План-конспект по теме
«Профилактика киберпреступлений и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий»

В настоящее время киберпреступность представляет серьезную угрозу для развития экономики и общества. 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.

Мошенники регулярно меняют свои схемы обмана граждан, чтобы похитить их деньги. Основными формами обмана являются телефонное и интернет-мошенничество, а также фишинговые ресурсы.

НАИБОЛЕЕ АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ

Мошенники представляются сотрудниками мобильного оператора

Участились случаи, когда мошенники, представляясь сотрудниками мобильного оператора, под выдуманными предлогами (необходимость продления договора, страхование или декларирование денежных средств) предлагают установить приложение удаленного доступа, а получив доступ к мобильному устройству, похищают с карт-счета сбережения доверчивых граждан.

Запомните: установив фейковое приложение, вы тем самым предоставляете злоумышленникам доступ к своим данным, включая логины и пароли. Это позволяет преступникам свободно получать информацию о банковских счетах, личной переписке и других конфиденциальных сведениях!

Следует помнить, о том, что:

- сотрудники мобильных операторов не звонят абонентам через мессенджеры и не используют номера иностранных операторов, а также никогда не требуют изменить пароли под диктовку;

- договоры с компаниями мобильных операторов связи заключаются на бессрочной основе и продлеваются автоматически;

- если вы получаете звонок через любой мессенджер с неизвестного номера, не передавайте личные данные, прервите разговор и обратитесь в официальный контактный центр оператора связи для проверки информации;

- никогда не устанавливайте приложения по ссылкам, полученным от неизвестных источников через мессенджеры ил присланные в виде APK-файла, а скачивайте только из официальных магазинов Google Play, App Store и App Gallery.

Обманы под предлогом сдачи жилья

Имеют место случаи обмана населения, связанные с арендой жилья. Только доверчивые граждане не подозревают, что скрывается за привлекательной ценой и красивой картинкой.

Схема проста: в интернет-ресурсах злоумышленники размещают фальшивые объявления о сдаче квартиры/дома на выгодных условиях. Зачастую стоимость такого жилья ниже среднего показателя. Далее лжеарендодатели просят заинтересованных лиц внести частичную либо полную предоплату.

Главный акцент в таких махинациях делается на эффекте срочности и доверчивости потенциального съемщика. Опасаясь упустить выгодное предложение, граждане не задумываются, что могут общаться с мошенниками.

Будьте бдительны и следуйте простым правилам при аренде жилья:

- заключать договор найма следует только при личной встрече с владельцем квартиры/дома;

- осуществлять оплату/предоплату необходимо лишь после того, как вы убедились, что ваш собеседник – владелец жилья, а квартира/дом соответствует описанию, заявленному в объявлении.

Небезопасное инвестирование

В интернете встречаются предложения о быстром заработке путем вложения денежных средств в акции или криптовалюту.

Зачастую под видом специалистов валютно-фондовых бирж, сферы криптовалюты и сотрудников администраций онлайн-казино скрываются мошенники. С использованием различных мессенджеров злоумышленники создают аккаунты, где обещают доверчивым гражданам приумножить их сбережения.

Вот ***несколько примеров, как могут разворачиваться события***:

1. Мошенники просят перейти по предоставленной фишинговой ссылке, которая переадресует пользователя на сайт, внешне схожий с криптобиржей/валютно-фондовой биржей. Далее – просят ввести личные данные, реквизиты банковских счетов и зарегистрировать аккаунт, чем предоставляют всю необходимую злоумышленникам информацию.

2. Мошенники уговаривают граждан перевести сбережения на банковские счета и ожидать, пока деньги «не начнут работать». При

любом исходе результат один: злоумышленники присваивают себе деньги доверчивых граждан и перестают выходить с ними на связь.

Сотрудники милиции призывают граждан быть бдительными и ***напоминают о мерах безопасного общения*** в интернете:

- пользуйтесь только официальными платформами по осуществлению криптовалютных и фондовых сделок (обязательно сверьте URL-адрес интернет-ресурса);
- не следует осуществлять денежные переводы лицам, которые обещают приумножить ваши сбережения;
- не высылайте незнакомцам личные данные, номера ваших счетов и кошельков, а также аутентификационные данные (логины, пароли, коды двухфакторной защиты аккаунта и т.д.), позволяющие осуществить вход в ваш личный кабинет на крипто- и валютно-фондовых биржах.

