Министерства и ведомства,
Минский городской исполнительный комитет, администрации районов г. Минска, организации и предприятия г. Минска
(согласно списку рассылки)

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. В 2021 году в Республике Беларусь зарегистрировано свыше 14 500 таких хищений, что более чем в 7 раз превысило уровень пятилетней давности (2 069).

*Справочно: в 2021 году следственными подразделениями столицы возбуждено 5 196 уголовных дел о преступлениях в сфере высоких технологий. 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 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 2021 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.

*Справочно: в официальных отчетах о киберпреступности сообщается, что атаки хакеров во всем мире в 2020 году происходили каждые 14 секунд, то в 2021 году уже каждые 10 секунд. По своей значимости риски киберпреступность приравнивается к экологическим проблемам.*

Анализ деятельности злоумышленников на территории Республики Беларусь показал, что в 2022 году идет рост противоправных деяний в IT-сфере совершаемых с использованием фишинговых ссылок (в большинстве случаев направлен на хищение денежных средств граждан, разместивших объявление или покупавших какой-либо товар посредством крупнейшей площадки объявлений Республики Беларусь – «Kufar.by»), 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 в текущем году, 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. В настоящее время от действий группы мошенников пострадали уже свыше 150 граждан.

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.

На основании вышеизложенного, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 № 403-З «О Следственном комитете Республики Беларусь», в целях противодействия киберпреступности, повышения уровня кибербезопасности, защиты прав и законных интересов граждан, организаций, государственных и общественных интересов, прошу:

рассмотреть настоящее информационное письмо с руководителями структурных подразделений с целью недопущения совершения хищений, совершенных с использованием компьютерных систем и глобальной компьютерной сети Интернет;

с учетом темпа развития информационных систем, внедрения новых цифровых технологий, рекомендовать сотрудникам 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 и граждан о необходимости проявления осторожности и бдительности, соблюдении правил безопасности при работе в глобальной компьютерной сети Интернет;

инициировать освещение посредством различных источников, в том числе в СМИ, информации о новых средствах и способах совершения противоправных деяний (используемых ресурсах глобальной компьютерной сети Интернет, именах учетных записей, адресах и прочем), а также о лицах, их совершивших;

разработать и принять комплекс правовых, организационных и технических мер, направленных на сохранение благосостояния граждан, защиту прав и законных интересов граждан, организаций, государственных и общественных интересов;

принять дополнительные организационно-практические меры, направленные на внедрение системы дополнительной проверки (идентификации) пользователей при регистрации и осуществлении различного рода операций с использованием глобальной компьютерной сети Интернет, защиту полученной информации в целях недопущения доступа к кабинетам пользователей, а также иных неправомерных действий третьих лиц.

Начальник управления
генерал-майор юстиции С.М.Паско

15-5 Суворов 389 56 20