

МАТЕРИАЛ

для членов информационно-пропагандистских групп
(март 2024 г.)

Профилактика преступлений с использованием информационно-коммуникационных технологий

За истекший период 2024 на территории Жлобинского района возбуждено 37 уголовных дел по фактам хищений денежных средств у граждан с использованием информационно-коммуникационных технологий, из которых 25 составляют мошенничества, где, под различными предложениями, злоумышленники стремятся убедить владельца денег перевести их на другие, подконтрольные им, счета.

Рассмотрим самые распространенные схемы мошенничества сейчас:

1. «Звонок из Банка, сотового оператора и т.д.»

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка (другой организации), а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамouflирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить

- Мы звоним с официального номера, проверьте на сайте».
- «В целях конфиденциальности я включаю робота, который защитит ваши данные» (вы слышите в трубке лёгкий шелест).

- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а лотом вы сможете вернуть деньги»*.
- Или просит назвать ваши персональные данные или секретные коды из SMS робота, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать! Это же относится и к «вопросам» с сим-картам.

2. «Потенциальный покупатель»

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии - только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете. **Запомните!** Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

Примеры совершенных преступлений:

Мошенники действуют под маской интернет-магазинов!

За текущий период времени на территории Жлобинского района возбуждено девять уголовных, дел по ст. 209 УК Республики Беларусь по фактам обмана граждан под предлогом продажи различных товаров в сети Интернет на общую сумму 4183 рубля.

Наиболее типичная схема:

Злоумышленник, в ходе переписки в сети «Instagram» со страницы «flowers_ultima» с жительницей г. Жлобин, под предлогом продажи цветов и их последующей доставки путем обмана убедил последнюю перевести денежные средства в качестве предоплаты, но обязательство по предоставлению товара не выполнил, в результате чего причинил имущественный вред. Само собой социальная сеть, название магазина и предмета продажи меняются, но общая схема остается неизменной.

Советы как распознать фейковый интернет-магазин:

- Внимательно изучите сайт интернет-магазина. Если на нем отсутствует раздел «Контакты» - сразу проходите мимо. Иногда на фейковых страницах есть форма ввода вашего номера телефона и подпись вроде «Мы вам перезвоним». Если вы ввели свой номер телефона, не удивляйтесь, что Вам потом могут перезвонить какие-нибудь сотрудники банка и сказать, что у Вас одобренный кредит или Вы выиграли в лотерею 1 миллион долларов, и чтобы его забрать необходимо перечислить сумму на определенный расчетный счет.
- Относитесь критично к отзывам, размещенным на сайте интернет-магазина, в основном они только хвалебные и не всегда правдивые.
- Скопируйте фото товара, размещенного на сайте, и вставьте в поиск по картинкам в браузере Google или Яндекс. Если поисковик выдает ссылки на этот же магазин и еще на два-три известных, это нормально. Если же Вы увидите на экране невероятное количество разноименных сайтов, причем картинка везде будет одна и та же, это почти наверняка мошенники.

ТАКЖЕ РАСПРОСТРАНЯЮТСЯ СХЕМЫ «МГНОВЕННОГО» ЗАРАБОТКА:

Жлобинским РОСК возбуждено уголовное дело по ч. 3 ст. 209 УК Республики Беларусь (мошенничество в крупном размере) по заявлению жителя г. Жлобин о том, что в сети интернет им было найдено объявление о сайте «m-trade.finquotesfinancial.pro», где имелась возможность заработка в ходе операций на инвестиционной бирже, поддавшись искушению потерпевший перевел более 12 тысяч рублей но, как закономерный итог, остался ни с чем.

Советы ты как. распознать такую уловку:

- Внимательно изучите сайт. Отсутствие технической информации и обратной связи с владельцами должно вызвать подозрение в его реальности.
- Проверьте есть ли схожие, по названию, торговые площадки, есть о них отзывы, где размещены представительства и т.д.

ОВД Жлобинского райисполкома напоминает: приведенные способы совершения хищений не являются исчерпывающими, но

самыми распространенными. Форма и подача информации может меняться, неизменная суть - получение персональных данных (номер паспорта, банковской карты, личных кодов и т.д.), убеждение в установке различных приложений и получения из них информации. Не предоставляйте свои данные, не устанавливайте приложения по просьбе третьих лиц.

*Отдел внутренних дел
Жлобинского райисполкома*