**Онлайн:**

1. В соцсетях или чатах предлагают инвестировать в зарубежные фонды и приглашать в проект новых участников? Не торопитесь – это может быть финансовая пирамида – вы и ваши друзья потеряете деньги. Проверьте организацию на cbr.ru
2. Вам гарантируют огромный заработок на валютном рынке? Не верьте мошенникам – гарантия доходности на финансовом рынке запрещена законом.
3. В соцсетях приходит сообщение от давнего знакомого с просьбой перевести деньги на счет до зарплаты? Возможно, мошенники взломали его страницу. Позвоните другу и уточните, что случилось.

**СМС-информирование:**

1. Мошенники могут рассылать СМС о якобы неоплаченном штрафе, аресте имущества или блокировке счета. Не переходите по неизвестным ссылкам из СМС. Для уточнения позвоните в организацию по телефону, указанному на официальном сайте.
2. Вам приходит СМС с предложением получить компенсацию или неожиданный выигрыш с просьбой перейти по ссылке? Таким образом злоумышленники могут похитить ваши данные. Не переходите по ссылкам от неизвестных отправителей.

**Звонки:**

1. Если звонят якобы из банка и под любым предлогом просят назвать ваши личные данные, положите трубку, наберите номер вручную, указанный на обороте карты или на сайте банка, и уточните информацию.
2. Вам звонят с неизвестного номера и сообщают, что близкие люди попали в беду и нужно срочно перевести деньги? Это могут быть мошенники. Положите трубку и перезвоните родным сами.
3. Если вам звонят с предложением получить социальную выплату и просят перевести за нее налог, положите трубку. Это мошенники. Обо всех компенсациях и мерах поддержки читайте на официальных сайтах органов власти.
4. Вам звонят из банка и сообщают о подозрительном переводе денег с вашего счета или карты? Вам действительно могут позвонить, если обнаружат сомнительную операцию по вашему счету, чтобы убедиться, что ее действительно совершаете вы. Но банк никогда не будет запрашивать данные карты или пароли из СМС. ​

**Дополнительно о подозрительных переводах, звонок из СББ, пароль онлайн-банкинга.**

1. Помните, вам никогда не будут звонить из службы безопасности банка с просьбой сообщить пароль из смс или трехзначный код с обратной стороны карты. Если такое происходит, положите трубку, это – мошенники.
2. Вам звонят из банка и сообщают о подозрительном переводе денег с вашего счета или карты? Положите трубку и перезвоните в банк самостоятельно, набрав номер вручную.
3. Звонят от имени государственных органов или банка и сообщают о выплате компенсации? Предлагают подключить онлайн-доступ к любым банковским услугам? При этом просят назвать номер, срок действия вашей банковской карты и код с ее оборота? Так действуют только мошенники - повесьте трубку.
4. Пришло письмо или СМС, предлагающие вакцинацию от коронавируса без очереди? Не открывайте вложения, не переходите по ссылкам из сообщения. Они активируют вредоносный код, открывающий доступ к вашему банковскому счету.
5. Получили СМС с требованием оплатить штраф за нарушение ограничительных мер, отправив деньги на чью-то карту? Вас обманывают: частное лицо получателем штрафа быть не может. Сохраняйте голову холодной – это сбережет нервы. И деньги.