ВИШИНГ

Вишинг *— метод мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой.*

Основные правила защиты:

- остерегайтесь неожиданных звонков с незнакомых номеров

ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте.

- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы
- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.

Запомните! Сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен.

ФИШИНГ

Фишинг *— вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации.*

Основные правила защиты:

- избегайте перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки с «потенциальным покупателем» якобы для получения предоплаты или оформления доставки;
- ни в коем случает не устанавливайте на мобильный телефон приложения по просьбе «сотрудников банка»;
- очень внимательно относитесь к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты
- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);
- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);
- используйте наиболее современную версию антивирусного программного обеспечения;

Будьте особо бдительны, если в письме от имени банка у Вас запрашивают конфиденциальную информацию.