Уважаемые клиенты, обратите внимание!

Система «Интернет-Банк» в терминах Федерального закона №161-ФЗ «О национальной платежной системе» является электронным средством платежа. Выполняя требования статьи 9 указанного закона, Банк «Снежинский» АО информирует вас о случаях повышенного риска при использовании электронного средства платежа. До заключения Договора присоединения просим вас внимательно ознакомиться с возможными угрозами при работе с СЭД (системой «Интернет-Банк»).

Актуальные угрозы при работе с системой «Интернет-Банк»

1. Угрозы, вызванные действиями злоумышленников

Злоумышленники могут получить доступ к компьютеру или мобильному устройству клиента, на котором установлена система «Интернет-Банк» (далее «Система»), и/или получить доступ к логину, паролю и набору сеансовых ключей, тем самым получить возможность управлять счетом клиента.

Злоумышленники могут способствовать заражению компьютера или мобильного устройства, используемого клиентом для обслуживания в Системе, вредоносным программным обеспечением (вирусами).

Зараженный вредоносным программным обеспечением компьютер подвержен следующим угрозам:

1.1. Хищение набора сеансовых ключей клиента, логина и пароля доступа к Системе клиента.

Злоумышленник, похитивший набор сеансовых ключей, логин и пароль доступа, может удаленно (со своего компьютера) создавать от имени клиента платежные документы, подтверждать их сеансовым ключом, отправлять такие документы в Банк. Документы будут восприниматься Банком как документы, подтвержденные клиентом.

1.2. Использование сайта-двойника.

Мошенники часто фабрикуют фишинговые сайты (сайты-двойники) для хищения логина и пароля и, как следствие, финансовой информации.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, в основном, логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем, СМС-сообщений от имени популярных брендов, банков, а также личных сообщений внутри различных сервисов или социальных сетей. Рассылаемые мошенниками массовые электронные письма, которые играют роль приманки, часто похожи на настоящие электронные сообщения, направляемые банками своим клиентам, однако их целью является заманить клиента на сайт-двойник, замаскированный под веб-сайт банка, и получить финансовую информацию и персональные данные (номер банковской карты, ПИН-код карты, CVV/CVC, логин и пароль для входу в системы дистанционного банковского обслуживания, почтовую систему). В дальнейшем полученная информация может быть использована мошенниками для хищения денежных средств со счета клиента.

Даже если вы просто перешли по полученной ссылке и не соглашались на передачу персональных данных, компьютер или мобильное устройство уже может быть заражено вредоносным программным обеспечением, которое будет перехватывать результат работы средств ввода (клавиатура, мышь) в момент инициализации входа в системы дистанционного банковского обслуживания и передавать мошенникам все необходимые для хищения денежных средств данные.

1.3. Блокирование доступа клиента в Систему.

Злоумышленник блокирует возможность доступа клиента к Системе одним из нескольких способов:

- выводит из строя компьютер или мобильное устройство клиента;
- блокирует выход в интернет;
- блокирует доступ к сайту Банка.

1.4. Подмена платежного документа при его передаче для подтверждения.

Злоумышленники могут внедрить в компьютер или мобильное устройство клиента троянскую программу, изменяющую в подготовленных к отправке платежных поручениях информацию (например, реквизиты получателя платежа, его расчетного счета, наименования банка получателя, суммы платежа). Пользователь видит на экране монитора одну информацию, а в Банк отправляется другая. Параллельно подменяются данные об остатках на счетах, выполненных транзакциях и т.д.

2. Угрозы, вызванные действиями/бездействием сотрудников клиента

- использование чужих компьютеров или иных устройств для работы с Системой;
- использование компьютера или мобильного устройства, используемого клиентом для обслуживания в Системе, для посещения интернет-сайтов, отличных от сайта Банка;
- сохранение пароля доступа к Системе на жестком диске или в реестре операционной системы;
- передача пароля доступа к Системе другому лицу.

3. Угрозы, вызванные сбоями в каналах связи

Отсутствие возможности для клиента связаться с Банком и Банку связаться с клиентом из-за сбоев в работе каналов связи.

4. Угрозы, вызванные сбоями в информационных системах Банка

Временная недоступность одного или нескольких сервисов, предоставляемых Банком.

При любых подозрениях на компрометацию набора сеансовых ключей, подозрении на использование Системы без вашего согласия незамедлительно обращайтесь в Единую справочную службу Банка:

тел. 8-800-755-05-05 (круглосуточно, звонок бесплатный).

Обращаем ваше внимание, что соблюдение «Требований Банка по информационной безопасности при обслуживании клиента с использованием системы «Интернет-Банк» и своевременное обращение в Банк при угрозе потери конфиденциальности ваших ключей могут существенно снизить угрозу мошенничества с вашими средствами с использованием Системы.