Мошенники постоянно придумывают новые схемы обмана, однако существуют предлоги и способы, которые актуальны уже долгое время. Вот некоторые из основных «уловок», используемых злоумышленниками:

1. Мошенничество со старыми СИМ-картами.

При смене абонентского номера необходимо в обязательном порядке «отвязать» старый номер от личного кабинета портала государственных и муниципальных услуг «Госуслуги», от кошельков в маркетплейсах и онлайн-банков. Через несколько месяцев абонентский номер будет вновь выпущен в оборот и мошенники смогут восстановить доступ к Вашим интернет-сервисам.

2. Мошенничество посредством телефонных звонков и сообщений, в том числе в мессенджерах «WhatsApp», «Max» 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, домофона, продления действия сим-карты, доставки посылки, цветов, - это мошенники. После сообщения кода, злоумышленник получит доступ к Вашим онлайн сервисам, может оформить кредиты или проигрывать другие способы обмана.

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

3. 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 об «оперативной разработке», о «подозрениях в финансировании Украины» и «защитой денежных средств на безопасных счетах» не вступайте в диалог!

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. Эту фазу придумали и используют только мошенники.

4. Подозрительные ссылки и файлы

При получении сообщения в мессенджерах от знакомых, в совместных группах и чатах сообщений с файлом с надписью «Посмотри, это ты на фото», «Архив фото», «Посмотри видео с тобой» и другими названиями, содержащими интернет-ссылку, категорически запрещено нажимать на ссылку! При переходе по ссылке в Ваш мобильный телефон будет установлена 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.

5. Доставка или посылка товара

Мошенники сообщают о якобы готовой к доставке посылке. При этом утверждают, что заказ уже оплачен, и просят согласовать время вручения. Если человек отвечает, что ничего не заказывал, аферисты объясняют это ошибкой или “подарком от неизвестного отправителя”. Далее под предлогом “подтверждения личности” мошенники отправляют СМС-код и просят его назвать. Этот код используется для входа в личные кабинеты (например, на портале Госуслуг) или подтверждения банковских операций — тем самым мошенники получают доступ к персональным данным и финансам.

6. Мошенничество в отношении пожилых граждан

Сегодня многие пожилые граждане пользуются банковскими картами, онлайн-банками, зарегистрированы в мессенджерах, чтобы общаться со своими детьми и внуками. Однако их цифровизацию активно используют мошенники.

Злоумышленники звонят как на стационарные телефоны, так и на мобильные, сообщают о замене электрических счетов, счетчиков на воду, ключей от домофона, предлагают записаться к врачу, получить льготные лекарства, пересчитать пенсию и используют другие предлоги из социальной сферы и ПРОСЯТ НАЗВАТЬ КОД ИЗ СМС-СООБЩЕНИЯ. Назвав который, пенсионеры не только предоставляют доступ к онлайн-сервисам, но и тем самым попадают «на крючок мошенников». Дальше преступники могут использовать различные предлоги: от подозрительных переводов денег на Украину, до декларирования денег в Налоговой инспекции, чтобы избежать уголовной ответственности. ПРИ ЭТОМ ВСЕ ЧАЩЕ ЗА ДЕНЬГАМИ (КОТОРЫЕ ПЕНСИОНЕРЫ ЛИБО ХРАНЯТ ДОМА, ЛИБО СНИМАЮТ ПО УКАЗАНИЮ МОШЕННИКОВ) К НИМ ДОМОЙ ПРИХОДЯТ КУРЬЕРЫ (ИНКАССАТОРЫ).

Не называйте никому код из смс-сообщений и тем более не передавайте деньги!

7. Мошенничество с использованием детей

Мошенники могут использовать несовершеннолетних, чтобы похитить деньги взрослых родственников. В мессенджерах или социальных сетях ребенку пишут сообщения, представляясь сотрудниками «официальных и серьезных» ведомств (Полиция, ФСБ, Росфинмониторинг, Центробанк), сообщая о том, что родителям, бабушкам, дедушкам грозит уголовная ответственность или имеющиеся в вашей семье деньги будут списаны, или отобрана квартира и тд. Запугивая несовершеннолетнего, мошенники выясняют социальный статус родственников, финансовое положение, убеждают узнать пароли и коды от онлайн-банков и тайно взять телефон родителей или других родственников и перевести деньги, обещая, что они вернуться обратно, а родственникам больше не будет грозить опасность. Ребенок, думая, что спасает своих мам, пап, бабушек, дедушек, лишает их сбережений, а иногда и оформляет на них неподъемные кредиты.

Установите на телефоны блокировки с помощью отпечатка пальца или биометрии;
Не сообщайте детям пароли и коды от онлайн-банков;
Установите доверительные отношения с ребенком, чтобы в случае его общения с мошенником, он не боялся рассказать вам об этом.

ГЛАВНАЯ ЗАЩИТА ОТ МОШЕННИКОВ – ПОЛОЖИТЬ ТРУБКУ

Если вас просят назвать код из смс-сообщения – ПОЛОЖИТЕ ТРУБКУ
Если говорят, что взломаны «Госуслуги» - ПОЛОЖИТЕ ТРУБКУ
Если предлагают заменить счетчики – ПОЛОЖИТЕ ТРУБКУ
Если сообщают о доставке письма или посылки – ПОЛОЖИТЕ ТРУБКУ
Если говорят о сохранности денег и «безопасных счетах» - ПОЛОЖИТЕ ТРУБКУ
Если предлагают пройти диспансеризацию или записаться в поликлинику – ПОЛОЖИТЕ ТРУБКУ
Если говорят об окончании договора на обслуживание сим-карты - ПОЛОЖИТЕ ТРУБКУ
- если угрожают уголовной ответственностью за финансирование ВСУ – ПОЛОЖИТЕ ТРУБКУ.

Сотрудники полиции напоминают, что с 1 марта 2025 у россиян появилась возможность установления самозапрета на кредиты, что позволяет ограничить возможности оформления кредитов или выполнение операций с денежными средствами клиента без его ведома.
В случае возникновения потребности в оформлении кредита, гражданин сможет снять самозапрет и воспользоваться банковским продуктом. Устанавливать и снимать самозапрет можно бесплатно неограниченное количество раз.