Топ-8 грязных схем

БУДЬТЕ ВНИМАТЕЛЬНЫ!

! ИНТЕРНЕТ-МОШЕННИКОВ

ЗВОНОК ИЗ БАНКА

Звонящий представляется сотрудником службы безопасности банка и уверяет: «С вашей карты кто-то хотел похитить деньги, для отмены операции назовите свои данные». Выманив сведения, мошенник выводит со счета все средства и исчезает.

Как не попасться? Скажите, что вы не клиент этого учреждения (даже если это так). Если на той стороне мгновенно переключат на «специалиста из вашего банка» - это точно мошенничество.

Или просто положите трубку и перезвоните в банк сами. Только номер телефона смотрите не во «Входящих», а на сайте.

СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

Мошенники в соцсетях создают группу якобы с целью сбора средств на лечение тяжелобольного. Деньги предсказуемо забирают себе.

Как не попасться? Запросите у администратора группы справки, документы, другие дополнительные сведения.

ПИСЬМО ОТ ДРУГА

Преступник взламывает чужие соцсети и рассылает друзьям пользователя сообщения с просьбой сбросить денег или отправить откровенные фото. Мошенник заранее изучает переписку жертвы и выбирает максимально похожий стиль письма.

Как не попасться? Позвоните другу и уточните, действительно ли он вам пишет.

Если нет возможности позвонить - напишите в другом мессенджере.

ДЕШЕВЫЕ ВЕЩИ

Вор создает в социальной сети (чаще - в Instagram и «ВКонтакте») страницу якобы интернет-магазина с подозрительно низкими ценами. Когда жертва вносит предоплату или перечисляет всю стоимость товара, то оказывается в «черном списке» и больше не может связаться с продавцом.

Как не попасться? На странице найдите реквизиты продавца (как минимум, УНП, который должен указываться обязательно) и проверьте их на сайте kartoteka.by, поищите отзывы через поисковик.

Настаивайте на отправке с наложенным платежом (оплата при получении).

АРЕНДА КВАРТИР

Выставив низкую цену за аренду квартиры, мошенник ждет откликов. В переписке уверяет: интерес большой, чтобы оставить бронь - внесите предоплату. Дальше два пути: или бросает фейковую страницу и сразу крадет введенные данные карты, или дает реальные реквизиты своего пластика (усыпляет бдительность). Во втором случае будьте готовы получить сообщение об отмене сделки с извинениями и просьбой прислать информацию о счете якобы для возврата средств.

Как не попасться? Настаивайте на личной встрече для передачи денег под расписку.

Еще одна простая проверка - попросить созвониться: фальшивые «арендодатели» под разными предлогами избегают живых разговоров.

ЗАНЯТОЙ ПОКУПАТЕЛЬ

Человек активно интересуется товаром на торговой площадке (том же «Куфаре») и просит либо отправить посылку курьером (тяжело нести с почты/не может отлучиться с работы), либо прямо сейчас принять предоплату на карту. Следом в переписку летит фишинговая ссылка, где нужно указать данные карточки.

Как не попасться? Откажитесь от таких форм оплаты/доставки.

Не вводите данные карты (особенно - срок действия и CVV-код) на сайтах, куда перешли по ссылкам от незнакомцев.

Не соглашайтесь уходить с торговой площадки и продолжать переписку в другом приложении.

РОЗЫГРЫШИ И ЛОТЕРЕИ (=ОТДАМ ДАРОМ)

На почту или в личку приходят письма вроде «Вы сделали репост и выиграли приз!». Или кто-то на сайте-барахолке обещает отдать даром дорогой гаджет. Следом - условия получения: надо указать паспортные данные и заплатить за доставку (страховку).

Как не попасться? Не переходите ни по каким ссылкам из письма (даже если они якобы ведут к результатам игры). Через поисковик узнайте, действительно ли розыгрыш был проведен, есть ли другие призеры.

МНЕ ТОЛЬКО ПОЗВОНИТЬ

Человек просит ваш телефон срочно позвонить кому-то, потому как у него сел аккумулятор. Получив мобильный, мошенник быстро устанавливает на него следящее приложение. Как только вы решите войти в интернет-банкинг, вор перепишет данные и опустошит счет или прямо в личном кабинете возьмет кредит.

Как не попасться? Лучше вовсе не давать свой смартфон кому-то. Или набирайте номер сами и блокируйте экран, когда будете передавать гаджет для разговора.

Интернет-преступлений становится больше!