

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

!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 фейковое приложение, чтобы продлить услугу. Такие приложения дают возможность мошенникам видеть всю информацию с экрана смартфона (коды из смс, логины и пароли к банкингу). Надо 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 фейковые 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».

◆ Самые опасные кибермошенники те, которые представляются брокерами или трейдерами торговых площадок и предлагают жертве увеличить доход, инвестировав небольшую сумму. В Интернете 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 большие 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 УК 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 определен Указом Президента Республики Беларусь от 20.09.2024 № 367, 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!

Виды мошенничества

◆ Фишинг – вид мошенничества, заключающийся в размещении мошенниками в сети Интернет поддельных сайтов Интернет-банкингов;

◆ Попасть на фишинговый сайт может каждый. Желая воспользоваться «Интернет-банкингом», многие пользователи задают соответствующий запрос в популярных поисковых системах (Google, Яндекс и т.д.). Мошенники, зная это, создают рекламные объявления в данных поисковых сервисах, которые затем отображаются первыми в результатах поиска.

Переходя по данным ссылкам, пользователи попадают на поддельные сайты, которые визуально выглядят почти как настоящая страница «Интернет-банкинга», а адрес мошеннического ресурса может быть похож на официальный <https://ibabek.asb.by>.

◆ Вишинг – вид мошенничества, заключающийся в применении методов социальной инженерии (звонки от имени правоохранительных органов, сотрудников Банка и т.д.).