, Telegram и др.), в которых размещаются объявления о продаже (покупки) какого-либо имущества, пользующегося спросом и т.д., и выставляется цена, как правило, ниже рыночной. В настоящее время для совершения противоправных действий также стал активно использоваться раздел Интернет-сайта «Onliner.by», посвященный сдаче жилья в аренду, а именно злоумышленники размещают объявления о сдаче квартиры по заниженной стоимости. После того как граждане откликаются на объявления злоумышленники осуществляют с ними общение с использованием глобальной компьютерной сети Интернет (социальных сетей и мессенджеров), в ходе чего предлагают различными способами произвести оплату (предоплату).

Справочно: злоумышленники стали активно использовать поддельные учетные записи в социальной сети «Instagram», при этом в большинстве случаев используются поддельные-аккаунты различных брендов с большим количеством подписчиков (от 30 тысяч человек).

К примеру, в социальной сети «Instagram» и мессенджерах злоумышленники создавали учетные записи (cocon.belarus, mebli.belarus, mebel_interest и другие), с помощью которых «якобы» изготавливали и продавали садовую мебель. В ходе общения с которыми посредством глобальной компьютерной сети Интернет и обсуждения товара, условий

и сроков его изготовления, гражданам предлагалась произвести оплату товара (его часть) на банковские платежные карты Республики Беларусь используемые злоумышленниками, что последние и делали. Затем злоумышленники переставали выходить на связь, а денежные средства сразу же переводили на иные расчетные счета, подконтрольные злоумышленникам.

Злоумышленниками наиболее часто создавались и использовались следующие учетные записи (аккаунты) в «Instagram»: «firbir_shop_ru», «room_dream», «Zona_est.2020», «euphoria.women.bq», «raspiv_parfum_by», «queen.shop_pol», «romashka_showroom.bel», «guanto_mens_fashion», «dreamroom_ru», «soffi__boutique» и другие.

Также с четвертого квартала 2022 года в несколько раз возросло количество преступлений, связанных с поддельными сайтами. Так, граждане (потерпевшие) с целью оплаты различных услуг (коммунальные платежи, оплата услуг различных организаций и т.д.) в поисковой строке Интернет-браузера вводят запрос для осуществления перехода в свой личный кабинет системы дистанционного банковского обслуживания. При этом переходят по первой попавшейся ссылке (фишинговой) и в открывшемся окне вводят необходимую информацию для осуществления доступа к своему личному кабинету, тем самым предоставляют идентификационные данные и доступ к нему злоумышленнику. После этого с банковских счетов граждан похищаются денежные средства.

Также в производстве Ленинского (г. Минска) районного отдела Следственного комитета в 2022-2023 гг. **находилось более 100 уголовных дел, возбужденных по фактам завладения имуществом путем обмана или злоупотребления доверием, – по так называемым фактам «телефонных мошенничеств».** Потерпевшими от преступных действий мошенников по вышеуказанной схеме стали более 111 граждан, проживающих на территории Ленинского района г. Минска.

Зачастую потерпевшими по уголовным делам признаются лица пенсионного возраста, а также престарелые лица.

Сценарии обмана могут быть разными, суть одна: звонок с незнакомого номера, экстренная ситуация и просьба передать курьеру крупную сумму денег.

Телефонные звонки поступают от неизвестных лиц посредством телефонной связи по мобильному либо стационарному телефону пожилым гражданам и гражданам преклонного возраста, в ходе которых мошенники рассказывают о **якобы** серьезной аварии, в которой «виноват» их близкий родственник, а чтобы «решить вопрос» необходимо уплатить крупную сумму денег.

Доверительная манера говорить, четкие инструкции, поступающие от преступника, для убедительности в трубке раздаются всхлипы

виновника дорожно-транспортного происшествия (далее – ДТП). В итоге финансовые потери несут лица, которым звонят.