Мошенники и код от домофона: как работает новая схема обмана

Мошенники начали обманывать граждан, используя новый предлог. Аферисты звонят и представляясь сотрудниками компаний по установке домофонов, предлагают бесплатную замену ключей. Под видом «плановой замены чипов» запрашивают личные данные человека. Если «клиент» соглашается, то следом они запрашивают код из SMS, который направляется якобы «от компании» и будет использован для открытия домофонной двери.

Позже с другого номера поступает звонок от лжеправоохранителя, который сообщает о попытке взлома системы и под предлогом предотвращения мошеннических действий, убеждает гражданина сообщить ФИО, дату рождения, реквизиты банковских карт, коды из SMS и пин-коды.

Получая доступ к личным данным (аккаунтам, кабинетам) жертвы, злоумышленники имеют возможность совершать от ее имени различные действия: оформлять кредиты (доверенности), похищать денежные средства с банковских счетов и т.п.

Как не потерять свои сбережения*:*

- никогда не сообщать одноразовые SMS-коды посторонним;
- помнить, что сотрудники правоохранительных органов, банковских и иных учреждений не связываются с гражданами по мессенджерам;
- незамедлительно прекращать разговор с незнакомцем;
- обращаться к представителям банков, в государственные органы и учреждения только через официальные сайты и контактные телефоны, размещенные на них;
- не переходить по подозрительным ссылкам и не скачивать приложения из неизвестных источников.

Если незнакомцы по телефону требуют от вас совершить какие-либо манипуляции с финансами (задекларировать, положить на безопасный счет и т.д.) – немедленно прекратите разговор и сообщите об этом в милицию!

Как не стать жертвой туристических мошенников

С каждым годом мошенники в сфере туризма становятся все более изобретательными. Они придумывают новые схемы обмана граждан, многие из которых собирают деньги или берут кредиты на долгожданный отдых.

Схема обмана проста. Мошенники в социальных сетях регистрируют аккаунт, зачастую созвучный с известным туроператором. На странице выкладывают весьма заманчивое предложение: «Отдых в Турции по самым низким ценам», «Горящие туры» и тому подобное. Отзывы о поездке, которые размещаются ниже, являются фальшивыми, а число подписчиков – накрученным.

При покупке туристических путевок необходимо опасаться компаний с «ударными скидками» и «выгодными ценами». Отсюда простое правило: при выборе туров не следует обольщаться слишком высокими скидками.

Кроме того, зачастую все общение между клиентом и «турфирмой» происходит в социальных сетях или в мессенджере. Прежде чем подписывать договор об оказании услуг или направлять предоплату, попросите у представителя турагентства номер телефона для связи, а также уточните адрес местонахождения самого офиса для того, чтобы его посетить и вживую пообщаться, уточнив все интересующие вас вопросы. Только после этого следует рассматривать вопрос о бронировании и приобретении тура. Запомните, если действует мошенник, то он никогда вживую с вами не станет встречаться, объясняя это различными причинами: занятость, слишком большой поток клиентов, акция на тур действует только сегодня и так далее.

Чтобы не стать жертвой злоумышленников рекомендуем: никогда не перечисляйте деньги незнакомым людям в интернете и с большой настороженностью относитесь к гражданам (организациям), предлагающим туристический тур ниже рыночной стоимости.

Как мошенники обманывают граждан под видом «Белпочты»

Имеют место случаи, когда злоумышленники действуют от имени представителей почтовых отделений. Схема проста: они рассылают sms-сообщения с фишинговыми ссылками, утверждая, что доставка посылки невозможна ввиду отсутствия адреса. Потенциальной жертве предлагают перейти на «официальный сайт», ввести свои персональные данные и

оплатить повторную отправку посылки.

Также мошенники регистрируют личные кабинеты на портале «Белпочты». После чего связываются с гражданами посредством мессенджеров и пытаются узнать код подтверждения из сообщения, чтобы далее действовать от их имени.

Помните: коды из sms-сообщений – это конфиденциальная информация, которую нельзя сообщать третьим лицам. Если вы стали жертвой подобной схемы обмана, незамедлительно смените пароль на портале «Белпочты» или в мобильном приложении организации и сообщите по номеру «102».

Сотрудники почтовых отделений информируют о прибытии отправлений, но никогда не требуют онлайн-оплаты услуг через сомнительные ссылки и ввод данных банковских карт. Проявляйте осторожность при переходе в интернете и всегда проверяйте адрес сайта.

По материалам УПК КМ УВД