Следчы камітат
Рэспублікі Беларусь
Управленне
па горадзе Мінску
вул. Сапёраў, 7, 220035, г.Мінск
тэл. (017) 389 55 55, факс (017) 389 56 56
e-mail: mn@sk.gov.by

Следственный комитет
Республики Беларусь
Управление
по городу Минску
ул. Сапёров, 7, 220035, г.Минск
тел. (017) 389 55 55, факс (017) 389 56 56
e-mail: mn@sk.gov.by

25.01.2024 № 15-4/2244
На № _____ от _____

ГУП «Белэнерго»

220004, г. Минск, ул. Шорная, д.17

О вопросах профилактики преступлений против собственности и информационной безопасности

В Республике Беларусь продолжают быть актуальными проблемы преступности в сфере высоких технологий. На киберпреступность влияет ежегодный рост числа абонентов сотовой электросвязи, держателей банковских платежных карточек (далее – БПК), а также пользователей сети Интернет.

В настоящее время значительным является количество принимаемых решений о возбуждении уголовного дела о хищениях путем модификации компьютерной информации (ст. 212 УК Республики Беларусь).

Не смотря на принимаемые Следственным комитетом, иными государственными органами и банковскими учреждениями мероприятия профилактического характера, продолжают фиксироваться случаи хищения денежных средств с банковских счетов, доступ к которым обеспечивается при использовании БПК, после передачи либо завладения информацией о реквизитах БПК злоумышленниками.

Современные методы оплаты в сети Интернет позволяют совершать платежи без знания PIN-кода карточки, путем введения в компьютерную систему сведений о номере карточки, сроке ее действия, владельце, а также коде безопасности – CVC (трехзначный код, находящийся на оборотной стороне карты). Данные обстоятельства позволяют злоумышленникам, завладевшим указанными реквизитами БПК, совершать платежи в сети Интернет без ведома владельца, обладая всей необходимой для этого информацией.

Вместе с тем Интернет-банкинг постепенно завоевывает статус основной платформы для заказа банковских услуг, осуществления денежных переводов и управления открытыми расчетными счетами. Для доступа к системе виртуального банкинга клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте финансового учреждения. Авторизация производится с привязкой к номеру телефона. Часто пользователи Интернет-банкинга указывают пароль, который совпадает с логином пользователя в учетной записи, то есть номером телефона клиента, что позволяет методом подбора осуществлять вход в личные кабинеты пользователей.

Так, в производстве следственного управления УСК Республики Беларусь по г. Минску находится уголовное дело, возбужденное по признакам преступления, предусмотренного частью 2 статьи 212 УК Республики Беларусь, по факту совершения 01.10.2020 хищения денежных средств, принадлежащих гражданину Т... (является работником ГУП «Белэнерго»), путем модификации компьютерной информации, чем указанному потерпевшему причинен имущественный вред.

Согласно материалам уголовного дела, гражданину Т... (является работником ГУП «Белэнерго») поступил звонок на сотовый телефон, в ходе которого неизвестное лицо, представившись представителем ОАО «АСБ Беларусбанк», убедило его в том, что с его банковского счета пытаются похитить денежные средства, а для предотвращения данной операции необходимо сообщить реквизиты БПК, CVC-код и приходящие на мобильный телефон посредством SMS-информирования одноразовые коды для авторизации.

Примеры наиболее распространенных в настоящее время противоправных действий в сфере информационных технологий, а именно хищений с БПК и счетов физических и юридических лиц, примеры подобных фактов приведены далее.

1. Злоумышленник после несанкционированного доступа к страницам пользователей в социальных сетях рассылает от его имени пользователям, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи в переводе денежных средств под различными предлогами: «Привет, не мог ли ты одолжить мне денег, отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)». Далее входит в доверие к неравнодушным пользователям и, якобы для перевода им денежных средств, просит сообщить реквизиты БПК и коды из SMS-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение.

Проведя несанкционированную операцию по переводу денежных средств, злоумышленник часто сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых).