Основная преступная схема следующая: человеку (потерпевшему) поступает звонок по мобильному либо стационарному телефону, невнятным расстроенным голосом собеседник представляется родственником (супругой, дочерью, внучкой, племянником и т.д.) или знакомым и говорит, что по его вине произошло ДТП, в результате которого пострадал другой человек. Также звонивший сообщает, что если в кратчайшие сроки не будут переданы деньги на лечение пострадавшего, то будет возбуждено уголовное дело.

Если потерпевший говорит, что не узнает по голосу родственника, мошенники отвечают, что получили травму в ДТП (разбиты губы, выбиты зубы и т. д.), что затрудняет речь. В некоторых случаях в разговор включается **якобы сотрудник правоохранительных органов**, который подтверждает совершение ДТП с тяжкими последствиями. Он же указывает сумму, которую необходимо передать, чтобы избежать привлечения к уголовной ответственности. Как правило, требуют 50000 рублей, иногда суммы достигают 10000-50000 долларов, а если потерпевший сообщает, что такими средствами не располагает, тогда спрашивают какие есть и убеждают передать все имеющиеся денежные средства.

Мошенники в ходе разговора создают для потерпевших стрессовую ситуацию, поддерживают постоянный контакт, лишая возможности посоветоваться с кем-либо, и, находясь в таком состоянии, граждане не обращают внимания на то, что им звонят с номеров другой страны.

Для того, чтобы быть **более убедительными, мошенники диктуют потерпевшим текст заявления в милицию или Следственный комитет о прекращении уголовного преследования, предлагают передать родственнику в больницу личные вещи и постельные принадлежности.**

Мошенники долго находятся на связи с потерпевшими – вплоть до момента передачи денег, перезванивают с городского телефона на мобильный и продолжают разговор, препятствуя связи потерпевшего с третьими лицами (в отдельных случаях, мошенники общались с потерпевшими более 2 часов). После того как потерпевший соглашается передать деньги, ему указывают алгоритм действий. Чаще всего к потерпевшему приезжает курьер, в редких случаях предлагают перевести деньги на счет в банке или на карту.

Для того, чтобы обезопасить себя и свои денежные средства от подобных действий мошенников, необходимо:

• Не поддаваться эмоциям и не терять бдительности, если вам позвонили с незнакомого номера телефона и рассказывают, что с вашим

близким случилась беда – **положите трубку и перезвоните родственнику**! Прежде всего, уточните, так ли это.

• Сообщите о звонке в милицию.

• Не доверяйте незнакомцам по телефону и не соглашайтесь на сомнительные сделки по передаче денег!

На основании вышеизложенного, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 № 403-З «О Следственном комитете Республики Беларусь», в целях противодействия киберпреступности, а также преступлениям против собственности, повышения уровня правовой осведомленности, защиты прав и законных интересов граждан, организаций (предприятий), государственных и общественных интересов, прошу:

рассмотреть информационное письмо с участием заинтересованных лиц, при необходимости с участием представителя Ленинского (г. Минска) РОСК, с целью предотвращения (предупреждения) совершения преступлений в отношении сотрудников (работников) и членов их семей, рекомендовав принимать дополнительные меры по осуществлению безопасности при работе в глобальной компьютерной сети Интернет, а также принимать дополнительные меры по безопасному использованию банковских продуктов;

на системной основе информировать сотрудников (работников), посетителей, граждан и клиентов, а также лиц пенсионного и престарелого возраста, о проявлении осторожности и бдительности, соблюдении установленных правил безопасности пользования персональными БПК, а также о порядке действий в случае поступления им звонков от мошенников;

рассмотреть вопрос о размещении на информационных стендах в учреждениях (организациях) профилактических листовок (прилагаются).

Копию настоящего письма направить руководителям подведомственных организаций для сведения и реализации изложенных предложений.

О принятых мерах прошу уведомить ленинский (г. Минска) районный отдел Следственного комитета в месячный срок.

