ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРОФИЛАКТИКА ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ДЕРЖАТЕЛЕЙ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТ

В соответствии с п. 5 ст. 5 Закона Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. №99-З (далее – Закон), до получения согласия на обработку персональных данных субъекту персональных данных предоставляется следующая информация:

1. Оператор, получающий согласие субъекта персональных данных на обработку персональных данных.

2. Цели обработки персональных данных (например, банк, как правило, указывает в качестве цели принятие мер реагирования на поступившую информацию о противоправных действиях и информирование правоохранительных органов).

3. Перечень персональных данных, на обработку которых дается согласие субъектом персональных данных (например, фамилия, собственное имя, отчество (если таковое имеется);число, месяц, год рождения;номера контактных телефонов);

4. Срок, на который дается согласие субъекта персональных данных на обработку персональных данных.

5. Перечень действий с персональными данными, на совершение которых дается согласие субъекта персональных данных, общее описание используемых оператором способов обработки персональных данных.

Субъект персональных данных вправе:

в любое время без объяснения причин отозвать свое согласие на обработку своих персональных данных, посредством подачи оператору заявления в письменной форме либо в виде электронного документа, либо в форме, посредством которой получено его согласие;

бесплатно, за исключением случаев, предусмотренных законодательными актами, посредством подачи оператору заявления в письменной форме либо в виде электронного документа, получать информацию, касающуюся обработки своих персональных данных, содержащую:

наименование оператора персональных данных и его место нахождения;

подтверждение факта обработки персональных данных оператором;

перечень персональных данных и источник их получения;

правовые основания и цели обработки персональных данных;

срок, на который дано его согласие;

наименование и место нахождения уполномоченного лица, если обработка персональных данных поручена такому лицу;

иную информацию, предусмотренную законодательством. При этом субъект персональных данных не должен обосновывать свой интерес к запрашиваемой информации;

требовать от оператора внесения изменений в свои персональные данные в случае, если персональные данные являются неполными, устаревшими или неточными;

получать от оператора информацию, посредством подачи оператору заявления в письменной форме либо в виде электронного документа, о предоставлении своих персональных данных третьим лицам один раз в календарный год бесплатно, если иное не предусмотрено Законом и иными законодательными актами;

требовать от оператора, посредством подачи оператору заявления в письменной форме либо в виде электронного документа, бесплатного прекращения обработки своих персональных данных, включая их удаление, при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами;

обжаловать действия (бездействие) и решения оператора, нарушающие его права при обработке персональных данных, в уполномоченный орган по защите прав субъектов персональных данных в порядке, установленном законодательством об обращениях граждан и юридических лиц. Принятое уполномоченным органом по защите прав субъектов персональных данных решение может быть обжаловано субъектом персональных данных в суд в порядке, установленном законодательством.

1. Персональные данные в социальных сетях: важные правила безопасности

Неотъемлемым элементом нашей повседневной коммуникации становятся социальные сети и мессенджеры.

Вместе с позитивными изменениями соцсети и технологии больших данных способствуют возникновению нового общества наблюдения, которое создает угрозы конфиденциальности. В большинстве случаев условием получения интересующих услуг выступает указание своих персональных данных, предоставление согласия на их обработку, согласие с политиками конфиденциальности. Все это подвергается анализу и используется для самых разных целей.

Страницы в соцсетях, куда люди добровольно выкладывают личную информацию и фотографии, смотрят не только друзья (исключение – закрытый профиль).

Часто – это безграничный источник сведений для мошенников.

Приведём несколько примеров.

Фото из отпуска оповещают, что вас нет дома.

Хвалебные посты о дорогостоящих покупках сориентируют других на предмет Вашего финансового состояния.

Метка геолокации на фото в соцсети, сделанном по месту проживания, позволяет установить дом, в котором живёт лицо, опубликовавшее фотографию.

Размещая личный номер мобильного телефона или электронной почты в сетях, Вы рискуете получить шквал ненужных Вам звонков, сообщений, рассылок с рекламными предложениями, а можете попасться «на удочку» аферистов.

Предупрежден – значит вооружен. Напомним о базовых правилах безопасного оборота Ваших персональных данных в социальных сетях.

