**Как работают мошенники?**



Что нельзя говорить незнакомцам по телефону? Предлагаем разобраться в новых схемах мошенников и познакомиться с основами личной финансовой безопасности. Вишинг – это один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную связь и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя банковской платежной карточки конфиденциальную информацию или стимулируют к совершению определенных действий с карточным счетом/платежной карточкой с целью хищения денежных средств. Злоумышленники звонят клиентам банков и, представляясь сотрудниками банков (могут представится сотрудником Национального банка), под различными предлогами просят предоставить паспортные данные, а также реквизиты банковских платежных карточек и коды, поступающие на телефонный номер человека. В большинстве случаев номера телефонов звонящих могут быть скрыты либо принадлежать операторам связи других государств. Однако в отдельных случаях мошенниками используются программы-анонимайзеры, IP-телефония. При этом номера телефонов, с которых осуществляются звонки, определяются как официальные номера, указанные на сайте банка. Обращаем внимание на то, что сотрудник банка при звонке клиенту заранее должен знать все необходимые ему данные. Поэтому сообщать кому-то реквизиты своей банковской платежной карточки, пароли и коды доступа, паспортные данные ни в коем случае нельзя. Национальный банк рекомендует в случае поступления подобных звонков сразу же обратиться в контакт-центр банка, выпустившего карточку, рассказать о ситуации и далее следовать рекомендациям сотрудника банка. Если злоумышленнику все же удалось получить реквизиты карточки или был установлен факт хищения денежных средств, следует незамедлительно заблокировать карточку и обратиться с заявлением в правоохранительные органы.