Приложение 2
К приказу № 144 от 01.09.2014г.

НОВОКИБ

ПАМЯТКА
ДЛЯ КЛИЕНТОВ

“О ЗАЩИТЕ ОТ SMS И E-MAIL МОШЕННИЧЕСТВА”

г. Новокузнецк

1. Мошенничество через SMS-рассылки

SMS-мошенничество является типичным примером использования методов социальной инженерии и основано на доверии клиентов к уведомлениям (SMS), направляемым банками на их мобильные телефоны. Похожие сообщения могут быть направлены и мошенниками, при этом в последнее время для большей убедительности мошенники стали рассылать SMS, маскирующиеся под сообщения от банков подписанные от имени его служб и содержащие телефонные номера, визуально схожие с официальными номерами банков.

Мошеннические SMS, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую Клиента перезвонить на указанный в SMS номер телефона для уточнения информации. Перезвонившему держателю карты мошенники представляются сотрудниками службы безопасности банка, специалистами службы технической поддержки или контактного центра и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п. в зависимости от содержания SMS. Для этого предлагается подойти к ближайшему банкомату и еще раз перезвонить на указанный в SMS номер телефона. Далее, слепо следуя получаемым по телефону инструкциям, люди сами переводят средства на электронные кошельки, банковские карты, телефоны мошенников или подключают свои банковские карты к услуге Мобильный банк на телефон, указанный мошенником, что позволяет ему самому перевести деньги с карты.

Получение держателем карты такого SMS не свидетельствует о «взломе» банковской системы, об утечке баз «карточных» клиентов и номеров их телефонов. Мошенники действуют наугад, и получают их сообщения, в том числе граждане, вообще не имеющие банковских карт.

Как отличить мошенническое SMS от сообщения, действительно направленного банком, и предотвратить возможные убытки, если Вы всё же перезвонили мошенникам?

Вот несколько советов:

1. Изначально мошенники не знают, какая карта и какого банка есть у клиента, сколько на ней средств. Все это они пытаются узнать, задавая умело сформулированные вопросы. Ни в коем случае не сообщайте им информацию о своей карте.

2. Если все же полученное SMS вызывает любые сомнения или тревогу, необходимо сразу позвонить в банк по официальным телефонам, номера которых размещены на оборотной стороне карты ООО «НОВОКИБ» или на интернет-сайте www.novokib.ru.

В случае если Вы все же пострадали от SMS-мошенничества, необходимо:

1. Немедленно обратиться в банк по официальному телефону и заблокировать карту, реквизиты которой были сообщены мошенникам или по которой были совершены мошеннические операции;

2. Немедленно обратиться по телефону к оператору связи, в адрес которого переведены средства, с заявлением о мошенничестве и возврате средств (как правило, информация о номерах телефонах, на которые были переведены средства, сотовом операторе и телефоны контактного центра сотового оператора указаны на чеке, полученном в банкомате);

2. Мошенничество через email-рассылки

Мошенники проводят массовые email-рассылки, маскируясь под бренды банков, целями которых может быть:

– заманивание получателей сообщений на сайты-ловушки, на которых под различными предлогами мошенники попытаются получить персональные данные (идентификатор и пароль для входа в Иинтернет-банк, кодовые слова банковских карт, номера банковских карт, ПИН-коды, и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц.

– принуждение под различными предлогами получателей писем на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла.

Признаки того, что email-сообщение является мошенническим:

– сообщения замаскированы под официальные письма банка и требуют от Вас каких-либо быстрых действий или ответа;

– адрес отправителя и тема сообщения замаскированы под обращения от имени банка.