Приложение: на 6 листах.

Заместитель начальника А.С.Суворов

ВНИМАНИЕ!

Сотни граждан Республики Беларусь стали жертвами телефонных мошенников в 2022 году.
Каждый пострадавший лишился от 1000 до 50 000$.

Сценарии обмана могут быть разными, суть одна: звонок с незнакомого номера, экстренная ситуация и просьба передать курьеру крупную сумму денег.

Не доверяйте голосу в телефоне!
Не дайте себя обмануть!

ПРАВИЛЬНЫЕ ДЕЙСТВИЯ:

1. **Положите трубку;**
2. **Перезвоните родственнику и уточните, всё ли с ним в порядке;**
3. **Сообщите о звонке в милицию по телефону 102.**

Не станьте жертвой мошенников

незнакомого номера Вам звонит родственник и сообщает, что попал в жуткое ДТП и ему грозит тюрьма или он находится в больнице. Потом трубку берет якобы следователь и говорит, что срочно нужны деньги, чтобы откупиться или оплатить дорогостоящее лечение.
Не доверяйте голосу по телефону!

Ваши действия:

1. Положите трубку;

2. Перезвоните родственнику и уточните, все ли с ним в порядке;

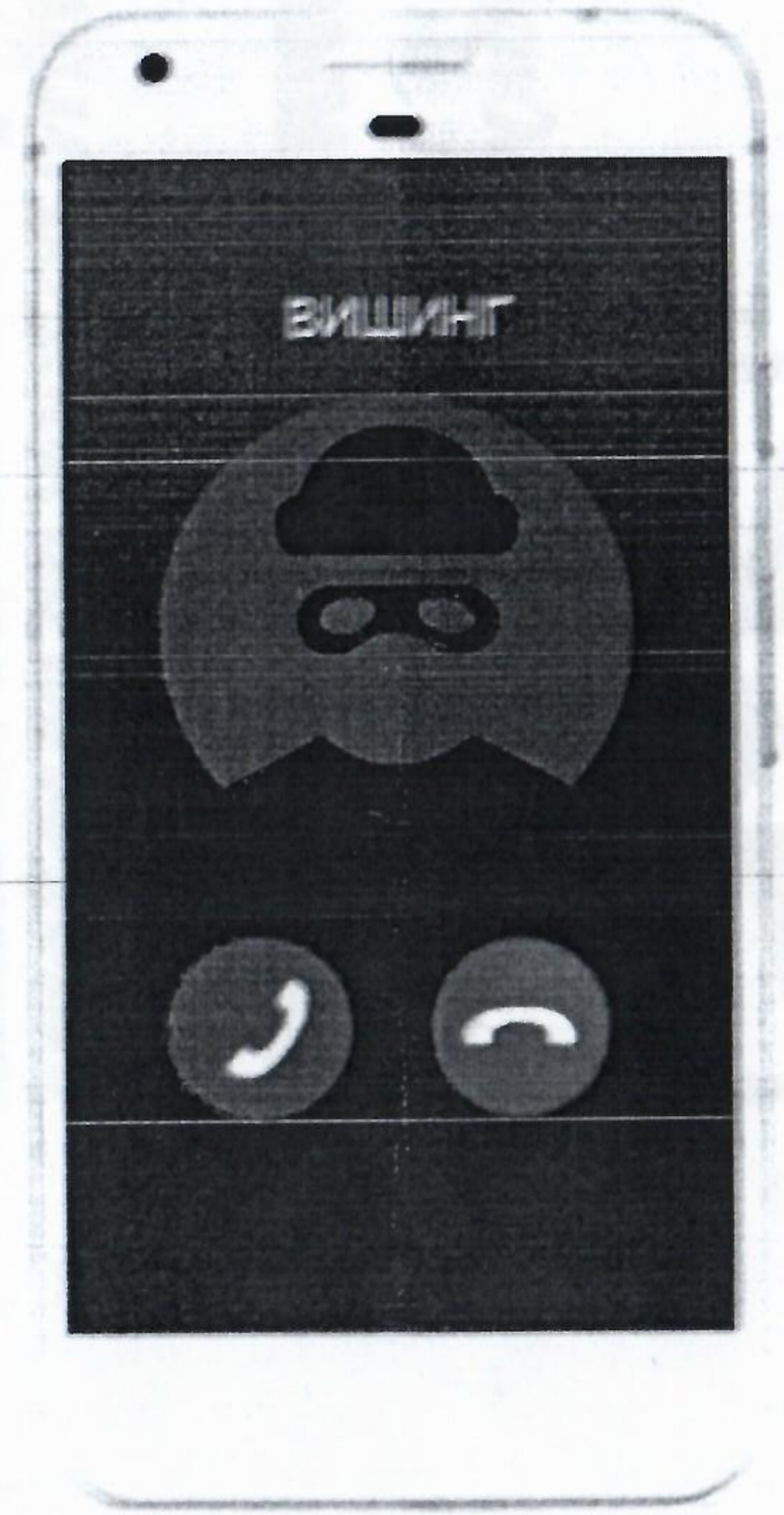
3. Сообщите о звонке в милицию.

