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

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.

Социальная опасность указанных преступлений в настоящее время обусловлена широким применением в Республике Беларусь систем безналичных расчетов и сопряжена с причинением или угрозой причинения существенного вреда правоохраняемым интересам.

В современных условиях для эффективного противодействия преступности и обеспечения информационной безопасности необходимо вовремя реагировать на новые тенденции, в первую очередь, связанные с уголовно-наказуемыми деяниями в IT-сфере.

В Партизанском (г. Минска) районном отделе Следственного комитета Республики Беларусь 26.12.2024 возбуждено уголовное дело № 24121051012 по признакам преступления, предусмотренного частью 4 статьи 209 Уголовного кодекса Республики Беларусь.

В ходе предварительного расследования установлено, что неустановленное лицо с использованием достоверно неустановленного абонентского номера в мессенджере «Telegram» в период с 26.10.2024 по 18.11.2024 путем телефонных звонков, а также смс-сообщений, реализуя умысел на умышленное противоправное безвозмездное завладение имуществом с корыстной целью, путем обмана и злоупотребления доверием, под предлогом изобличения мошенников, склонило потерпевшую, к осуществлению ряда переводов денежных средств на общую сумму в размере 57400 белорусских рублей, а также при вышеуказанных обстоятельствах потерпевшая осуществила передачу наличных денежных средств неизвестному лицу на общую сумму в размере 217410,4416 белорусских рублей. Таким образом последней причинен имущественный вред в особо крупном размере

Из показаний потерпевшей известно, что в октябре 2024 года посредством мобильной связи с ней начал общение сотрудник оператора сотовой связи СООО «МТС», который указал ей, что необходимо улучшить её мобильную связь. Она

согласилась и по его указаниям проделывала различные манипуляции в мобильном телефоне. После чего посредством мобильной связи с потерпевшей связался сотрудник Следственного комитета, который рассказывал о том, что на счета потерпевшей хотят посягнуть мошенники, поэтому для безопасности её счетов их необходимо задекларировать и перечислить на безопасные счета. В последующем под различными предлогами он просил переводить денежные суммы, при этом в переписке сообщал данные лиц, на имя которых необходимо оформить перевод, что потерпевшая и делала. Таким же образом потерпевшая продала свою квартиру, а денежные средства передала курьеру с целью того, чтобы задекларировать свои денежные средства.

В Партизанском (г. Минска) районном отделе Следственного комитета Республики Беларусь особое внимание уделяется раскрытию данных преступлений, расследованию уголовных дел и профилактической работе.

Одним из приоритетных направлений в укреплении правопорядка в современном мире и основным критерием предупреждения преступности является информирование населения, в том числе в целях повышения компьютерной грамотности и упреждения противоправных деяний.

Анализ правоприменительной практики показывает, что 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 клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте учреждения.

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.

К примеру, на мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником банка (правоохранительных органов и т.д.) - может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах. Злоумышленник сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков, в том числе с целью финансирования экстремистской деятельности. Когда пользователь отвечает, что никаких операций он не производил, злоумышленник говорит, что указанные операции необходимо заблокировать (или оказать помощь в поимке мошенников), в связи с чем просит пользователя установить на мобильный телефон различные приложения, сообщить отдельные реквизиты БПК либо паспортные данные, и при необходимости информирует, что в адрес пользователя высылает смс-сообщения с кодами, которые необходимо назвать после звукового сигнала. В это время всю злоумышленник использует всю полученную информацию и получает доступ к денежным средствам пользователя и совершает их хищение.

«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 отмечается 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 с популярными доменными именами, к примеру: «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», а также путем уговоров убеждают граждан оформить на свое имя кредиты и перевести денежные средства на счета подконтрольные злоумышленникам.

