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 зачастую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых), чтобы также завладеть денежными средствами.

2) На торговой площадке **«kufar.by»,** «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 воспользоваться услугами «Доставка Куфар», «Белпочта (ЕМС)», «курьерская служба (СДЭК)», а также произвести оплату путем перевода денежных средств на банковскую платежную карту пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку на фишинговый интернет-ресурс, который визуально схож с сайтом какого-либо банковского учреждения либо торговой площадке, на которой было размещено объявление пользователя (фишинговый интернет-ресурс отличается только символом в адресной строке доменного имени сайта). В результате перехода пользователя по ссылке в открывшемся окне на указанном сайте, как правило, под предлогом получения денежных средств ему предлагается ввести свой логин и пароль от интернет- банкинга, либо паспортные данные, либо реквизиты банковской платежной карты, 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 зачастую 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 «kufar.by», «Барахолка» и т.д. злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену зачастую ниже рыночной. Пользователи, увидевшие указанное объявление, пишут разместившему его лицу 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. Когда пользователь, заинтересованный в покупке товара, соглашается, 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 зачастую 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 (в том числе в различных мессенджерах).** 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 (идентификационный номер паспорта), 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 запрашиваемая информацию известна сотрудникам банка, и они не стали бы спрашивать ее в ходе телефонного разговора, в том числе сотрудники банка не пишут и не звонят клиентам банка в различных мессенджерах).

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

1. Не разглашать третьим лицам логины, финансовые номера телефонов (номер, который используется для входа в интернет-банкинг), пароли от личного кабинета в интернет-банкинге, ПИН-коды, реквизиты расчетных счетов, реквизиты банковских платежных карт: номер, срок действия, секретные CVV/CW-коды, данные касательно последних платежей.
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, которая 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. Исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, каким бы то ни было способом.
4. Производить регулярный мониторинг выполненных операций, используя раздел с историей платежей.
5. Не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации).
6. Подобрать сложный пароль для входа в личный кабинет в интернет-банкинге, 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.
7. Не использовать автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется общественный компьютер.
8. В ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит.

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

Информация Московского (г. Минска) районного отдела Следственного комитета Республики Беларусь