**Как обманывают мошенники. Схемы обмана/ ТОП 5 схем.**

Наверное, многим из вас звонили и представлялись работниками банка. Якобы оператор банка говорит вам о подозрительных действиях по вашему счету и просит вас озвучить номер карты и три цифры на обороте. Конечно. никакого списания не было и все это обман. Этот способ мошенничества стал очень популярным в последнее время. Но мошенники, словно изобретатели, постоянно придумывают что-то новое и более ухищренное.

**1) Фейковый сайт минздрава**



Мошенники публикуют в группах в соцсети "ВКонтакте" новости о якобы опасности вакцинации и таким образом заманивают пользователей на сайт-клон минздрава, а затем перенаправляют на ресурс, который крадет деньги.

Схема работает так: в комментариях к постам в популярных группах-миллионниках "ВКонтакте" злоумышленники публикуют фейковые новости о новом штамме коронавируса, ссылка ведет на сайт-клон Минздрава России с фейковым интервью министра здравоохранения Михаила Мурашко, в котором говорится о том, что новая волна пандемии якобы уничтожит до 80% страны и первыми жертвами станут люди, получившие вакцину. Далее, через несколько секунд, жертву с лжесайта минздрава перенаправляют на мошеннический сайт с розыгрышем или получением "крупного денежного перевода" в размере 237 568 рублей. Деньги можно вывести в течение 48 часов, но для этого необходимо ввести данные банковской карты.

Пользователям соцсетей нужно критически относиться к информации и быть особенно внимательными, переходя по ссылкам с сомнительным содержанием. При переходе на сайт необходимо обратить внимание на доменное имя ресурса - например, лжесайт минздрава отличается от настоящего. Вводите свои конфиденциальные данные и реквизиты банковских карт только на проверенных сайтах.

**2) Лжебанки**

Существует огромное количество лжебанков - ресурсов, которые маскируются под действующие кредитные организации. С начала 2021 года их количество выросло в 125 раз.

По статистике каждый двадцатый вызов с неизвестного номера - это звонок мошенника. Проверить банк и удостовериться в том, что данная организация добросовестная, можно на сайте ЦБ в разделе “проверить финансовую организацию”

Сейчас ЦБ совместно с поисковыми системами реализует совместный проект по маркировке сайтов добросовестных финансовых организаций с целью защиты интересов потребителей.

Сайты реальных организаций помечены цветным кружком с галочкой, при наведении курсора появляется надпись о внесении в реестр ЦБ РФ.

Число мошеннических ресурсов растет в связи с пандемией и удаленным использованием банковскими сервисами. но прежде чем оставлять какие-то данные убедитесь в добросовестности организации и внимательно посмотрите на домен сайта, если вы уже являетесь клиентом банка.

**3) Кредит с потерей жилья**



В России фиксируется новый тренд в финансовом мошенничестве, жертвы которого рискуют остаться с кредитом на руках и лишиться квартиры.

Преступники уговаривают россиян вместе с кредитом закладывать или продавать свои квартиры. И в результате люди остаются с кредитом и плюс без квартиры.

Сейчас предпринимают меры такие сотовые операторы МТС, "Билайн", "МегаФон", Tele2. Они тестирует свою систему верификации звонков.

Сейчас 90% банковского мошенничества - телефонное, а девять из десяти звонков происходят с подменой номера.

[К сожалению, никто не застрахован от обмана. Если вы или ваши близкие попали в непростую ситуацию из-за мошенников и вам необходима юридическая помощь, то обращайтесь в нашу компанию.](https://tonkiy.com/)

**4) Фишинг с автостраховками**



Специалисты "Лаборатории Касперского" обнаружили 56 фишинговых и скам-сайтов, в названии которых фигурирует слово osago.

На одном из таких сайтов пользователь хочет получить страховку. Он вводит данные автомобиля, получает список предложений, далее заполняет необходимые данные и оплачивает.

**Итог: водитель без страховки и денег.**

Проблема еще и заключается в том, что мошенникам удается продвигать свои сайты со страхованием и выводить их на первые строчки поисковиков.

Поэтому необходимо быть осмотрительными. особенно тем, кто желает быстро, выгодно и дистанционно оформить страховку.

На самом деле отличить мошеннический сайт от настоящего трудно. Но стоит обращать внимание на несоответствия. Например, ошибки в URL-адресах, наличие опечаток и использование посторонних элементов, неверных цветов в логотипах.

Домены, оканчивающиеся на .su, .net, .biz, .info .tv, .mobi, .org. - подозрительны.

**5) Кредит под низкий процент**

Финансовые мошенники под видом сотрудников банков начали предлагать гражданам оформить кредит под низкий процент (5%).

Далее злоумышленники присылают ссылку на якобы официальную онлайн-страницу банка, где нужно ввести логин и пароль. В результате мошенники получают доступ к данным жертвы. Для правдоподобности мошенники подключают к прозвону потенциальных жертв роботов.

Мошенники делают ставку на эмоции обманутого человека, который от радости не будет проверять достоверность информации и перейдет по ссылке и передаст все свои данные. После чего мошенники выводят деньги со счета.

И здесь в группе риска находятся именно те люди, которые заинтересованы в кредитных продуктах. И таких людей выявляют благодаря утечкам информации из банков или их партнеров.

*Теперь вы знаете о новых мошеннических схемах, непременно расскажите о них своим близким, чтобы обезопасить себя и не стать жертвой обмана.*

Напишите в комментариях, с каким видом мошенничества сталкивались вы или ваши близкие?

#схемымошенников #юристмосква #юридическаякомпания #фишинг