Грабли: истории о финансовых мошенничествах

По материалам сайта Fincult.info

История 1. «Поддержите разработку вакцины от коронавируса»

Довольно часто мошенники активизируются во время стихийных бедствий и эпидемий.

Они призывают людей делать пожертвования якобы для помощи пострадавшим. Часто обманщики маскируются под официальные организации.

Чтобы не попасться на уловки преступников, необходимо соблюдать правила кибербезопасности:

- не переходите по ссылкам из писем незнакомых отправителей;
- проверяйте адресную строку сайта - часто фишинговые сайты отличаются от официальных всего одной-двумя буквами;
- используйте отдельную карту для онлайн-платежей и кладите на нее нужную сумму непосредственно перед покупкой;
- установите на все свои устройства антивирус и регулярно обновляйте его. Хороший антивирусный пакет включает защиту от спама и фишинговых писем;
- если преступники уже получили данные вашей карты, заблокируйте ее и попросите банк выпустить новую.

История 2. «Купите золотые серьги – и получите кэшбэк 200%»

Эта история имеет все признаки финансовой пирамиды:

- обещают золотые горы: доходность в несколько раз выше того, что вы вкладываете;
- чтобы получать больше дохода, нужно привести как можно больше участников;
- ведется агрессивная реклама;
- факты о самой компании скрыты;
- людям предлагается не товар, а инвестиции, но у компании нет лицензии Банка России для работы на финансовом рынке, и она не имеет права привлекать деньги инвесторов.

Ювелирная пирамида предлагает прибыль в виде кэшбэка за покупку. Такую промоакцию **нельзя оспорить в суде**, ведь продавцы могут менять условия программы лояльности.

По закону серебряные и золотые украшения невозможно сдать назад, так что **вернуть потраченные деньги не получится**. Тем более **нельзя потребовать обещанного дохода**, ведь с покупателем не был заключен договор вклада, в котором зафиксированы проценты

История 3. «Срочно оплатите страховку, чтобы получить кредит»

Просьба внести **предоплату за кредит** — это явный **признак мошенничества**. Легальные финансовые организации не требуют от заемщика предоплаты или комиссии за одобрение кредита или займа.

Банк не может заставить вас купить страховку для оформления кредита. При оформлении кредита со страховкой вы вправе самостоятельно выбрать подходящую страховую компанию.

Как не попасться на уловки обманщиков?

Перепроверьте звонящего. Если вам звонят из незнакомого банка и делают заманчивое предложение, первым делом проверьте, есть ли у организации лицензия Банка России.

Не принимайте финансовые решения второпях. Мошенники специально подгоняют вас, чтобы вы не смогли проанализировать ситуацию. Если мошенникам все же удалось выманить у вас деньги, обращайтесь в полицию.

История 4. «Вы скоро обогатитесь, но сначала подскажите конфиденциальные данные»

Это типичный пример мошенничества от имени реально существующей организации. Злоумышленник нашел ФИО и номер телефона клиента в открытых источниках. Под предлогом «проверки доверенности» для «перевода в несколько тысяч евро» мошенник надеялся выведать персональные данные.

Чтобы не дать злоумышленникам обогатиться за ваш счет, следуйте правилам финансовой безопасности:

- никому ни под каким предлогом не диктуйте секретные данные: только мошенники просят назвать коды с обратной стороны банковской карты, ПИН-коды и пароли из СМС от банка;
- никогда не делитесь персональной информацией о ваших банковских счетах с незнакомыми людьми. Ни в коем случае не отправляйте копии своих документов компаниям, с которыми вы раньше не имели дела, пока не проверите информацию о них;
- если вам звонят от имени Банка России, позвоните на горячую линию и сообщите об этом: 8-800-300-3000. Вы также можете пожаловаться на мошенников через интернет-приемную.

История 5. «Введите номер СНИЛС и получите 120 000 рублей!»

Мошенники активно используют социальные сети, чтобы выманивать персональные данные пользователей: подделывают аккаунты известных СМИ, чтобы распространять объявления о социальных выплатах, конкурсах с денежными призами и т.п.

Чтобы избежать неприятностей, следуйте важным правилам финансовой безопасности:

- всегда перепроверяйте информацию из социальных сетей; если государство назначает выплаты и компенсации, то необходимо найти сам закон и изучить его;
- не доверяйте конкурсам, опросам, в особенности если требуется что-либо оплатить;
- не спешите переводить деньги неизвестным получателям и никогда не переходите по ссылкам от незнакомцев;
- не вводите на сомнительных сайтах конфиденциальные данные;
- подключите СМС-оповещения или push-уведомления об операциях по карте; в этом случае вы сразу же узнаете о платеже, который вы не совершали, и сможете заблокировать карту;
- установите антивирус на всех своих гаджетах — это поможет защитить их от вредоносных программ.

История 6. «У вас долг по ЖКХ, закройте немедленно»

Сообщение о задолженности по ЖКХ, уводящее на фальшивый сайт, - классический пример СМС-мошенничества.

К преступникам попала база данных жильцов дома, они подделали страницу сайта управляющей компании и принялись рассылать СМС. Расчет мошенников простой: из тысячи человек несколько что-нибудь да переведут.

Как поступить, если пришло сообщение о задолженности?

- Сделайте паузу, прежде чем совершать какие-либо операции с деньгами. Если вы исправно оплачиваете услуги ЖКХ, подобное сообщение – повод насторожиться.
- Не отвечайте на СМС, не перезванивайте по номеру, не переходите по ссылкам.
- Позвоните в управляющую компанию или ТСЖ и объясните, что произошло.
- Если вы перевели деньги мошенникам, подайте заявление в полицию, указав все известные вам данные об отправителе: номер, адрес сайта, время рассылки. Если вы отправили злоумышленникам персональную информацию (ввели номер карты, имя с лицевой стороны и код с обратной стороны, срок действия), позвоните в банк и заблокируйте карту.

История 7. «Суперпредложение – круиз за полцены»

На самом деле путешествие было лишь рекламной уловкой. Мошенники преследовали только одну цель – убедить как можно больше людей принести им свои деньги. Злоумышленники зарегистрировали компанию-однодневку и сняли временный офис. Как только они собрали нужную сумму – исчезли.

Чтобы распознать обман, важно следовать основным правилам финансовой безопасности:

- не стоит слепо доверять рекламе, под громкими и заманчивыми акциями нередко скрываются сомнительные предложения, которые на деле не приносят выгоды;
- проверяйте сведения о компании; найдите данные о ней на сайте Федеральной налоговой службы – там есть информация обо всех компаниях, зарегистрированных в России;
- найдите компанию в официальных реестрах, например, финансовая организация обязательно должна быть в реестре Банка России, туроператор – в реестре Ростуризма;
- изучите отзывы о компании в интернете;
- внимательно читайте договор; изучите, какие обязательства берет на себя компания и что будет, если она их не выполнит.

Если вы стали жертвой финансового мошенничества:

- соберите все документы, которые у вас есть: договоры, заключенные с посредником-мошенником, чеки на перевод денег, сделайте скриншоты с сайта – и отправляйтесь в полицию писать заявление;
- сообщите в Банк России, все жалобы рассматриваются.

Составитель:
Елена Слепова

ГБУК РО «Библиотека им. Горького»
Отдел правовой информации и образовательных ресурсов
rounb_odpi@mail.ru