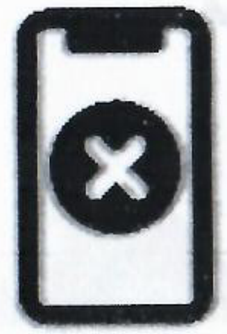
Не дайте себя обмануть!

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ сообщай неизвестным лицам свои персональные данные





НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ переводи деньги незнакомым людям в качестве предоплаты

МОШЕННИК: КАК ЭТО РАБОТАЕТ?

- общение с продавцом ведет в интернет-мессенджере, а не на сайте торговой площадки
- в процессе общения изъявляет желание приобрести товар по предоплате или оформить доставку
- пишет с номеров, не зарегистрированных в Республике Беларусь
- высылает поддельную (фишинговую) ссылку для получения якобы предоплаты
- присылает поддельный чек об оплате доставки или пересылки товара

ВАЖНО БУДЬТЕ ОСТОРОЖНЫ!

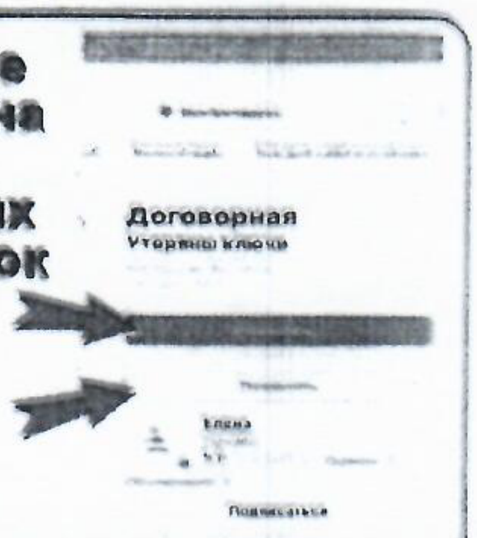
Мошеннические страницы могут быть как две капли воды похожи на официальные сайты торговых площадок или служб доставки

Всегда проверяйте адрес официального сайта торговой площадки или сервисов служб доставки

- Это место, где записывают адрес сайта

Позвоните покупателю, чтобы убедиться, что его номер телефона реальный

Общение ведите на сайтах торговых площадок



НЕ

- сообщайте никому данные банковской карты
- сообщайте никому пароли и коды из SMS-сообщений
- сообщайте никому CVC/CV2-код, даже если Вам обещают перевести деньги
- переходите по предоставленым ссылкам для осуществления сделок
- сканируйте QR-коды, которые Вам высылают
- выполняйте действия с банковской картой по просьбе третьих лиц