1. Читайте политику конфиденциальности соцсети. Важно знать, кто будет обрабатывать Ваши персональные данные, как хранить и использовать.

2. Делитесь сокровенными моментами своей жизни только с близкими, а для этого уделите внимание настройкам конфиденциальности в соцсетях, закройте страницы. В настройках профиля есть раздел «Приватность». В нём Вы можете ограничить круг тех, кто сможет писать вам сообщения, оставлять комментарии или видеть основную информацию Вашей страницы. Следуйте правилам безопасности, если Вы решили оставить профиль открытым и видимым для всех.

3. Установите в соцсетях и мессенджерах двухэтапный вариант проверки, который позволяет создать персонализированный PIN-код для большей безопасности от нарушений и хакеров.

4. Не публикуйте в открытом доступе избыточную информацию: адреса, номера телефонов, даты рождения. Это же касается и сведений о родных и близких, не публикуйте чужие фото и видео (даже совместные) и иную личную информацию без согласия на то человека. Вы просто не имеете на это права.

5. Не используйте геолокацию, когда размещаете в соцсетях фото дома, не отмечайте на нем адрес. Зачастую по умолчанию к каждому снимку, который Вы делаете, привязывается местоположение. Оно сохраняется в метаданных изображения. Функция вполне удобная: можно открыть карту и посмотреть, в каких местах Вы делали фотографии. Но зачем это знать посторонним людям?

6. Получили новый паспорт, водительское удостоверение? Не публикуйте фото с документами, где видны данные. Это же касается билетов на самолет.

7. Не пересылайте и не храните в соцсетях и мессенджерах документы, пароли, коды, реквизиты банковской карты и счетов. Это очень чувствительные данные.

8. Не рекомендуем входить и авторизироваться на сторонних сайтах через учетную запись соцсети. Не всегда перед входом можно проверить «надежность» ресурса, а это, в свою очередь, чревато тем, что доступ у управлениюстраницей могут перехватить.

9. Настройте уникальные и надежные пароли для всех своих учетных записей. Использование одних и тех же паролеймногократно увеличивает риск их взлома.

10. Используйте проверенные антивирусные службы и лицензионное ПО.

Помните, информация, размещенная в социальных сетях, остается там навсегда. Прежде чем публиковать очередной пост или что-то писать в комментариях, необходимо подумать, проверить и убедиться в необходимости такой публикации. И хотя всегда можно удалить нежелательные сообщения, Вы не знаете, кто собрал эту информацию и Ваши персональные данные раньше и что с этими данными намеревается делать, в том числе, возможно, использовать против Вас.

2. Рекомендации по противодействию мошенничеству с использованием социальной инженерии

Все большую популярность у мошенников в последнее время набирает социальная инженерия (метод получения доступа к информации, основанный на особенностях психологии людей). Основной целью социальной инженерии является получение доступа к конфиденциальной информации, персональным данным, данным карточек, паролям, банковским данным и другим защищенным системам с последующим осуществлением мошеннических операций. Обезопасить себя от мошенничества с применением социальной инженерии можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Ниже приведены самые распространенные мошеннические схемы.

Взлом.

Схема действий мошенников:

Злоумышленники взламывают страницы в социальных сетях и рассылают от имени владельца аккаунта фишинговые сообщения с просьбой от имени владельца странички занять или перевести некоторую сумму либо с целью выманивания реквизитов банковских платежных карточек, а также паролей для проведения в дальнейшем мошеннических операций.

Способы защиты:

при обращении родственников/друзей/знакомых через социальные сети с просьбами о помощи в переводе денежных средств на карточку/оплаты мобильной связи, билетов и т.д. убедитесь, что лицо, обратившееся через страницу социальной сети, является именно тем, за кого себя выдает;

наряду с номером и сроком действия карточки, логином и паролем от интернет-банкинга, паролем 3-D Secure и SMS-паролем (ключом), также не следует сообщать CVV2/CVC2-код (трехзначное число на обороте карточке), данный код используется исключительно для расходных операций и абсолютно не нужен для перевода денежных средств на Вашу карточку.

