Как защитить граждан от кибермошенничества!

(руководство для сотрудников правоохранительных органов)

Кибермошенники постоянно совершенствуют методы обмана, используя новые технологии и социальную инженерию. Ваша задача — быть в курсе актуальных схем и уметь донести эту информацию до граждан. Ниже представлены наиболее распространённые сценарии мошенничеств и рекомендации по профилактике.

Основные схемы кибермошенничества

Мошенничество под видом работников коммунальных служб и государственных органов. Злоумышленники выдают себя за сотрудников коммунальных служб (энергонадзора, водоканала, газовой службы), а также представителей правоохранительных органов, банков или других государственных структур. Они могут звонить по телефону, в том числе по стационарной линии, или использовать мессенджеры (Viber, Telegram, WhatsApp). Цель — под любым предлогом получить личные данные, реквизиты банковских карт или вынудить перевести деньги на «безопасные» счета. Часто работают в паре: один представляется сотрудником коммунальной службы, другой – правоохранительных органов или банка, убеждая жертву, что ее данные скомпрометированы, и для «спасения» средств необходимо оформить кредит или перевести деньги.

Мошенничество с использованием мобильной связи. Мошенники представляются сотрудниками операторов сотовой связи (А1, МТС). Под предлогом окончания срока действия договора или необходимости обновления услуг они убеждают жертву перейти по ссылке из мессенджера и скачать поддельное приложение. Такие приложения дают злоумышленникам полный доступ к данным на смартфоне, включая коды из SMS, логины и пароли к онлайн-банкингу. Важно помнить: безопасное скачивание приложений возможно только из официальных магазинов, таких как Google Play, App Store, App Gallery. Никогда не устанавливайте приложения, переходя по сомнительным ссылкам.

Использование дипфейков и нейросетей. Киберпреступники активно применяют нейросети для создания поддельных голосовых сообщений и видео (дипфейков) с использованием голоса или изображения родственников и знакомых жертвы. Затем такие фальшивые сообщения рассылаются контактам жертвы с просьбами о материальной помощи на лечение или другие нужды, часто с указанием реквизитов банковской карты или просьбой передать деньги через «знакомого».

Психологическое давление и угрозы. Мошенники, выдавая себя за сотрудников правоохранительных органов или даже вашего руководителя, пишут в мессенджерах, сообщая о якобы совершенном вами преступлении или соучастии в нем. Они могут угрожать обыском, изъятием имущества или денежных средств. Для «сохранения» денег предлагают перевести их на «защищенный» счет или передать курьеру, который на самом деле является их пособником. В таких случаях мошенники могут даже «переключать» жертву на подставных «сотрудников» различных ведомств (милиции, Следственного комитета, КГБ, ДФР, КГК).

Финансовые пирамиды и лжеинвестиции. Это одна из наиболее опасных схем. Мошенники, представляясь брокерами или трейдерами торговых площадок, предлагают жертвам быстрый и высокий доход от инвестиций. Они создают фейковые веб-сайты несуществующих бирж с имитацией графиков и диаграмм, регистрируют «личные кабинеты» и демонстрируют «прибыль». Могут даже позволить вывести небольшую сумму, чтобы убедить жертву в реальности заработка. Цель — вынудить человека вложить как можно больше денег, включая заемные средства или деньги от продажи имущества. После получения крупной суммы мошенники исчезают.

Использование "дропов" и ответственность. Для вывода похищенных средств мошенники активно используют «дропов» — подставных лиц, которые за вознаграждение предоставляют доступ к своим банковским счетам. «Дропы» являются ключевым звеном преступной цепочки, через которое деньги переводятся через несколько банков на иностранные счета или конвертируются в криптовалюту. Важно знать и доносить до граждан: «дропы» несут уголовную ответственность за распространение чужих данных для доступа

к банковским счетам по статье 222 УК, предусматривающей наказание до 10 лет лишения свободы. За предоставление своих личных данных для использования в мошеннических схемах предусмотрена административная ответственность по статье 12.35 КоАП.

Регулирование оборота криптовалюты в Республике Беларусь. Операции по покупке и продаже криптовалюты за денежные средства (белорусские рубли, иностранная валюта или электронные деньги) разрешены только через криптобиржи (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий. Запрещены и являются незаконными операции по купле-продаже криптовалюты на иностранных криптобиржах и у физических лиц. Порядок осуществления сделок с криптовалютой регулируется Указом Президента Республики Беларусь от 20.09.2024 № 367, за нарушение которого предусмотрена ответственность по ч. 3 ст. 13.3 КоАП, предусматривающей штраф с конфискацией всей суммы дохода.

Рекомендации для сотрудников правоохранительных органов. Постоянно повышайте свою осведомленность о новых видах и схемах кибермошенничества. Следите за новостями, аналитическими материалами и рекомендациями профильных ведомств. Особое внимание уделяйте уязвимым категориям граждан: пожилым людям, несовершеннолетние, а также тем, кто активно пользуется интернетом, но недостаточно осведомлен о рисках. Подчеркивайте важность критического мышления: учите граждан проверять любую информацию, особенно ту, что вызывает беспокойство или предлагает легкую прибыль. Объясняйте, что правоохранительные органы, банки и государственные структуры никогда не запрашивают конфиденциальные данные по телефону или в мессенджерах и не требуют переводить деньги на «безопасные» счета. Акцентируйте внимание на ответственности «дропов», чтобы граждане понимали риски предоставления своих счетов третьим лицам. Разъясняйте правила легального оборота криптовалют в Республике Беларусь.

Помните: наша общая цель — защитить граждан от преступных посягательств в цифровом пространстве. Чем лучше информированы сотрудники правоохранительных органов, тем эффективнее мы сможем противодействовать киберпреступности.