- Обновлено 07.08.2020 12:24
Опубликовано 07.08.2020 12:22
Автор: ОПРИиОС
Просмотров: 623

Ранее мы неоднократно сообщали о фактах хищения денег у держателей платежных карт. Речь идет о вишинге – одном из видов мошенничества с использованием социальной инженерии.

Ранее мы неоднократно сообщали о фактах хищения денег у держателей платежных карт. Речь идет о так называемом вишинге – одном из видов мошенничества с использованием социальной инженерии.

Представляясь сотрудниками контакт-центра или специалистами по безопасности банков, злоумышленники звонят клиентам таких учреждений. Последним они сообщают о совершенном в отношении них мошенничестве и под различными предлогами просят предоставить реквизиты платежных карт. А заполучив необходимые данные – похищают деньги.

– Во время звонка они могут сообщить, что в отношении счета клиента происходят мошеннические действия. Чтобы не допустить перевода средств либо их обналичивания в банкомате, запрашивают данные БПК и другие персональные сведения. Среди распространенных сценариев аферистов – уведомление от имени банка о якобы ошибочно оформленной заявке на кредит, зачислении перевода или списании денег со счета, – рассказали в управлении «К» МВД.

Борцы с киберпреступностью обращают внимание, что злоумышленники нередко используют программы-анонимайзеры. В таком случае номера телефонов, с которых осуществляются звонки, определяются как официальные, указанные на сайте банка. Также аферисты могут подменить официальный номер не целиком, а лишь одну его цифру, и визуально этот подлог не столь незаметен.

Для большей правдоподобности в качестве шумового фона во время телефонного разговора используется имитация звуков работающего контакт-центра.

В управлении «К» МВД отмечают: сотрудник банка при звонке клиенту ни при каких обстоятельствах не потребуют реквизитов банковских карт или иной конфиденциальной информации. Просьба незнакомого абонента о предоставлении таких сведений свидетельствует о том, что разговор ведется с мошенником!

В этом случае немедленно завершите разговор и обратитесь в контакт-центр банка, эмитировавшего карточку, расскажите о ситуации и далее следуйте рекомендациям представителя учреждения.

Если злоумышленнику все же удалось получить реквизиты БПК или был установлен факт хищения денежных средств, незамедлительно заблокируйте карточку (номер телефона указан на обороте карты) и обратитесь с заявлением в правоохранительные органы.

Помните, если хищение произошло по причине передачи потерпевшим реквизитов своей БПК либо данных, полученных в SMS, третьим лицам, банки могут отказать в возврате денежных средств.

Посмотрите и послушайте, как мошенник пытается выманить персональные данные у жертвы.

leILayURehY |Разговор с мошенником||t_width=250, t_height=150, pages=1, break=0, lightbox=0, button=1

ПРОФИЛАКТИКА

- ни под каким предлогом не передавайте и не сообщайте платежные реквизиты, полный номер карточки и срок ее действия, логин и пароль к интернет-банку, иную персональную информацию;
- не вступайте в переговоры с незнакомцем. Положите трубку и самостоятельно обратитесь в банк по номерам, указанным на официальном сайте;
- применяйте все доступные способы защиты, предлагаемые банками (двухфакторная авторизация, смс-оповещение о расходных операциях, лимит снятия денежных средств и др.);
- используйте сложные пароли доступа к учетным записям электронной почты, к системам «интернет-банкинг», социальным сетям и другим интернет-сервисам;
- не открывайте электронные почтовые сообщения, полученные от неизвестных отправителей и не запускайте их содержимое;
- не переходите по неизвестным ссылкам и не посещайте интернет-ресурсы сомнительного содержания;
- при посещении интернет-сайтов обращайте внимание на веб-адрес интернет-ресурса;
- в случае утери или кражи карты необходимо незамедлительно заблокировать ее по телефону, или обратиться в банк;
- ни под каким предлогом не отправляйте реквизиты карты фотоизображения по сети Интернет;
- не сообщайте данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Secure» и т.д.;
- при обнаружении несанкционированного списания денежных средств с карт-счета незамедлительно обратитесь с заявлением в банк для их возврата по принципу «нулевой ответственности».

По информации сайта МВД