## Как не попасться на уловки мошенников

**1. Приобретая товары** (*цветочная продукция, мобильные телефоны, предметы гардероба, шины, мебель, сезонные товары, продукты питания и пр.),* а также **услуги** *(аренда недвижимости, помощь в оформлении виз, туров и т.п.)* **в сети Интернет**:

**!** обращайте внимание на стоимость товаров и услуг. Подозрительно низкие цены должны вас насторожить;

**!** не приобретайте товары и услуги, за которые просят 50% либо 100% предоплату;

**!** не переходите по подозрительным ссылкам и не вводите реквизиты банковской платежной карты, а также личные данные;

**!** заведите отдельную банковскую платежную карту для оплаты товаров и услуг в сети Интернет и переводите на нее сумму равную сумме покупки;

**!** выбирайте надежных продавцов и проверяйте их репутацию через поисковую строку любого браузера.

**2.** Если вам **позвонили по стационарному или мобильному телефону**, представились сотрудником правоохранительных органов, банковского учреждения, сотовой компании, работником коммунальных (Мингаз, Минскэнерго, Энергосбыт и пр.) или телекоммуникационных предприятий (Белтелеком), медицинских организаций и т.п. и под предлогом дистанционного продления договора на оказание услуг, замены устаревшего оборудования, сверки показателей счетчиков, приглашения на диспансеризацию, попросили предоставить персональные данные (идентификационный номер паспорта, номер мобильного телефона, иные личные данные, коды из смс-сообщений) для верификации (подтверждения личности), а также стали говорить, что:

- на вас оформили кредит;
- с ваших расчетных счетов осуществляется финансирование террористической деятельности либо военных действий в Украине;
- необходимо оказать помощь правоохранительным органам в поимке аферистов;
- в отношении вас возбуждено уголовное дело и в ближайшее время по вашему месту жительства будет проведен обыск, в связи с чем необходимо срочно обезопасить накопленные денежные средства, для чего осуществить их декларирование либо перевод на специальный «безопасный» счет;
- необходимо оказать содействие другим жертвам мошенников, которые в силу возраста или физических особенностей не могут самостоятельно обратиться в банк для зачисления наличных денежных средств на безопасный счет.

**Не совершайте** этих ошибок:

**!** ни под какими предлогами не сообщайте посторонним паспортные данные, реквизиты банковской карты (номер, сроке действия, CVV2/CVC2-код), одноразовые пароли из поступивших смс-сообщений;

**!** не проводите через банкоматы и иные устройства самообслуживания (включая систему дистанционного банковского обслуживания (интернет-банкинг) никакие операции под психологическим давлением или по инструкциям, полученным по телефону или мессенджерам;

**!** не устанавливайте на мобильный телефон приложения по просьбе третьих лиц, даже если они настоятельно этого требуют;

**!** не становитесь курьером мошенников путем собирания денежных средств у других граждан, попавших в неприятную жизненную ситуацию;

**!** при поступлении ЛЮБОГО сомнительного звонка, незамедлительно завершите разговор и обратитесь в милицию.

ПОМНИТЕ, сотрудники правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работники государственных организаций и предприятий, коммунальных служб или телекоммуникационных компаний НИКОГДА не выясняют ваши персональный данные по телефону!

**3.** Если вам **предложили дополнительный заработок** с помощью инвестиций или трейдинга и пообещали быстрый и высокий доход, то:

**!** не верьте обещаниям легкого заработка в интернете. Прежде чем вкладывать деньги в какие-либо проекты, проверьте достоверность предложения поиском в браузере, на различных форумах или по телефонам организаций, размещенным на их сайтах;

**!** ведите переписку и совершайте сделки только на официальных биржах.

ПОМНИТЕ, интернет-мошенники – хорошие психологи, которые знают, как вызвать интерес, расположить собеседника к себе и убедить человека расстаться с собственными сбережениями.

**4.** Имея аккаунты в социальных сетях (Одноклассники, ВКонтакте, Instagram, Facebook, TikTok) и мессенджерах (Telegram, Viber, WhatsApp), **во избежание несанкционированного доступа (взлома) ваших аккаунтов** и последующей рассылки от вашего имени сообщений с просьбой перевода денежных средств в долг либо оказания материальной помощи на лечение, либо вымогательства денежных средств за нераспространение личной информации, которую вы желаете сохранить в тайне, следуйте следующим рекомендациям:

**!** для обеспечения безопасности своих аккаунтов необходимо устанавливать сложные пароли и двухэтапную аутентификацию;

**!** не переходите по ссылкам из различных сообщений, поступивших даже от родных и знакомых людей;

**!** при поступлении подобного рода сообщений созвонитесь с человеком, который просит у вас финансовой помощи, для удостоверения правдивости происходящего;

**!** не храните в переписках личную информацию, фотографии и видеозаписи, которые желаете сохранить в тайне;

**!** ни в коем случае не переводите деньги мошенникам под угрозой распространения вашей личной информации.

**5.** Если вам **поступило сообщение** (как правило в мессенджере Telegram) **от вашего руководителя**, в котором говорится о необходимости оказать содействие правоохранительным органам в проверке на предмет причастности к финансированию террористической деятельности либо под предлогом одалживания денежных средств (сообщения могут быть как текстовыми, так и голосовыми), то:

**!** убедитесь в достоверности аккаунта и номера телефона с которого поступило сообщение, а также свяжитесь с руководителем по стационарной связи либо иным возможным способом;

**!** не вступайте в диалог, пока не убедитесь в достоверности происходящего.

**6. При знакомстве в Интернете** соблюдайте следующие меры предосторожности:

**!** тщательно изучайте аккаунт собеседника;

**!** как можно лучше узнайте нового знакомого;

**!** созванивайтесь по мобильному телефону и/или по видеосвязи;

**!** не ведитесь на просьбы оказать материальную помощь, тем более не отправляйте деньги на «посылки», «госпошлины», «лечение» и прочее незнакомым вам людям;

**!** ни под какими предлогами не переходите по подозрительным ссылкам, отправленным вам собеседником, и не вводите личные данные и тем более реквизиты банковской платежной карты.

**7.** Если вы осуществляете **платежи или покупки в сети Интернет**, или же вам поступило сообщение, содержащее подозрительный текст со ссылкой, то:

**!** внимательно посмотрите на адрес ссылки – если есть странные буквы, цифры или что-то лишнее это плохой знак, не переходите по ссылке;

**!** убедитесь, что в адресе есть https: и значок замка – это значит, что интернет-соединение защищено;

**!** если сайт оформлен с ошибками в тексте или странными картинками, это должно насторожить;

**!** не переходите по подозрительным ссылкам и не вводите реквизиты банковской платежной карты, а также личные данные;

**!** если сайт настойчиво требует срочно ввести пароли, данные карты или другую личную информацию – будьте осторожны.