1. Мошенничество со старыми СИМ-картами.

При смене абонентского номера обязательно необходимо отвязать его от личного кабинета портала государственных и муниципальных услуг «Госуслуги», так как после прекращения его использования мошенники с его помощью могут восстановить доступ к Вашему личному кабинету, а также личных кабинетов онлайн банков.

2. Мошенничество с инвестициями.

Не осуществляйте инвестиции в подозрительные проекты, такие как криптовалютная торговля, торговля акциями, стартапы и т.д. Вместо реальной прибыли Вы можете потерять вложенные средства. Инвестировать можно только на официальных брокерских площадках, имеющих лицензии ЦБ РФ.

3. Подозрительные ссылки Мошенничество посредством телефонных звонков и звонков посредствам мессенджеров «WhatsApp» и «Telegram».

Не сообщайте ни кому, код из СМС-сообщения, даже если звонивший представится сотрудником поддержки портала «Госуслуги», «Пенсионного фонда», «Операторов сотовой связи», «Энергосбыта», МВД, ФСБ, банковских учреждений, а так же под предлогом замены счетчика, продления действия сим-карты - это мошенники. После сообщения кода, злоумышленник получит доступ к вашим онлайн сервисам и может оформить кредиты.

Должностные лица не совершают звонков, тем более посредством мессенджеров, и не выясняют поступившие в смс-сообщениях цифровые коды.

4. Сообщения и звонки от имени начальников, родственников, знакомых.

При получении сообщения или звонка от руководителя, коллеги, родственника, знакомого в том числе со страницы его профиля с просьбой займа денежных средств, оформления кредита, а так же сообщением о том, что правоохранительные органы установили что денежные средств уходят на поддержку Украины и нужно перевести деньги на «безопасный счет».

Денежные средства кому-либо переводить не нужно, необходимо убедиться, что звонит именно ваш знакомый перезвонив ему лично, на имеющийся у вас номер телефона.

Безопасных счетов не существует. Звонит мошенник.

5. Подозрительные ссылки и файлы

При получении сообщения в мессенджерах от знакомых, в совместных группах и от других лиц файл с надписью «Посмотри, это ты на фото», «Архив фото» и другими названиями, а так же ссылки для дальнейшего перехода в другие группы или сайты при открытии (переходе) может на ваш телефон установиться вредоносная программа, с помощью которой будут похищены денежные средства и получен доступ к вашему сотовому телефону.

Не переходите по сомнительным ссылкам и не открывайте сомнительных файлов.

ЗАПОМНИТЕ!!!

Не отвечайте на подозрительные звонки;
Не сообщайте коды из смс-сообщений, а также другую важную информацию;
Не вводите данные банковской карты на сомнительных сайтах;
Проверяйте подозрительные сайты;
Не авторизуйтесь на незнакомых сайтах;
Подключите двухфакторную аутентификацию к своим аккаунтам и личным кабинетам;
Не открывайте подозрительные письма, файлы и приложения.