Меры безопасности, чтобы не стать жертвой мошенников

1. Не сообщайте никому свои финансовые сведения: номер банковской карты, ФИО владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и других сайтах в интернете. Не храните данные карт и PIN-коды на компьютере или в смартфоне.

2. Не перезванивайте на номер, с которого пришло СМС о том, что банковская карта заблокирована и не отправляйте ответных СМС. Позвоните в банк, выпустивший и обслуживающий карту. Телефон указан на обороте банковской карты.

3. Не доверяйте СМС о крупном выигрыше, победе в конкурсе или лотерее, особенно в тех случаях, когда для получения выигрыша просят оплатить налог. Настоящий розыгрыш призов не подразумевает денежные выплаты с вашей стороны.

4. Не отправляйте денежные средства на неизвестные адреса, в том числе с целью приобретения вещей в интернете.

5. Кладите трубку, если вам звонят с неизвестных номеров и представляются сотрудниками банка, полиции, ФСБ. Официальные органы при необходимости всегда присылают повестку. А с банком можно связаться через горячую линию - перезвоните сами и выясните, действительно ли вам звонил менеджер.

6. Если купили новую сим-карту, сразу обновите информацию по всем аккаунтам, к которым был привязан старый номер. Так мошенники не смогут зайти по нему в ваши аккаунты.

7. Если пришло сообщение или поступил звонок с просьбой денег якобы от начальника, родственника, знакомого, самостоятельно свяжитесь с ним по другому номеру, чтобы уточнить ситуацию.
Придумайте проверочное слово или фразу, которую знают только члены вашей семьи. Это поможет в случае необходимости подтвердить легитимность общения и идентифицировать в разговоре.

8. Установите специальное приложение, которое идентифицирует звонки и сообщения от незнакомых номеров или с адресов. Такие приложения обычно блокируют подозрительные звонки и сообщения, предотвращая возможные мошеннические атаки.

9. Регулярно проверяйте активные сессии в своих мессенджерах и социальных сетях. Если обнаружите активные сеансы на неизвестных устройствах или в местах, немедленно отключите их и меняйте пароли на новые.