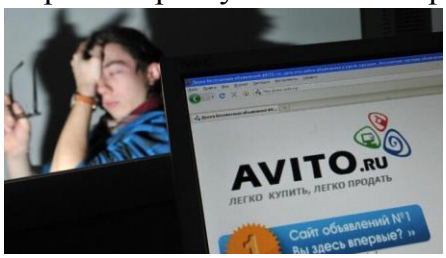
Схемы мошенничества появляются постоянно, а уже существующие совершенствуются новыми методами воздействия на человека. Аферисты используют «свежие» способы воровства на онлайн-сервисах «Авито», «Циан», «Домофонд», «Юла» и других. На «крючок» регулярно попадают клиенты российских банков и лица, активно использующие в своей деятельности сотовые телефоны. Как не стать жертвой преступников и сохранить свои деньги?




Сервисы объявлений пытаются обезопасить своих пользователей от мошенничеств. «Юла» ввела видео-звонки и прямую связь через приложение, а «Авито» свою доставку, чтобы товар без проблем пришел к покупателю. Продавец получает деньги только тогда, когда покупатель забирает вещь из пункта выдачи и подтверждает ее заявленные характеристики. Но и тут мошенники разработали свой способ завладеть чужими средствами.

При совершении покупки непосредственно через «Авито», обратите внимание на то, что продавец может предложить вам выслать платежку. Мошенник отправляет ссылку на оплату товара, вы вводите данные карты, оплачиваете, а преступник блокирует вас и пропадает. Жертва переходит по полученной ссылке на специальный сайт, похожий на «Авито», но это подделка! Такие сайты-двойники существуют не только у онлайн-платформ, но и у официальных ведомств России.

Все владельцы банковских карт давно знают, что сотрудник банка не имеет право спрашивать пароль от карты и уж тем более, его нельзя никому сообщать. Наверняка, вам поступали звонки от якобы менеджера банка с просьбой предоставить информацию и пароль для того, чтобы предотвратить подозрительное движение средств на счету. Чтобы не стать жертвой этой аферы, достаточно повесить трубку и перезвонить в банковскую организацию по телефону, указанному на официальном сайте или на обороте карты. Уточните у оператора, действительно ли кто-то пытается снять деньги, и сообщите номер телефона мошенников.

Взлом онлайн-банка через приложения банков на телефонах крайне удобное изобретение и кажется, что финансовые организации делают все, чтобы обезопасить своих клиентов, но мошенники нашли их уязвимые места. Мошенники ищут объявления продавцов на таких площадках, как «Авито», «Циан», «Юла» и другие, а потом отправляют SMS с предложением обмена товара и прикрепляют ссылку.


При переходе по ссылке, на ваш телефон скачивается стороннее приложение, которое получает доступ к вашим онлайн-банкам и выводит денежные средства со счетов. Крайне не рекомендуется открывать эти ПО, лучше сразу удалить их и установить антивирус.