

Мошенничество с SIM-картами

Приобрести SIM-карту, зарегистрированную на другого владельца, и сегодня можно буквально на каждом углу. Абоненту достаточно пополнить счет номера и пользоваться.

Приобретая SIM-карту у дилера, который игнорирует ее регистрацию, пользователь автоматически попадает в зону риска.

Например, SIM-карта может содержать вредоносную программу – «троян», который попытается украсть деньги либо со счета мобильного номера, либо с привязанного к номеру банковского счета. То есть программа будет вместо пользователя отправлять соответствующие СМС - сообщения и прочие запросы, попутно стирая из памяти устройства их следы.

Не исключен вариант, когда продавец «ради удобства клиента» не просто зарегистрировал SIM-карту на себя, но и завел уже личный кабинет. В этом случае он имеет возможность распоряжаться средствами мобильного счета (например, увести сразу всю сумму после первого пополнения счета или долгое время отщипывать от пополняемого счета понемногу, чтобы было незаметно).

Пользователям рекомендуется при заключении договора с оператором сразу установить ограничения на перевыпуск SIM-карты: запретить действия по доверенности и замену паспорта любым иным документом.

Но самая лучшая защита, завести для финансовых операций отдельный номер. Соответственно, если он не будет использоваться для звонков, «не засветится» в Интернете, потенциальные злодеи вряд ли узнают о его существовании.

Установить SIM-карту с этим номером необходимо в отдельный аппарат, который ни для чего иного, кроме мобильного банкинга, использоваться не будет.

И если для СМС - сервисов не требуется специальное приложение в смартфоне, лучше всего выбрать самый простой кнопочный телефон – в нем вирусы точно не поселятся.

Прокуратура Пушкинского района