

ВНИМАНИЕ МОШЕННИКИ!!!

Следует соблюдать меры, направленные на противодействие хищению денежных средств:

1. Не переходить ни под каким предлогом, в том числе для оплаты, для получения возврата денежных средств, бонусов, кэшбэка и т.д. по ссылке, полученной в сообщении от неизвестного лица, с которым лично не знакомы, нужно ввести адрес сайта в браузере вручную.
2. Нужно знать настоящее название сайта, его запомнить, после чего при работе с разными сайтами внимательно смотреть на соответствие настоящему названию. Чтобы знать оригинальные названия сайтов, следует при большом их количестве выписать на листок, который использовать для сравнения названия сайта, перед тем как ввести свой логин и пароль, иную конфиденциальную информацию.
3. Не нажимать на появившиеся всплывающие окна с рекламой, на крестик с целью закрытия, так как указанные окна могут содержать вирус, рекомендуется закрыть браузер.
4. Оплачивать товары и услуги онлайн только на проверенных ресурсах, только лицам, с которыми лично знакомы, не переводить онлайн переводом крупные суммы денежных средств!
5. Если нашли мошеннические объявления на крупной платформе, рассказать об этом администрации сервиса.
6. Использовать надежную защиту, которая заблокирует фишинг или мошеннический сайт, при попытке на него перейти
7. В случае сообщения Вам информации по телефону о блокировке банковской карты, либо получения СМС-сообщения о ее блокировке, нужно звонить по соответствующему телефону Банка, указанному на официальном сайте, а не перезванивать по номерам, указанным в СМС-сообщении.
8. Запомнить, что Банки осведомляют клиентов об отсутствии необходимости в совершении операций по инструкциям звонящего, так как все операции для защиты сотрудник банка выполняет самостоятельно, а такие данные, как коды безопасности с оборотной стороны карты (CVV/CVC), логин, коды из СМС, номер банковской карты, сотрудник Банка самостоятельно просить не будет!
9. Следует помнить, что ни сотрудники Банка, ни другие третьи лица не могут запрашивать важную конфиденциальную информацию по телефону, в связи с чем звонки с соответствующей просьбой вероятнее всего являются мошенническими.
10. Идеальным способом защиты при телефонном мошенничестве выступает прекращение разговора с собеседником, личность которого вызывает подозрение.