

Приложение
к письму начальника
департамента образования
от 20.06.2022 № 44/15/09579



ПРОКУРАТУРА Г. НОВОСИБИРСКА РАЗЪЯСНЯЕТ

В последнее время участились случаи мошенничества в сети «Интернет». Наиболее распространенными способами являются следующие:

Способ №1. Фейковые СМС от банка. Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце сообщения указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит и попадает в руки злоумышленника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки.

Способ №2. Звонки от сотрудников банка. Злоумышленники звонят Вам и представляются сотрудниками банка, сообщая о несанкционированном списании денежных средств с Вашего счета, при этом просят сообщить им реквизиты банковской карты. Доверчивое лицо выполняет просьбы звонившего, чем предоставляет ему доступ к своему банковскому счету, денежные средства с которого в последующем похищаются.

Следует помнить, что сотрудники банка не вправе требовать от держателя карты ее реквизиты (код, номер, срок действия).

Способ №3. Мошенничество на бесконтактных платежах. Современные банковские карточки оснащены чипом, позволяющим совершать быструю оплату, поднося карту к терминалу, который считывает информацию и списывает соответствующую сумму со счета. Мошенники носят в сумке самодельные портативные терминалы и прислоняются к «жертвам», чтобы украсть деньги с карты.

Способ №4. Поддельный домен. К примеру существует сайт попутчиков –

VLAVLACAR, на котором люди размещают объявления о свободных местах в машине. Когда пользователь откликается на объявление, мошенники в чате просят связаться в WhatsApp и отправляют номер телефона словами, поскольку политика сервиса запрещает передавать контактные данные. Когда речь заходит об оплате поездки, жертве предлагают «купить билет» по ссылке якобы VLAVLACAR, но на самом деле это схожий мошеннический сайт.

Способ №5. Продажа несуществующего товара. Посетителя интернет-магазина привлекают низкими ценами на дорогостоящий товар. В последствии жертва посылку не получает.

Способ №6. Поддельные ресурсы. Есть популярный сайт, где Вы можете быстро оформить онлайн-займы или инвестировать свои деньги, но злоумышленники могут зарегистрировать похожий домен и сделать точно такой же дизайн и личный кабинет. На первый взгляд ничего подозрительного. Вы вкладываете свои деньги, чтобы получать проценты, а как оказалось Вас обманули мошенники. Всегда проверяйте название домена.

Способ №7. Аферисты сидят на Avito и других сайтах объявлений в поисках жертвы. Они отправляют СМС по поводу объявления со ссылкой. Если перейдете по ней, можете «получить» вирус, который позволит злоумышленникам списать с Вашего телефона денежные средства.

Первое, что нужно сделать, если Вы стали жертвой мошенника, это сообщить о случившемся в ближайшее отделение полиции.