2. На торговых площадках «Куфар», «Барахолка» и других правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хотел бы приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности лично за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на БПК пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского или иного учреждения (страница может быть визуально схожа со страницей Интернет-банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится не на действующей странице Интернет-банкинга определенного банка. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свои реквизиты БПК, логин и пароль от Интернет-банкинга либо паспортные данные, а также коды из SMS-сообщений. Введя указанную информацию пользователю, как правило, сообщается об ошибке либо невозможности совершить платеж. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может осуществить операцию, и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых).

3. На торговых площадках «Куфар», «Барахолка» и других злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену, как правило, ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности лично встретиться для передачи указанного в объявлении имущества, предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (EMC)», «курьерская служба (СДЭК)» и т.п. При согласии покупателя злоумышленник высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты банковской карты для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также коды из SMS-сообщений. После ввода указанной информации пользователю обычно сообщается об ошибке либо сайт перестает загружаться («зависает»). В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получая доступ к денежным средствам

пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых).

4. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, при этом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, либо использует для осуществления звонка мессенджер «Viber», где у вызывающего абонента имеется ярлык с логотипом банковского учреждения. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карточки либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков. Когда пользователь сообщает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя сообщить отдельные реквизиты БПК либо паспортные данные, и сообщает, что в адрес пользователя высылает SMS-сообщения с кодами, которые необходимо назвать после звукового сигнала. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка, получает доступ к денежным средствам пользователя и совершает их хищение.

Запрашиваемая преступником указанная в вышеобозначенных ситуациях информация **либо известна сотрудникам банка, либо не требуется им ни при каких обстоятельствах. Сотрудники банка никогда, в том числе и в ходе телефонного разговора, не будут узнавать у клиента подобную информацию**.

Для того чтобы обезопасить себя и свои денежные средства от подобных способов хищения, необходимо:

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты БПК, расчетных счетов, секретные CVC/CVV-коды, данные касательно последних платежей и срока действия пластиковых карточек третьим лицам;

в ходе использования карты подключить и использовать технологию «3D Secure». На настоящий момент это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. Позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества

по карте. При использовании этой технологии держатель банковской карточки подтверждает каждую операцию по своей карточке специальным сеансовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученных в SMS-сообщениях сеансовых паролей для подтверждения операций, а также своих банковских карточек, каким бы то ни было способом;

вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с **https://**, а не **http://**;

производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации; SMS-информирования о расходных операциях);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2 – 4 недели, если пользуетесь чужими компьютерами для входа в систему Интернет-банкинга;

не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется компьютер общего доступа;

в ходе использования Интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адресу. Это действие обеспечит максимальный уровень безопасности.

В случае обнаружения утерянной кем-либо БПК не стоит выкладывать ее фотографию в сети Интернет с целью поиска владельца. Информации, имеющейся на изображении БПК, может быть достаточно для совершения операций с использованием этих данных без ведома владельца банковской карточки, чем и пользуются злоумышленники.

В целях устранения причин и условий, способствовавших совершению преступления, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 № 403-З «О Следственном комитете Республики Беларусь», прошу:

рассмотреть информационное письмо с сотрудниками ГУП «Белэнерго»;

в соответствии с требованиями Закона Республики Беларусь от 04.01.2014 № 122-З «Об основах деятельности по профилактике правонарушений» на системной основе проводить информирование сотрудников о проявлении осторожности и бдительности, соблюдении установленных правил безопасности пользования персональными БПК, предупредить о недопустимости игнорирования и пренебрежения действенных требований, направленных на сохранение благосостояния граждан.

С учетом темпа развития информационных систем, внедрения новых цифровых технологий принимать дополнительные меры по безопасности использования банковских продуктов.

О принятых мерах прошу уведомить следственное управление Управления Следственного комитета Республики Беларусь по г. Минску в месячный срок.

Руководитель следственной группы –
следователь по ОВД следственного управления
УСК Республики Беларусь по г. Минску П.Л.Кушнирик

15/4_3899153
Кушнирик