В Республике Беларусь все чаще становятся актуальными проблемы преступности в сфере высоких технологий. Активизация киберпреступлений происходит на фоне ежегодного роста числа абонентов сотовой электросвязи, держателей банковских платежных карт (далее - БПК), а также пользователей сети Интернет.

В настоящее время наряду с тенденцией роста противоправных деяний в сфере высоких технологий существенно увеличилось количество принимаемых решений о возбуждении уголовного дела о хищениях имущества путем модификации компьютерной информации (ст. 212 УК).

Участились 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 пин-кода карты, путем введения в компьютерную систему сведений о номере карты, сроке ее действия, владельце, а также коде безопасности - CVC (как правило, 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.

Следует отметить, что в последнее время участились случаи 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 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 смс-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 картой (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 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 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 отсутствии платежа. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, 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 картой (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 встретиться для передачи указанного в объявлении имущества и предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (EMC)», «курьерская служба (СДЭК)» и т. д. 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 смс-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 картой (родственников или знакомых).

4. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку, организации (например УП «А1», Энергосбыт) или схожий с ним. Далее он представляется сотрудником банка/УП «А1»/энергосбыта/сотрудником органов внутренних дел (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 в крупных суммах на карт-счета иностранных банков или о том, что у пользователя закончился договор пользованиями услугами УП «А1». 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 смс- сообщения с кодами, которые необходимо назвать после звукового сигнала.

Или же пользователь хочет продлить договор пользования услугами УП «А1» и сообщает об этом злоумышленнику. По просьбе злоумышленника пользователь устанавливает различные приложения на свой мобильный телефон, через которые злоумышленник получает доступ к вашему телефону. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка и получает доступ к денежным средствам пользователя и совершает их хищение.

Или же пользователь звонит на стационарный телефон и сообщает, что необходимо поменять счетчики в квартире, в которой проживает потерпевший. В этот момент потерпевший сообщает свои паспортные данные и ему на мобильный телефон поступает звонок уже от органа внутренних дел и сообщает, что он осуществляет общение с мошенниками и ему немедленно надо положить трубку. После, в ходе разговора с потерпевшим злоумышленник сообщает, что на имя потерпевшего открыты кредиты в банковских учреждениях и их необходимо закрыть путем взятия нового кредита. Потерпевший соглашается и неукоснительно выполняет указания злоумышленника. После взятия кредитов потерпевший осуществляет переводы денежных средств на счета, которые ему сообщает злоумышленник. Также спустя время злоумышленник сообщает, что необходима помощь потерпевшего. Что таким же аналогичным образом обманывают иных граждан и необходимо сохранить их средства. В связи с этим потерпевших направляют по адресам, где они забирают денежные средства у иных потерпевших и по указаниям злоумышленника переводят на счета, которые им указывают.

5. В мессенджере «Telegram» и на сайтах знакомств злоумышленник осуществляет общение с потенциальным потерпевшим. Злоумышленник изъявляет желание познакомиться и ближе узнать друг друга. После того как он

втирается в доверие к потерпевшему просит оказать ему помощь. Так как его мобильный телефон (Iphone) сломался, то он теперь не может войти в свой Icloud и скачать свою личную информацию, в связи с чем просит потерпевшего выйти из своего Icloud и войти в его аккаунт. При этом он направляет потерпевшему логин и пароль для входа. Потерпевший, доверившись злоумышленнику делает то, что он ему говорит. После ввода чужих данных для входа мобильный телефон потерпевшего блокируется и на экране появляется иконка «Телефон утерян. Для разблокировки писать @аккаунт». После чего потерпевший пишет указанному аккаунту, чтобы ему разблокировали мобильный телефон, однако ему выставляют требование, чтобы он оплатил данную услугу. Суммы варьируются от 100 до 300 долларов США. После всех произведенных действий потерпевший более не может вернуть свой мобильный телефон к обычным настройкам и более не может им пользоваться. Таким же образом происходят действия, когда потерпевшему необходимо скачать какое-либо приложение и он просит помощи в установке приложения у неустановленных лиц в различных группах в мессенджерах.

