Как СМС-мошенники крадут ваши деньги и личные данные.

Каждому обладателю мобильного телефона периодически приходят СМСки от мошенников. Чаще всего люди рискуют своими деньгами из-за невнимательности, доверчивости, отсутствия информации и забывчивости. **Банк предупреждает своих Клиентов, будьте внимательны!** Приведем примеры самых изощренных уловок СМС-охотников за деньгами.

"Вам отказали в кредите". И через пару дней спустя людям приходит напоминание о сроках погашения кредита и пугающая сумма. Вспомнив о прошлой СМС, человек старается быстрее перезвонить по указанному номеру для уточнения деталей, который оказывается платным.

"Узнайте, где человек, по номеру телефона". Для получения услуги нужно отправить желаемый номер, со счета спишут определенную сумму, а в ответ должна прийти геолокация.

"Пришли денег, потом объясню". Пишут, как правило, с незнакомого номера со слезной просьбой пополнить баланс.

"Верните деньги, отправил по ошибке". Перед этим приходит СМС с номера, похожего на ваш онлайн-банк или любую платежную систему, например, QIWI-кошелек. Пример:

"Вы получили наследство". Как вариант, выиграли в лотерею или автомобиль. Чтобы получить заветное вознаграждение, предлагают сообщить паспортные данные, реквизиты карты, которые мошенники используют в личных целях.

"Ваша карта заблокирована". Тут же указан номер, на который можно перезвонить для уточнения деталей. На звонок отвечает "специалист", уточняющий данные вплоть до пин-кода вашей карты.

"Смените тариф на более выгодный". Со счета либо списывают средства, либо вам подключат "медвежью" услугу с ежемесячным платежом. По такой же схеме действуют при рассылке сообщений *"Вас приглашают на собеседование", "Привет, давай познакомимся", "Отпишитесь от спама"*.

"Действие услуги заканчивается. Она будет продлена автоматически. Подробности в личном кабинете". В конце СМС дана ссылка на зараженный вирусом ресурс, который поражает телефон и позволяет злоумышленникам получить доступ к личным данным. Такая же история с сообщениями *"Хорошо отдохнули, фотки тут ссылка"*.

"Сбой в Сети. Ваша SIM-карта будет заблокирована". Для отмены предлагается срочно перерегистрировать симку, набрав комбинацию цифр, перейдя по ссылке или перезвонив "оператору".

Банк рекомендует своим Клиентам – не реагировать (не отвечать, не перезванивать, не переходить по сомнительным ссылкам). Нужно быть очень внимательным, помнить или внести в список контактов номера вашего оператора связи и банка. Ваш СКБ-Банк. Контактный телефон: 8-800-100-600.