

## Памятка по безопасности в сети

**В большинстве случаев мошенники:**

- представляются сотрудниками банков, правоохранительных органов или иных организаций и предлагают отменить подозрительную операцию, заявку на кредит, либо под предлогом участия в специальном расследовании оформить кредит для выявления недобросовестных работников банка;
- под видом покупателей товара, реализуемого на интернет-площадках, выманивают реквизиты карт через мессенджеры или копии известных сайтов (Куфар, Европочта, Белпочта, СДЭК, интернет-банк и др.);
- предлагают в сети интернет, социальных сетях быстрый заработок или выгодные вложения без заключения договора или через сомнительные интернет-площадки

Ознакомьтесь с постером, чтобы не попасться на уловки мошенников. ➔

## КАК ЗАЩИТИТЬ СЕБЯ И СВОИ ДАННЫЕ



- 1 НЕ ПЕРЕДАВАЙТЕ НИКОМУ СВОИ КОДЫ И ПАРОЛИ!**
  - Храните в тайне номер карточки, CVC и ПИН-коды
  - Не вводите данные своей банковской платёжной карты на сомнительных интернет-ресурсах
  - Заверните карту для оплаты платежей в интернете
- 2 НЕ УСТАНАВЛИВАЙТЕ НЕИЗВЕСТНЫХ ПРИЛОЖЕНИЙ НА ТЕЛЕФОН!**
  - Загружайте приложения из проверенных источников
  - Не устанавливайте программы по просьбе незнакомцев
  - Используйте последние версии программ
- 3 ПРОВЕРЯЙТЕ АДРЕСА САЙТОВ, НА КОТОРЫЕ ПЕРЕХОДИТЕ!**
  - Проверяйте адресную строку сайта
  - Не переходите по ссылкам из сообщений от незнакомых адресатов
  - Не платите через небезопасные страницы
  - Не отвечайте на подозрительные письма
- 4 УСТАНАВЛИВАЙТЕ ЛИМИТ НА КАРТАХ!**
  - Не используйте одну и ту же карту для всех платежей
  - Не переводите денежные средства на счета незнакомых лиц
  - Не перезванивайте и не отвечайте на SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту
- 5 МЕНЯЙТЕ ПАРОЛИ, ВКЛЮЧАЙТЕ ДВУХФАКТОРНУЮ АВТОРИЗАЦИЮ!**
  - Не используйте один пароль для всех интернет-ресурсов
  - Используйте сложные пароли
  - Меняйте пароли периодически
  - Включайте двухфакторную авторизацию
- 6 ПРИ ПОДОЗРИТЕЛЬНЫХ ЗВОНКАХ И ПОПЫТКАХ ВЫЯСНИТЬ ВАШИ ЛИЧНЫЕ ДАННЫЕ – ЗАВЕРШАЙТЕ РАЗГОВОР!**
  - Насторожьтесь, если требуют немедленных действий
  - Не размещайте в открытом доступе и не передавайте информацию личного характера
  - При получении сомнительного sms от друга - перезвоните ему лично

**БУДЬТЕ БДИТЕЛЬНЫ!  
НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!**