Вся **запрашиваемая преступником** указанная в вышеобозначенных ситуациях информация **известна сотрудникам банка, которые не устанавливают ее в ходе телефонного разговора.**

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

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW- коды, данные касательно последних платежей и срока действия пластиковых карт 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 карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, 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://;

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

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;

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

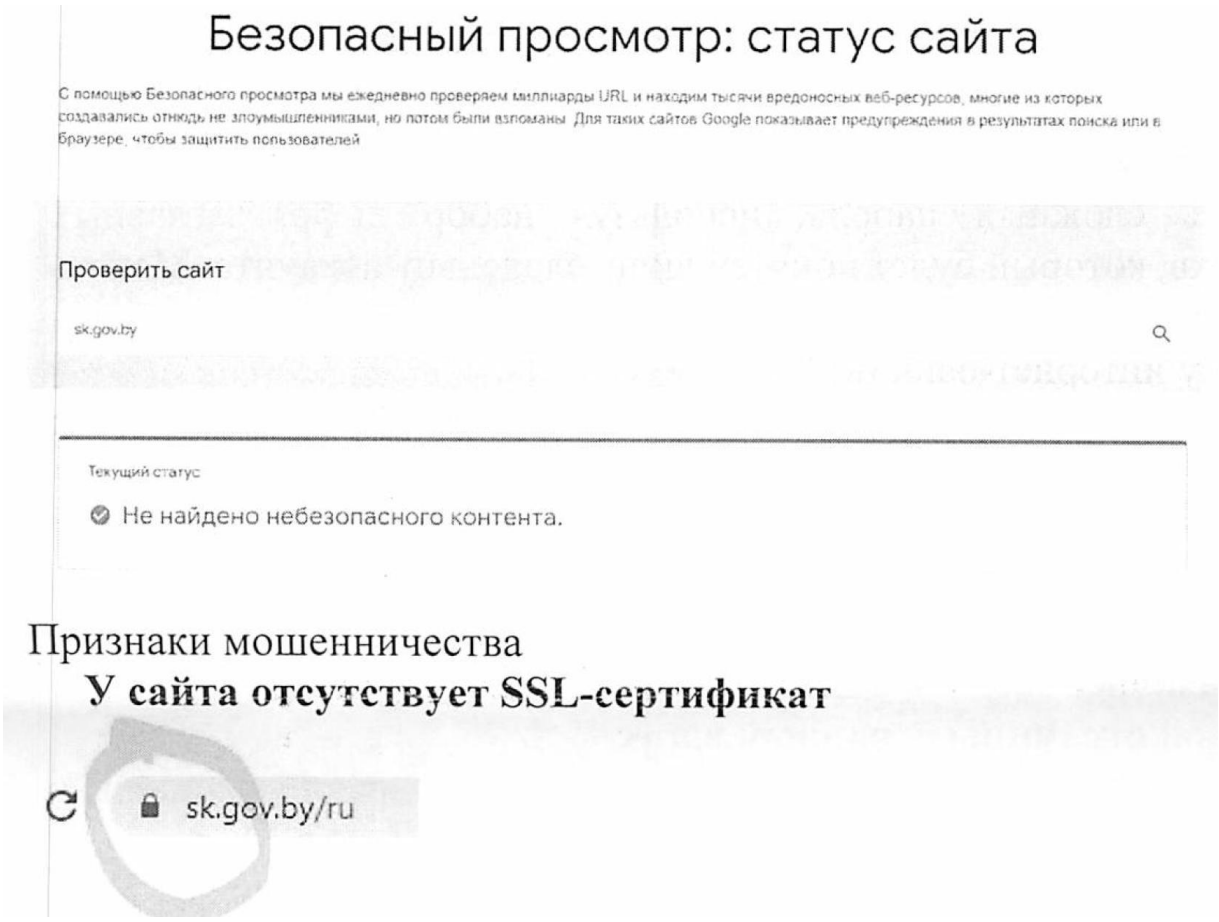
Четыре признака кибермошенника: алгоритм от экспертов

Вместе с ростом покупок в сети Интернет активизируются и кибермошенники. Для них это самое прибыльное время: миллионы людей просматривают десятки миллионов страниц интернет-магазинов.

