Главе управы Таганского района г. Москвы

Мишакову А.С.

ул. Воронцовская, д. 21, г. Москва, 109147

ИНФОРМАЦИЯ

для размещения на сайте Управы Таганского района г. Москвы

**«Способы мошенничества с использованием**

**информационно – коммуникационных технологий»**

**Заблокированная карта**

**Мошенническая схема:**

Жертвам приходит СМС-сообщение о том, что карта заблокирована, для разблокировки нужно позвонить по указанному в сообщении номеру телефона.

Далее, либо звонок окажется платным и с жертвы спишут деньги, либо жертва дозвонится до лже-сотрудника банка, который попытается вытянуть полную информацию о карте, включая CVC и код подтверждения из СМС, что позволит мошенникам списать деньги со счета жертвы.

Кстати, такие сообщения и звонки не всегда поступают с незнакомых номеров. Иногда мошенники пользуются программами, которые имитируют настоящие номера банка.

**Как не стать жертвой:**

Получив сообщение или звонок, не торопитесь следовать инструкциям. Наберите номер телефона, указанный на обороте вашей карты, и расскажите сотрудникам о том, что случилось. Кроме того, ни один настоящий работник банка не станет просить у вас код из СМС.

**2. Ложный покупатель**

**Мошенническая схема**

Вы выставляете товар на «Авито», «Юле» или других интернет-площадках для продажи б/у вещей. Вам звонит потенциальный покупатель, задаёт пару вопросов. Иногда ещё на этой стадии можно заподозрить неладное: вопросы очень поверхностные и выдают, что собеседник совсем не разбирается в том, что хочет приобрести. Затем лже-покупатель начнет сокрушаться, что он живёт далеко или сейчас в отъезде, отправит курьера или таксиста, а оплату произведет безналичным расчетом по карте.

При оплате ему также понадобится не только номер вашей карты, но и дата выдачи, имя и фамилия владельца, а также трёхзначный код СVC. Объяснения обычно невнятные: якобы средства переводятся со счёта организации, там более сложная процедура и т.д. Указанных данных может быть достаточно, чтобы у вас похитить денежные средства со счета, но иногда мошенники просят, помимо вышеперечисленного, назвать им код из СМС.

Как правило, действия по оплате происходят в спешке, потому что рядом уже стоит раздражённый таксист или курьер. Завладев кодом, аферисты могут расплатиться вашей картой за покупки или перевести деньги на другой счёт.

**Как не стать жертвой:**

Не называйте никому CVC-код, а также код из СМС, для перевода нужен только 16- или 18-значный номер. Если всё же сообщили мошенникам все данные, срочно звоните в банк и блокируйте карту.

**6. Знакомый в беде**

**Мошенническая схема**

Мошенники взламывают страницу в социальные сети, и размещают пост от имени жертвы о том, что случилось горе (умирает близкий родственник, кто-то попал в аварию, кого-то арестовали), а также размещают номер банковской карты с просьбой о помощи. Иногда к посту прилагаются даже фото медицинских документов. Начинается рассылка по друзьям.

Тот, кто откликнулся на просьбу о помощи и отправил какую-то сумму, вскоре узнаёт, что помог заработать аферистам: страницу взломали, а изображения документов украдены из других источников и изменены в графических редакторах.

Самые продвинутые авантюристы звонят как будто с личного номера телефона «виновника» — с помощью программ, которые подменяют

**Как не стать жертвой**

Задавайте вопросы, ответы на которые может знать только настоящий владелец страницы. Свяжитесь с вашим знакомым или его близкими по телефону, электронной почте или через другую социальную сеть.

Межрайонный прокурор Д.К. Боков