В этой памятке говорится

о важной проблеме, с которой встречаются в современном мире очень многие люди. Это пользователи всевозможных сотовых телефонов. В наш век уже не представляешь себя без них. Вводим данные, проводим через это устройство по сети интернет информацию, финансовые операции. Мошенники не дремлют, разрабатывая бесконечные схемы обмана.

Какие же они схемы мошенничества?

Расскажем о самых распространенных.

1. «Ваша карта заблокирована» (СМС-сообщение о якобы заблокированной банковской карте, для разблокировки которой требуется сообщить ПИН-код Вашей карты либо произвести определенные действия с помощью банкомата).

2. «Хищение денежных средств по телефону» (на номер приходит СМС с просьбой перезвонить и подробным объяснением причины для звонка при перезвоне. Вас очень долго держат на телефоне.

3. «Проверка служебной банковской безопасности» (на номер телефона поступает звонок, якобы от отдела безопасности банка. В разговоре просят сообщить данные о карте для прохождения проверки и при этом угрожают блокировкой карты.

4. «Ложный покупатель» (т.е люди, которые пользуются услугами торговых площадок в зоне риска. На номер телефона поступает звонок от мошенника покупателю, который просит предоставить данные карты для перечисления денег).

5. «Родственник в беде» (требование крупной суммы денег для решения проблемы с якобы попавшим в беду родственником).

6. «Неожиданное списание средств» (через мессенджер пришло сообщение о списании средств с Вашей карты. Банки пользуются СМС.

7. «Работы на линии» (мошенник просит ввести Вас на своем телефоне какие-либо цифры, якобы для настройки).

8. «Вы выиграли» (смс-сообщение о том, что Вы стали победителем и Вам приз).

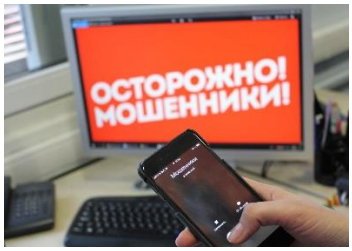
9. «Вирусная атака» (смс-сообщение со ссылкой на какой-либо ресурс, содержащий вредоносную программу, дающую быстрый доступ к Вашей банковской карте).

10. «Ошибочный перевод средств» (Вас просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства по чеку).

11. «Предоплата за товар на сайте» (в социальных сетях, на сайтах доверчивым покупателям предлагают внести предоплату за несуществующий товар, однако в дальнейшем связь с лжепродавцом прекращается).

12. «Вам начислена компенсация» (Вам якобы положена компенсация за приобретенные раннее БАДы и др.).

13. «Просьба о помощи» (на телефон приходит СМС-сообщение с незнакомого номера с просьбой перевести деньги не на обычный номер, а на тот, с которого пришла СМС либо на указанные карты и т.д. При этом используются стандартные обращения: папа, мама, брат, сестра и т.д.).



Правила безопасности

1. Не паниковать, когда Вам сообщат какую-либо информацию!

2. Проверить поступившую информацию (перезвонить в структуры, из которых якобы поступил звонок).

3. Не передавать мошенникам личные номера карт, не перезванивать на незнакомые номера.

4. Не верить ни в какие призы, тем более если Вы нигде не участвовали.

5. При покупке в сети интернет, пользоваться только проверенными сайтами, по возможности не вносить предоплату.

6. Завести отдельную, виртуальную карту для покупок в сети интернет.

Будьте внимательны и бдительны!