в случае, если Ваш аккаунт в социальных сетях был взломан, по возможности оповестите об этом подписчиков Вашей страницы и смените пароль.

Вишинг.

Схема действий мошенников:

Злоумышленники используют телефонные звонки с целью выманивания у держателей банковских платежных карточек личной информации, номера банковской платежной карточки, логина и пароля от систем дистанционного банковского обслуживания, SMS-кодов и другого. Мошенники могут представляться работниками банка или Службы сервиса клиентов ОАО «Банковский процессинговый центр», использовать скрытые телефонные номера или программы-анонимайзеры, подменяющие номера телефонов на реальные номера, размещенные на официальных ресурсах организаций.

Способы защиты:

важно помнить, что при звонке работники банков или Службы сервиса клиентов никогда не запрашивают информацию о полном номере банковской платежной карточки, сроке действия, CVC/CVV коде, пароле 3D Secure, одноразовых подтверждающих кодах. Ни под каким предлогом не сообщайте информацию о реквизитах банковской карточки, логинах и паролях, SMS-кодах, сеансовых ключах к Интернет-банкингу и мобильным приложениям!

в случае возникновения звонков с просьбами уточнить Ваши данные незамедлительно обратитесь в банк по номерам телефонов, указанным на официальном сайте.

Мошенничество при осуществлении сделок на интернет-площадках.

Схема действий мошенников:

Добросовестный продавец размещает информацию о продаже товара на общедоступной площадке. Чаще всего внимание мошенников

привлекают объявления о продаже дорогостоящего имущества (бытовая техника, мебель, автомобили). Мошенники под видом покупателей связываются с продавцом и просят предоставить им реквизиты банковской платежной карточки для осуществления предоплаты либо сами предоставляют мошенническую ссылку для перевода денежных средств. Используя полученную информацию (зачастую держатели карточек разглашают не только номер карты, но и CVV2/CVC2-код, а также пароли 3D Secure) злоумышленники переводят деньги с карточки жертвы на свои карточки (телефонные счета, электронные кошельки и пр.).

В другом случае добросовестный покупатель обращается к продавцу (мошеннику под видом продавца) по вопросу приобретения того или иного товара, после чего мошенники просят произвести предоплату путем перевода средств с карточки на карточку или электронный кошелек. Получив деньги, продавец перестает выходить на связь.

Способы защиты:

при покупке товаров и услуг у незнакомых людей или на интернет-площадках необходимо обращать внимание на форму оплаты, если с Вас требуют предоплату (частичную или полную), то есть основания предполагать, что Вы имеете дело с мошенником.

не следуйте просьбам перевести оплату за предоставляемые по привлекательной цене товар или услугу на банковскую пластиковую карточку продавца или его электронный кошелек. Если Вы это сделаете, то Вы не сможете доказать, что произвели оплату за несуществующий товар или сервис.

Сообщения о выигрыше ценных призов.

Схема действий мошенников:

Злоумышленники рассылают сообщения о выигрыше ценных призов и провоцируют потенциальную жертву перевести на счет некую сумму денег для получения «приза» или участия в розыгрыше и объясняют это тем, что ему нужно оплатить комиссию, таможенную пошлину, налоги либо транспортные расходы для доставки «выигрыша».

Способы защиты:

если Вы решили испытать удачу и связаться с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения.

помните, что упоминание вашего имени на интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией выигрыша. Необходимо задуматься над тем, принимали ли

Вы участие в розыгрыше призов, знакома ли Вам организация, направившая уведомление о выигрыше, откуда организаторам акции известны Ваши контактные данные? Если Вы не можете ответить хотя бы на один из этих вопросов, рекомендуем Вам проигнорировать поступившее сообщение.

любая просьба перевести денежные средства для получения выигрыша должна насторожить Вас.

помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или электронные кошельки.

Дополнительная информация о различных мошеннических схемах доступна по ссылке https://www.a1.by/ru/company/fraud-protection.

Материал подготовленна основе информации Национального центра защиты персональных данных Республики Беларусь,материалов официальных сайтов ОАО «АСБ Беларусбанк», ОАО «Банковский процессинговый центр», Унитарного предприятия по оказанию услуг «А1», государственных СМИ