

КАК ЗАЩИТИТЬ СЕБЯ ОТ ИНТЕРНЕТ-МОШЕННИЧЕСТВА!

Мошенники постоянно совершенствуют схемы обмана, чтобы заполучить ваши деньги. Для связи кроме интернет-звонков в мессенджерах, таких как Viber, Telegram или WhatsApp, могут использовать стационарную телефонную и мобильную связь, а также интернет-видеосвязь. Чаще всего они представляются сотрудниками правоохранительных органов, работниками операторов сотовой связи, государственных или банковских организаций, реже – вашим родственником или руководителем, брокером или трейдером криптобиржи.

НАИБОЛЕЕ АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

❖ Сообщают о возникшей проблеме и, войдя в доверие, предлагают помощь в ее решении. Например, жертву ошарашивают подозрением в соучастии в **преступлении, следовательно, вероятностью проведения обыска и изъятием денежных средств**. Для их сохранения предлагают перевести наличные на якобы защищенный счет или передать якобы работнику банка для **декларирования**.

❖ Сообщают, что **закончился срок действия договора на услуги связи** и убеждают по ссылке из мессенджера скачать фэйковое приложение, чтобы продлить услугу. Такие приложения дают возможность мошенникам видеть всю информацию с экрана смартфона (коды из смс, логины и пароли к банкингу). Необходимо знать, что безопасно скачивать приложения только из официальных магазинов «Google Play», «App Store», «App Gallery», а не по направленным ссылкам.

❖ Интернет-преступники умело пользуются возможностями нейросетей. При получении образца голоса или фото они создают фэйковые сообщения или видео **от имени родственников или знакомых**. Позже контактам жертвы рассылают такие поддельные **просьбы о материальной помощи на лечение на банковскую карту или через «знакомого»**.

❖ Основным видом регистрируемых киберпреступлений являются интернет-мошенничества. На сегодняшний день широко распространен такой вид преступной деятельности как обман, совершаемый в социальных сетях с использованием мошеннических интернет-магазинов под предлогом **купли-продажи товаров**.

Их ассортимент довольно обширный: **от предметов одежды и обуви, автотранспортной техники и запасных частей, мобильных телефонов, цветов и рыбной продукции**.

Как правило, стоимость таких псевдотоваров гораздо ниже рыночной стоимости. Добросовестный покупатель вносит предоплату, либо оплачивает полную стоимость приобретаемого товара и, как итог, остается и без денег, и без покупки. Чтобы не стать жертвой киберпреступников рекомендуем гражданам пользоваться только официальными сайтами

и не переходить (в том числе по ссылкам) на сомнительные площадки. Пользуясь различными интернет-ресурсами, не стоит доверять продавцу, требующему внести предоплату за покупку или услугу.

❖ Самые опасные кибермошенники те, которые **представляются брокерами или трейдерами торговых площадок и предлагают жертве увеличить доход, инвестировав небольшую сумму.** В сети Интернет они размещают сайт несуществующей биржи с графиками и диаграммами. Регистрируют вкладчикам личный кабинет и демонстрируют якобы полученный доход. Иногда дают вывести небольшую часть денег, но всегда убеждают продолжать вкладывать бóльшие суммы, которые, например, одолжить у знакомых, получить в кредит или от продажи жилья.

❖ Для вывода похищенных денег мошенники всегда используют подставных лиц – дропов, которые за вознаграждение предоставили доступ к своим банковским счетам. Дропы являются звеньями преступной цепочки и нужны для перевода денег через несколько банков на иностранные счета или в криптовалюту. **Дропы несут ответственность по ст. 222 Уголовного кодекса Республики Беларусь** вплоть до 10 лет лишения свободы.

❖ В нашей республике разрешено покупать и продавать криптовалюту за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается. Порядок осуществления сделок с криптовалютой в настоящее время определен Указом Президента Республики Беларусь от 17 сентября 2024 г. №367 «Об обращении цифровых знаков (токенов)», за нарушение которого предусмотрена ответственность по ч.3 ст.13.3 КоАП в виде штрафа с конфискацией всей суммы дохода.

❖ **Будьте бдительны! Эти знания помогут вам сберечь ваши деньги!**

По материалам УПК УВД Могилевского облисполкома