СКБ-БАНК

Мошенничество:
социальная инженерия и угрозы фишинга.
Меры предосторожности

2016

Причины возникновения угроз

Развитие рынка интернет-банкинга постоянно находится под пристальным вниманием кибермошенников.

Востребованность услуг и внедрение новых технологий в данном сегменте обслуживания банкоматов, терминалов, платежных средств, развития и создание комфортного использования дистанционных каналов связи, в том числе мобильных приложений в используемых Смартфонах сопровождается совершенствованием мошеннических схем и появлением их новых разновидностей.

Для завладения денежными средствами владельцев банковских карт мошенникам **необходимо выманить** у потенциальной жертвы конфиденциальную информацию, позволяющие проводить операции по карточному счету.

Реализации всему этому способствует развитие такого направления мошенничества как **социальная инженерия**.

Социальная инженерия и фишинг

Социальная инженерия

- метод управления действиями человека без использования специальных технических средств.
- При этом злоумышленники используют навыки убеждения с целью получения нужной информации или пробуждают интерес потенциальной жертвы к совершению действий, необходимых мошенникам.
- В своем арсенале злоумышленники используют рассылку по e-mail, sms-сообщения, либо звонят на телефон Клиента, представляясь сотрудником обслуживающего его Банка.

Фишинг (Phishing) – вид социальной инженерии

- Завладение обманным путем сведениями о банковских картах и персональными данными клиентов Банка с использованием поддельных сайтов в сети Интернет.
- Предварительно к потенциальной жертве злоумышленники применяют инструменты социальной инженерии.
- **Вишинг** (Voice Phishing) — вид телефонного мошенничества, позволяющий красть у клиентов банков конфиденциальную информацию. Клиент получает звонок от автоинформатора, который сообщает, что с картой, например, производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Далее, следуя инструкциям, клиент должен сообщить или ввести на телефонной клавиатуре реквизиты карты. Иногда злоумышленники сами звонят жертвам, убеждая, что являются сотрудниками банка.
- **Фарминг** – в этом случае используются механизм скрытого перенаправления пользователей на фишинговые сайты.

Среда взаимодействия

Источники угроз	Получаемая информация
СОЦИАЛЬНЫЕ СЕТИ И ИНТЕРНЕТ-ОПРОСЫ **Одноклассники, facebook, Вконтакте …где клиенту предлагается привязать карту для автоматической оплаты услуг и покупок.** **Опросники на острые социальные темы, где между делом клиенту предлагается заполнить поля, касающиеся его персональных данных. Под видом формы обратной связи клиенту предлагается указать свой контактный номер телефона.**	**Персональная информация о клиенте: ФИО, адрес, дата рождения, № телефона, состав семьи, место учебы и работы, круг общения и т.д.**
АВТОПЛАТЕЖИ	**№ карты клиента, привязанный к аккаунту, с которой будут осуществляются платежи, SVV код, срок действия карты, ФИО клиента.**
АКЦИИ И РАСПРОДАЖИ	**№ банковской карты клиента, SVV код, срок действия карты, ФИО клиента, № телефона**
МАССОВАЯ РАССЫЛКА СООБЩЕНИЙ РЕКЛАМНОГО ХАРАКТЕРА	**Заражение компьютера вредоносными программами. Вредоносный код автоматически отправляет мошенникам персональные данные и данные карты без ведома пользователя.**
ЧЕК БАНКОМАТА **Обрывочная, но читаемая информация из чеков, выданных банкоматом после проведения расходной операции**	**Неполный номер карты, сумма, дата и место совершения последней операции, остаток на счете, фамилия и имя клиента**

Пресечение и профилактика

Технологические способы защиты

Наличие на компьютере клиента регулярно обновляемого антивирусного программного обеспечения;

Использование технологии антиспам (фильтр ненужных сообщений и возможность избежать засорения электронного ящика бесполезными письмами).

Использование современных версий интернет-браузеров, обладающих технологией «антифишинг».

По любым вопросам, связанными с картой, обращайтесь только в обслуживающий Вас банк (номера телефонов указаны на Вашей банковской карте).

Помните! Банки в телефонном режиме не запрашивают и не уточняют у своих клиентов реквизиты предоставленных им карт.

СПАСИБО ЗА ВНИМАНИЕ!
ОАО «СКБ-Банк»