Можно привести в пример уголовное дело о хищении денежных средств в особо крупном размере. Так, минчанке позвонила на Viber неизвестная, которая представилась сотрудником банка. Она сообщила, что прямо сейчас с ее банковской карточки мошенники переводят деньги на другой счет. Пожилая женщина сразу поправила звонившую, пояснив, что у нее есть банковский счет, но к нему банковская

карта не имитировалась. После чего звонившая сообщила, что переключит ее на другого специалиста. Который сообщил, что необходимо пресечь хищение, и с этой целью ей необходимо установить на мобильный телефон приложение удаленного доступа, что последняя и сделала. После чего представитель банка начал убеждать, что зафиксированы несанкционированные операции и что в скором времени с ней свяжутся сотрудники милиции.

И действительно, через некоторое время снова на Viber начал звонить якобы представитель правоохранительных органов. Он подтвердил слова ранее звонившего, сообщил что необходимо написать заявление о несанкционированной операции и рассказал, что в банке произошла утечка данных и в настоящее время никому нельзя сообщать о произошедшем.

На следующий день ей вновь позвонил сотрудник банка и смог убедить женщину, и она, следуя его инструкциям, в несколько этапов сняла со счета деньги и зачислила их на свой счет, открытый в ином банковском учреждении, которым имелась возможность управлять с помощью системы дистанционного банковского обслуживания (интернет-банкинг), в том числе взяла несколько кредитов в банковских учреждениях и также зачислила их на вышеуказанный счет. Более того, минчанка передала данные для входа в установленное на мобильном телефоне приложение удаленного доступа и по просьбе сотрудника банка запустила его, что позволило злоумышленнику с помощью удаленного доступа, авторизовался от имени минчанки в личном кабинете интернет-банкинга и дистанционно распорядиться деньгами. В результате с карт-счета пенсионерки похищено более 236 тыс. рублей.

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 40 % больше по сравнению с аналогичными периодами прошлых лет), 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. 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_rm>, «room_dream», «Zonaest.2020», «euphoria.women.bq», «raspiv_parfum_by», «queen.shop_pob>, «romashkashowroom.bel», «guanto_mens_fashion», «dreamroom ru», «soffi boutique» и другие.

Возрастает также 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.

Кроме того, с 2024 года значительно увеличилось количество преступлений, связанных с трейдингом (торговля валютой, ценными бумагами, товарами и т.д.).

К примеру, гражданам по телефону поступают звонки от сотрудников компаний с предложениями об открытии торговых счетов или же сами потерпевшие с целью осуществления трейдинга находят в глобальной компьютерной сети Интернет поддельные (фишинговые) сайты, используемые для выманивания денежных средств пользователей (на указанных сайтах потерпевшие оставляют свои контактные данные или проходят аудентификацию).

В последующем потерпевшие осуществляли общение с злоумышленниками с использованием различных мессенджеров и звонков (зачастую использовалась IP-телефония).

В ходе общения представители компаний (брокеры) рассказывали о сути предлагаемых услуг, а именно: на имя клиента компания открывала личный торговый счет, финансовые операции по которому должен проводить клиент по советам сотрудника компании (брокера).

В дальнейшем, под их руководством потерпевшие проходили процесс регистрации посредством глобальной компьютерной сети Интернет на различных фишинговых сайтах, затем по электронной почте получали уведомления о том, что регистрация для открытия счета успешно завершена. Все денежные средства, которые потерпевшие переводили на личные счета, отображалась в их личных кабинетах. Далее потерпевшие пребывали в полной уверенности в том, что они под руководством брокеров проводят реальные операции (с криптовалютой, драгоценными металлами и т.д.), однако, на самом деле играли в онлайн-игру, которая имитирует работу форекс-компании, в том числе онлайн-торги.

В последующем, при попытке вывести денежные средства потерпевшим поступали различные требования, которые необходимо выполнить для осуществления

вывода денежных средств (уплата налогов и т.д.), а затем доступ к аккаунтам блокировался, как и возможность пользоваться услугами, проводить какие-либо операции и выводить денежные средства. Затем денежные средства исчезали.

Стоит отметить и тот факт, что отдельные потерпевшие в последующем находили в глобальной компьютерной сети Интернет различные контактные данные организаций, которые за денежное вознаграждение готовы оказать помощь в возврате денежных средств.

