В текущем году продолжает расти активность кибермошенников‚ посягающих на имущество жителей Лидского района. Уже Лидским районный отделом Следственного комитета возбуждено около 40 уголовных дел, сопряженных с фактами несанкционированного доступа к учетным записям в социальной сети «ВКонтакте», выманиванием в ходе общения с использованием «взломанных» страниц реквизитов банковских платежных карт (далее БПК) и совершением хищений денежных средств с их использованием. В ряде случаев сумма списаний с БПК превышала тысячу рублей. При этом среди потерпевших есть и студенты, и рабочие, и педагоги, и представители военизированных организаций, и молодые мамы, находящиеся в декретном отпуске.

**- как злоумышленник осуществляет несанкционированный доступ к учетной записи в соцсети?**

Существует достаточно много способов получить ваш логин и пароль в «ВКонтакте». Наиболее актуальные из них – это использование авторизации на различных интернет-ресурсах посредством учетной записи в соцсети, что позволяет недобросовестным владельцам таких ресурсов использовать полученные логины и пароли в противоправных целях, а также создание злоумышленниками фишинговых сайтов, имитирующих внешний вид реальных интернет-страниц и требующих ввода логина и пароля от личной странички, например, под предлогом каких-либо розыгрышей или возможности просмотра скрытой пользователями информации.

**- как не стать жертвой?**

Не использовать реквизиты страниц в соцсетях для авторизации на иных ресурсах, использовать двухфакторную аутентификацию, перед вводом логина и пароля убедиться в том, что попали на реальный сайт, работающий по безопасному протоколу (обычно в таком случае адресная строка браузера становится зеленой либо содержит пиктограмму в виде замка). Не использовать простые пароли, а также одинаковые логины и пароли на различных ресурсах.

**- как преступник получает реквизиты БПК в интернете?**

Взломав страницу в соцсети, злоумышленник ведет переписку с вашими друзьями: обычно под предлогом наличия проблем с БПК просит сообщить реквизиты БПК (номер, срок действия, имя владельца, CVV/CVC-код, указанный на обратной стороне карты) для перечисления денег на их карт-счет с условием последующего возврата. Правда, фантазия злоумышленников практически безгранична, и излагаемые причины для нарушения правил использования БПК (а передача ее реквизитов является таким нарушением и не позволит в дальнейшем вернуть деньги с использованием принципа нулевом ответственности) могут быть и другими. При поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо, в крайнем случае, идентифицировать личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам. CVV/CVC-код передавать не стоит, тем более что он нужен только для осуществления расходных транзакций.

**- как злоумышленник похищает деньги с БПК?**

Обладая всеми реквизитами БПК, это не составляет никакого труда. Он может перечислить деньги на другую БПК, в том числе иностранного банка, приобрести электронные деньги, зачислить средства на баланс мобильного телефона, приобрести товары и услуги в интернет-магазинах. При том остановит злоумышленника только нулевой баланс на БПК. Совет: для использования в интернете крайне желательно завести отдельную БПК с отдельным балансом, благо многие белорусские банки предоставляют такую возможность бесплатно. На балансе такой БПК нелогично хранить значительные суммы денег, а лишь при необходимости перечислять средства с основной БПК. Ни при каких обстоятельствах нельзя передавать третьим лицам реквизиты зарплатной, сберегательной или кредитной БПК. Если вы не планируете использовать БПК для интернет-платежей, установите соответствующие ограничения (лимиты) через систему интернет-банк либо обратившись в офис банка. При использовании БПК в сети интернет, по возможности, используйте технологии обеспечения дополнительной безопасности платежей, такие как 3D-Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ. Установите лимиты, ограничивающие операции в определенных странах, в определенных типах устройств либо в отдельных категориях магазинов. Подключите услугу SMS-информирования и при поступлении информации о несанкционированном списании денег с БПК в срочном порядке принимайте меры к ее блокированию путем обращения в сервисную службу банка. Будет правильным сохранить номер такой службы в адресной книге телефона, чтобы не тратить время на его поиск.

Органами внутренних дел во взаимодействии со следователями по всем фактам хищений денежных средств в интернете проводится комплекс мероприятий, направленных на установление злоумышленников. Учитывая, что большинство таких фактов совершаются с использованием компьютерной техники, находящейся за пределами Республики Беларусь, при проводимой работе активно используются механизмы оказания международной правовой помощи. Однако необходимо отметить, что описанные выше факты во многом стали возможными ввиду неосмотрительности самих владельцев интернет-страниц и держателей БПК. Помните, что только ваша предусмотрительность и бдительность уберегут вас от неприятностей, в том числе имущественного характера.

Во всех случаях несанкционированного доступа к учетным записям в соцсетях и совершения хищений денежных средств с карт-счетов Лидским районный отделом Следственного комитета возбуждаются уголовные дела такие как: «Несанкционированный доступ к компьютерной информации» (статья 349 Уголовного кодекса Республики Беларусь), «Хищение путем использования компьютерной техники» (статья 212 Уголовного кодекса Республики Беларусь). Санкции данных статей предусматривают вплоть до лишения свободы сроком до пяти и двух лет, соответственно.