Провайдер электронных платежей bePaid утверждает, что разработал специальный алгоритм действий, используя который любой покупатель в Сети сможет с максимальной вероятностью определить мошеннический сайт за 1 минуту и сохранить свои деньги.

“Мы рекомендуем использовать этот алгоритм абсолютно во всех случаях. Неважно, как вы зашли на этот сайт: через поисковик, получив письмо на почту или сообщение в Вайбере, кликнув на рекламное объявление или по ссылке от вашего налогового инспектора. У мошенников огромное количество способов заманить вас к себе. А ваши хорошие знакомые могут и не знать, что сайт поддельный - они просто увидели привлекательное предложение в чате или соцсетях”.

Прежде всего проверьте сайт с помощью сервиса “Безопасный просмотр” от Google. Оптимальный вариант - если вы внесете ссылку на этот сервис в закладки и будете проверять все новые сайты, на которые заходите.



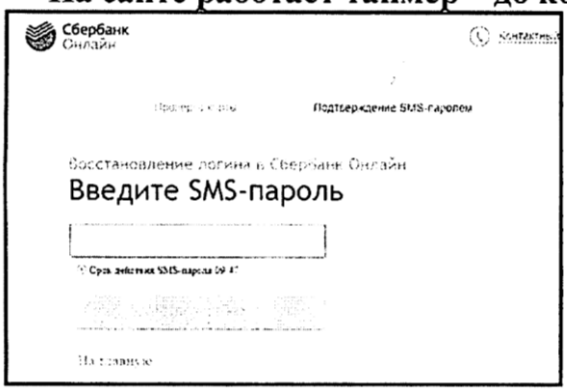
Речь идет о том самом “замочке” в браузерной строке в начале адреса сайта. Если его нет - лучше сразу закрыть этот ресурс. Ведь это означает, что сайт не использует безопасного шифрования, а это значит, что любая введенная информация может быть похищена.

Вам предлагают ввести реквизиты вашей карты прямо на сайте

Если на сайте вас просят ввести номер карты и CVV/CVC код (те самые заветные 3 цифры с обратной стороны вашей карты) - не делайте этого.

99,9% интернет-магазинов во всем мире пользуются услугами специализированных платежных сервисов. Для приема платежей создается специальная защищенная страница, которая может открываться как на отдельной вкладке интернет-браузера, так и в айфрейме поверх сайта продавца. Именно на ней и следует вводить свои платежные данные. Интернет-магазин не может и не должен получить информацию, которую вы там введете.

На сайте работает таймер – до конца акции от 5 до 15 минут



Начинайте опасаться: такой таймер - излюбленный прием мошенников. Сделано это для того, чтобы вы меньше обращали внимание на нестыковки на сайте, а побыстрее вводили свои данные.

У платежной страницы странный адрес

У платежной страницы, как и у всех остальных, есть адрес. Внимательно проверьте: он должен содержать основной домен провайдера. Мошенники пытаются подделать ссылку - отличия могут быть в сдвоенных (или наоборот, пропущенных) символах, замене символов на похожие. Самый простой вариант - скопировать доменное имя и зайти на основной сайт провайдера. Если не получается или сайт провайдера выглядит странно и не вызывает доверия - немедленно закройте страницу. Точно так же можно проверить и достоверность платежной ссылки, которую вам прислали.

На все действия, указанные выше, уходит 1-2 минуты. Но это может сэкономить солидную сумму. Кроме того, для покупок в Сети проще всего завести бесплатную виртуальную карту и проводить расчеты через нее. И не переводить на нее больше денег, чем вы собираетесь потратить на покупку.