Вместе с тем, в свою очередь указанные организации (лица) имея умысел на противоправное завладение денежными средствами, путем обмана, под предлогом оказания помощи, заранее не намереваясь выполнить взятые на себя обязательства, также склоняли потерпевших, к переводу денежных средств, с целью оказания им помощи, а после переставали выходить на связь.

Также хотелось бы отметить о появлении в 2024 году новой мошеннической схемы «FAKE BOSS».

Так как, звонки от якобы сотрудников правоохранительных органов, сотрудников банковских учреждений, операторов сотовой связи перестали удивлять, что послужило появлению новой усложненной и многоступенчатой схемы мошенничества, получившего название **«FAKE BOSS».** Она состоит из нескольких этапов, на которых преступники «ведут» жертву, передавая ее из рук в руки.

Установлено, что злоумышленники изучают средства группового обмена сообщениями (чаты) в различных мессенджерах, используемые работниками таких учреждений 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.

Такими предлогами совершения хищений денежных средств могут быть:

- участие в специальной операции по поимке «преступников», которые якобы пытаются похитить деньги с использованием счетов гражданина или от его имени;
- наличие информации о якобы совершении гражданином преступных финансовых операций, для снятия подозрения в которых необходимо совершить требуемые действия;

- планируемое проведение обыска по месту жительства гражданина с целью выявления и изъятия незадекларированных наличных денежных средств.

Убедив работника учреждения (предприятия) в правомочности своих действий, звонящий предлагает передать посреднику наличные денежные средства или внести их на указанные им банковские счета; перечислить денежные средства с банковских счетов, в том числе оформив на свое имя для этих целей кредиты; предоставить реквизиты своих банковских карт, аутентификационные данные для доступа к банковским счетам, коды из поступивших sms-сообщений и т.д.

В этих случаях можно рекомендовать:

- 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;
- никому не сообщать реквизиты банковских карт, аутентификационные данные для доступа к банковским счетам, содержание sms-сообщений, поступивших на личные абонентские номера;
- незамедлительно информировать о выявленных попытках руководителя учреждения образования для принятия мерпо упреждению подобных действии и правоохранительные органы для реагирования. .

В настоящее время также наиболее актуальны так называемые факты «телефонных мошенничеств». 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 различные вещи и денежные средства.**

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 (приезжает курьер за деньгами или потерпевшие сами переводят их на предоставленные счета).

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!

Кроме того, анализ правоприменительной практики показывает, что в настоящее время для хищения денежных средств стали активно **использоваться банковские счета, открытые на имя граждан Республики Беларусь в возрасте от 16 до 27 лет.** В последующем данные лица добровольно передают реквизиты своих банковских платежных карт либо аутентификационные данные, посредством которых возможно получить доступ к их банковским счетам, третьим лицам за денежное вознаграждение.

Злоумышленники посредством глобальной компьютерной сети Интернет создают различные учетные записи (аккаунты) в социальных сетях и мессенджерах, где размещают объявления о «легальном» и быстром заработке. В ходе общения гражданам предлагается за денежное вознаграждение оформить на себя одну или несколько БПК, передать полученные в банковском учреждении документы и БПК курьеру либо предоставить доступ к системе дистанционного банковского обслуживания счетами, сообщить коды, приходящие посредством СМС-сообщений. При этом, держатели БПК вводятся в заблуждение относительно легальности данного вида заработка.

Указанные обстоятельства позволяют злоумышленникам, получившим необходимую электронно-цифровую информацию, использовать банковские счета в преступных целях, зачастую для хищения денежных средств граждан с использованием вышеуказанных методов социальной инженерии.

Действия граждан, связанные с оформлением банковских счетов и передачей электронно-цифровой информацией третьим лицам, могут повлечь за собой

уголовную ответственность, которая наступает с 16-летнего возраста.

Выявлены неединичные факты вовлечения несовершеннолетних в подобную незаконную деятельность, за совершение которой предусмотрено наказание в виде штрафа, или ограничения свободы на срок от двух до пяти лет, или лишения свободы на срок от двух до шести лет, а за те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере - ограничения свободы на срок от трех до пяти лет или лишения свободы на срок от трех до десяти лет со штрафом или без штрафа (статья 222 Уголовного кодекса Республики Беларусь).