

Мошенники выдают себя за службы доставки.

Новая схема мошенничества: поддельные уведомления от служб доставки. Злоумышленники начали притворяться популярными сервисами доставки, чтобы получить доступ к вашим личным данным и украсть деньги со счетов.

Сначала вы получаете ложное сообщение о том, что ваш заказ готов к отправке, хотя вы ничего не заказывали.

В последующем приходит смс-сообщение с предложением отследить посылку, чтобы узнать детали отправления. В данном сообщении находится ссылка на интернет-ресурс.

Не спешите переходить по ссылке из сообщения, поскольку ссылка ведет на фишинговый сайт, который очень похож на официальный сайт служб доставки (СДЭК, Яндекс Доставка, СберМаркет и др.).

Однако, если вы перейдете по ссылке, вас обяжут ввести номер банковской карты, паспортные данные либо логин и пароль банковского приложения.

Получив такие данные, мошенники списывают все ваши деньги со счета на банковские счета дропперов.

Не переходите по подозрительным ссылкам из сообщений, особенно если вы не ожидаете доставок.

Проверяйте отправителя сообщений, убедитесь, что сообщение пришло с официального номера или аккаунта службы доставки.

Не вводите личные данные на сайтах, перешедших по ссылкам из сообщений.

Если у вас есть сомнения, позвоните в службу поддержки официального сервиса доставки либо воспользуйтесь личным кабинетом в официальном приложении или на сайте службы доставки.

В условиях роста подобных преступлений в отношении граждан будьте бдительны и предупреждайте своих близких о новых видах мошенничества!