



РЕКОМЕНДУЕТ ПРЕДПРИНЯТЬ РЯД МЕР, КОТОРЫЕ ПОМОГУТ НЕ СТАТЬ ЖЕРТВОЙ ПРЕСТУПЛЕНИЯ:

- Устанавливайте на мобильных устройствах и персональных компьютерах **лицензионное антивирусное программное обеспечение** и регулярно его обновляйте.

- Скачивайте и устанавливайте приложения, программы, а также обновления к ним только **из проверенных источников.**

- Для авторизации, управления счетом и совершения операций с мобильных устройств **используйте официальные приложения**, предоставляемые банками.

- **Не посещайте сомнительные ссылки в сети Интернет** и не открывайте сообщения от незнакомых пользователей и абонентов, не переходите по ссылкам, содержащимся в письмах, а так же в СМС, ММС - сообщениях, сообщениях мобильных мессенджеров, не открывайте вложения, прикрепленные к таким сообщениям

- При смене, либо утере абонентского номера, незамедлительно, в банке, выдавшем карту, **отключайте услугу «Мобильный банк»** от старого номера телефона.

- **Совершайте покупки в сети Интернет только в проверенных магазинах.** Для осуществления таких покупок откройте отдельную банковскую карту, либо электронный кошелек

- Никогда и ни при каких обстоятельствах **не сообщайте никому своих персональных данных** или конфиденциальной информации (любые данные банковской карты, логин и пароль от страниц в социальных сетях и т.д.).

- Прежде чем реагировать на сообщения или звонки от «родственников» или «друзей», **попытайтесь дозвониться человеку, от имени которого пришло сообщение**, кому-то из его близких, с которыми он в настоящее время может находиться.

- **Задавайте вопросы.** Если звонящий представляется как сотрудник полиции, банка, доктор поликлиники, страховой агент, первое, что нужно сделать - попытаться узнать информацию о собеседнике. Простые вопросы, например, фамилия и должность звонящего, из какого отделения полиции, банка или страхового агентства звонят, контактные данные руководителя организации и прочее настоящего сотрудника не смутят, а мошенников заставят занервничать.

