УСК по Витебской области о примерах хищений с использованием компьютерной техники

Киберпреступления. Как не стать жертвой мошенников.

Вишинг — форма мошенничества, когда злоумышленники, используя телефон, представляются, например, сотрудником банка, и под разными предлогами выманивают персональные данные платежных банковских карт, чтобы похитить денежные средства.

Еще одним способом завладения реквизитами платежных банковских карт является фишинг. Мошенники рассылают людям электронные сообщения, в которых содержится ссылка на сайт, внешне неотличимый от настоящего. После того как пользователь попадает на поддельную страницу, мошенники побуждают его ввести на ней свои логин и пароль доступа к определенному сайту, что позволяет им получить доступ к аккаунтам и банковским счетам.

За 10 месяцев текущего года в Витебской области следователями возбуждено 1307 уголовных дел (за 10 месяцев 2020 года - 1709) по ст.212 (хищение имущества путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь и 110 уголовных дел (за аналогичный период 2020 года – 231) по ст.349 (несанкционированный доступ к компьютерной информации) Уголовного кодекса Республики Беларусь.

Так, 22 сентября этого года жительница Полоцка зашла на поддельный сайт интернет-банкинга, где ввела данные и пароли своей платежной банковской карты. В результате у женщины с карты похитили все денежные средства, находящиеся на ней, то есть 200 рублей. Возбуждено уголовное дело по ч.1 ст.212 Уголовного кодекса Республики Беларусь.

15 сентября жителю Витебска в мессенджере Viber позвонил мужчина и представился сотрудником банка. Он сказал, что мошенники пытаются похитить с его банковской карты деньги и оформить кредиты, а также предложил поучаствовать в спецоперации по их разоблачению и поимке. Для этого нужно было оформить на себя кредиты в различных банках и переводить полученные денежные средства на указанные счета. На протяжении семи дней потерпевший общался с лжесотрудником банка и следовал его указаниям. За это время он оформил на себя четыре кредита и перевел более 23 тысяч рублей. Возбуждено уголовное дело по ч.3 ст.212 Уголовного кодекса Республики Беларусь.

К странице жительницы Толочина в социальной сети мошенники получили доступ и осуществляли с нее переписку от её имени с целью завладения денежными средствами. Знакомые владелицы страницы увидели сообщения с просьбами оказания помощи и хотели перевести деньги, однако у них были только наличные. В связи с чем им удалось избежать потери своих денежных средств. По данному факту возбуждено уголовное дело по ч.1 ст.349 Уголовного кодекса Республики Беларусь.

Девушка разместила объявление о продаже товара в интернете. С ней 9 ноября в мессенджере связался «покупатель» и под предлогом оплаты товара сбросил ей ссылку на поддельный сайт. Введя реквизиты своей платежной банковской карты и пришедший в сообщении код, потерпевшая лишилась 110 рублей. Возбуждено уголовное дело по ч.1 ст.212 Уголовного кодекса Республики Беларусь.

Таких примеров совершения киберпреступлений в Витебской области можно приводить очень много, т.к. мошенники продолжают придумывать различные способы хищений денежных средств, а граждане во многих случаях проявляют излишнюю доверчивость и невнимательность. **Однако статистические показатели говорят о том, что профилактика помогает сохранить деньги людей.** Чтобы уберечь себя от киперпреступников, следователи в очередной раз рекомендуют:

- ни при каких обстоятельствах в ходе телефонного разговора никому не сообщайте данные своей платежной банковской карты;

- когда вам звонят в мессенджерах и представляются сотрудниками банка или правоохранителями обращайте внимание на номер телефона и код страны звонящего (чаще всего мошенники звонят из-за границы);

- не переходите по подозрительным ссылкам и не вводите данные своих платежных банковских карт в случае, если вам пришло сообщение о том, что если вы пройдете регистрацию по ссылке, то получите что-либо бесплатно, например, в подарок 100 литров дизельного топлива, скидку 500 рублей на покупки в магазине и т.д.;

- не передавайте данные платежной банковской карты, в том числе в ходе переписки в интернете или по телефону лицам, представляющимися сотрудниками банка. У сотрудников банка нет необходимости звонить Вам с просьбой сверить данные и пароли Ваших платежных банковских карт;

- помните, что правоохранители никогда не будут звонить и просить сообщить данные ваших платежных банковских карт;

- при покупке или продаже товара не передавайте данные своей платежной банковской карты и не сообщайте приходящие в сообщениях коды;

- если вам позвонили и сказали, что на ваше имя пытаются оформить кредит, говорят о подозрительной активности на ваших счетах и т.д., не сообщайте звонящему данные платежной банковской карты и приходящие в сообщениях коды, прекратите разговор и перезвоните в банк (номер его телефона указан на платежной банковской карте);

- если вы познакомились в социальных сетях с человеком, который рассказывает о занимаемых им высоких должностях, чинах и регалиях, говорит, что сказочно богат, обещает вам замечательную новую жизнь в достатке, однако постоянно просит вас перевести ему денежные средства – задумайтесь, не водят ли вас за нос;

- если вам пришло сообщение о том, что вы выиграли приз участвуя в конкурсе (но вы не участвовали ни в каком конкурсе) – не переходите по сомнительным ссылкам, не указывайте свои логин и пароль от персональных страниц в социальных сетях;

- если к вам в социальных сетях со страниц ваших знакомых обратились с помощью о переводе денежных средств с использованием вашей платежной банковской карты – будьте внимательны! Изначально убедитесь, что ваш знакомый действительно нуждается в помощи (перезвоните этому человеку, задайте собеседнику такой вопрос, ответ на который будете знать только вы). Эти действия необходимы для того, чтобы убедиться, что «аккаунт» (страница) вашего знакомого человека не взломан и он действительно нуждается в помощи;

- при обнаружении платежной банковской карты не выкладывайте их фотографии с реквизитами в социальных сетях (этим могут воспользоваться злоумышленники), отнесите найденную карту в банк;

- не сообщайте пин-коды от платежных банковских карт третьим лицам;

- постарайтесь не использовать WI-FI в общественных местах для входа в приложения интернет-банкинга и оплате каких-либо услуг в сети

Интернет (этим могут воспользоваться злоумышленники);

- если Вам пришло сообщение о необходимости уплаты штрафа за совершенный просмотр какого-либо видеофайла или сайта от имени правоохранителей – не переводите денежные средства. Изначально стоит обратиться в правоохранительные органы и уточнить, действительно ли это так;

- используйте сложные пароли и не сохраняйте их в браузерах;

- не переходите по подозрительным ссылкам и не открывайте подозрительные письма и вложения к ним;

- не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред;

- осуществляйте оплату в интернете только на проверенных ресурсах;

- проявляйте бдительность и осмотрительность! Поделитесь данной информации со своими друзьями, родными и близкими.

Официальный представитель УСК по Витебской области
Оксана Лазько