Противоправные действия в сфере информационных технологий

В последнее время участились случаи противоправных действий в сфере информационных технологий, а именно хищений с банковских платежных карт и счетов физических и юридических лиц, примеры подобных фактов приведены далее:

1) Злоумышленник после несанкционированного доступа к страницам пользователей в **социальных сетях** рассылает пользователям, находящимся в разделе **«Друзья»** сообщения носящие в себе просьбы в 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 неравнодушным пользователям он вбивается в доверие и якобы для перевода им денежных средств просит сообщить реквизиты банковских платежных карт и коды из смс-сообщений, после чего пользователь, будучи введенным в заблуждение относительно лица, осуществившего указанную рассылку и не догадываясь о преступности его 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 за частую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

2) На торговой площадке «Куфар», «Барахолка» и т.д. злоумышленник находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет указанному пользователю, о том, что хотел бы приобрести его имущество указанное в объявлении, однако по различным причинам не имеет возможности за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на банковскую платежную карту пользователя и после того как пользователь соглашается высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского 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 свой логин и пароль от интернет-банкинга, либо паспортные данные, а также коды из смс- сообщений. Введя указанную информацию пользователю как правило сообщается об ошибке либо отсутствия платежа. В это время всю введенную информацию видит злоумышленник и вводит на

действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник за частую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

3) На торговых площадках «Куфар», «Барахолка» и т.д. злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену за частую ниже рыночной. Пользователи увидевшие указанное объявление пишут лицу его разместившему и в ходе переписки злоумышленник сообщает, что не имеет возможности встретиться для передачи указанного в объявлении имущества и предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (ЕМС)», «курьерская служба (СДЭК)» и т.д. Согласившись, злоумышленник высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где на указанном сайте пользователю как правило предлагается ввести реквизиты банковской карты для оплаты товара либо услуг курьера, либо паспортные данные, номер мобильного телефона, а также коды из смс-сообщений. Введя указанную информацию пользователю как правило сообщается об ошибке либо сайт перестает загружаться (зависает). В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник за частую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

4) На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило в указанном способе злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее злоумышленник представляется сотрудником банка (он 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 на крупные суммы 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 банковской платежной карты, либо паспортные данные, после чего сообщает, что в адрес пользователя он высылает смс-сообщения с кодами, которые ему необходимо будет назвать после звукового сигнала. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. (Вся запрашиваемую информацию известна сотрудникам банка, и они не стали бы спрашивать ее в ходе телефонного разговора).

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

1. Не разглашать логины, финансовые номера телефонов пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW- коды, данные касательно последних платежей и срока действия пластиковых карт третьим лицам.

2. 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 карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон.

, 3, ИскЛ|очить передачу посторонним лицам полученные в SMS оообщенилх временные пароли для подтверждения **операций** а та^ своих банковских карт, каким бы то ни было способом.

■ Вводить секретные данные только на сайтах защищённых сертификатами безопасности и механизмами шифрования Доменные chttps://тм" РеСУРС0В В аДРеСН0Й оТР0Ке КаЖД0Го брау3еРа начинаются

5. ^ Производить регулярный мониторинг выполненных операции, используя раздел с историей платежей.

6. Не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации).

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.

8. Не использовать автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт пользуется общественный компьютер.

9. В ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит.

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

Обращаю особое внимание на то, что в случае обнаружения

выкладывать ее фотографию в сети интернет с целью поиска владельца. Информации, имеющейся на изображении карты достаточно для совершения операций с использованием этих данных без ведома владельца банковской карты, чем и пользуются злоумышленники.

Таким образом, основной причиной совершения преступления, явилось безответственное отношение потерпевшей И. к сохранности персональных данных своей банковской платежной карты.

На основании изложенного, в целях устранения причин и условии, способствовавших совершению преступления, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 №403-З «О Следственном комитете Республики Беларусь»,

утерянной кем-либо банковской платежной карты, не стоит