Как уберечься от кибермошенников!?!?!

Ежегодно в марте во всём мире отмечается Всемирный день защиты прав потребителей. Его проведение направлено на привлечение внимания общественности к той или иной актуальной проблеме, повышение осведомленности потребителей о способах защиты их прав.

В 2022 году Международная организация потребителей (Consumers international) предложила провести Всемирный день защиты прав потребителей под девизом «Fair Digital Finance - «Справедливые цифровые финансовые услуги».

В последние годы в связи с постоянно растущей популярностью безналичных платежей стало очевидно, что скорость развития мошеннических систем в финансовой сфере существенно превышает скорость построения защиты от противозаконных действий.

Роспотребнадзор неоднократно указывал, что требуется изменение механизмов защиты прав потребителей финансовых услуг в связи с низким уровнем безопасности операций по переводу денежных средств.

Мошенники практически ежедневно изобретают новые способы хищения у пользователей личной информации (номеров банковских карт, паспортных данных, паролей, кодов), чтобы получить доступ к банковскому счёту или придумывают схемы по выманиванию денег у граждан.

Количество денежных переводов без согласия клиентов банков ежегодно растет. Две трети несанкционированных операций произошло при оплате товаров и услуг в интернете. Пострадавшие от действий аферистов получили назад всего 7,4% от украденных денег. Доля возвратов невелика, так как клиенты чаще всего сами выдают мошенникам секретные данные для доступа к счетам, а в таких ситуациях банки ничего не компенсируют.

В последнее время получил широкое распространение так называемый фишинг – вид интернет-мошенничества, который используется для получения идентификационных данных пользователей. К примеру, вам приходит сообщение или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код карты или номер из СМС-подтверждения.

Если вам приходит сообщение о зачислении средств, которое похоже на обычное уведомление банка, а затем звонит человек, который якобы по ошибке зачислил вам деньги и просит вернуть, не спешите этого делать. Скорее всего, это происки злоумышленников. Обязательно проверьте состояние вашего счёта, закажите выписку о движении денежных средств или позвоните в банк.

Также мошенники научились списывать деньги с карты под видом продажи билетов на концерты, в театр и кино. Аферисты по электронной почте, через мессенджеры и соцсети рассылают фейковые предложения о продаже билетов. Но вместо пропуска на мероприятие человек покупает подписку, которая позволяет мошенникам списать все деньги с его карты. [Фишинговая](https://fincult.info/article/fishing-chto-eto-takoe-i-kak-ot-nego-zashchititsya/) ссылка из сообщения ведет на страницу оплаты, где нужно вбить персональные сведения и реквизиты карты. Если человек вводит данные, он фактически оформляет подписку на «услуги» мошенников. С карты жертвы тут же списываются деньги.

Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.

Есть такое понятие как социальная инженерия, или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить денежные средства и/или конфиденциальную информацию. Мошенники часто представляются сотрудниками банков, налоговой службы, [юридических контор](https://fincult.info/article/zachem-moshenniki-vydayut-sebya-za-yuristov/) и [других официальных организаций](https://fincult.info/article/moshennichestvo-ot-imeni-bankov-gosudarstvennykh-uchrezhdeniy-ofitsialnykh-lits/). Даже

самые умные и осторожные люди иногда попадаются на крючок к таким махинаторам. Вам звонит якобы ваш родственник и сообщает о том, что ему срочно нужны деньги в долг или он задержан правоохранительными органами, например, за совершение ДТП, незаконное хранение наркотиков, причинение телесных повреждений другому лицу. Не поддавайтесь на обман: в первую очередь прервите разговор и перезвоните родственнику, близкому человеку, чтобы поинтересоваться, все ли с ним в порядке. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями и родными для уточнения информации.

Ещё один относительно новый вид мошенничества – кража данных с портала Госуслуг. Пользователи портала начали получать сообщения о техническом сбое, из-за которого их якобы открепили от поликлиники. Ссылка из письма мошенников ведёт на [фишинговый](https://fincult.info/article/fishing-chto-eto-takoe-i-kak-ot-nego-zashchititsya/) сайт – двойник портала Госуслуг, где посетителя просят заполнить анкету с личными данными, в том числе указать логин и пароль от личного аккаунта. Затем человеку предлагают выбрать медицинское учреждение из списка и заплатить за повторное прикрепление пошлину – до нескольких тысяч рублей. В итоге вместе с деньгами преступники получают доступ ко всем персональным данным пользователя. Они могут продать эту информацию на черном рынке другим мошенникам, а также [набрать займов и кредитов](https://fincult.info/rake/poteryal-telefon-otdavay-million/) на имя владельца учётной записи. Вернуть деньги в таком случае практически невозможно: если пользователь нарушил правила кибергигиены и сам сообщил аферистам секретную информацию, банк [не обязан](https://fincult.info/article/chto-delat-esli-s-bankovskoy-karty-ukrali-dengi/) ничего компенсировать.

Если вы получили уведомление об откреплении от поликлиники, необходимо проверить, есть ли оно в вашем личном кабинете на Госуслугах. Обязательно нужно самостоятельно набрать [адрес портала](https://www.gosuslugi.ru/), а не переходить по ссылке из сообщения от незнакомцев.

Есть такое понятие как кибергигиена – комплекс правил цифровой безопасности при работе с интернетом. Для того, чтобы защитить свои деньги и персональные данные, необходимо придерживаться некоторых правил.

Никогда не переходите по ссылкам из электронных писем, сообщений в мессенджерах, СМС или рекламных объявлений. Безопаснее самостоятельно найти официальный сайт компании, услугами которой вы хотите воспользоваться. Для [онлайн-покупок](https://fincult.info/article/bezopasnye-pokupki-v-internete/) лучше завести отдельную карту и каждый раз вносить на нее необходимую для покупки сумму либо установить лимит по количеству и размеру операций. Совершайте покупки и заходите в свой интернет-банк или мобильный банк только с личного компьютера, планшета или смартфона, обязательно установите на них пароль и антивирусную программу и регулярно обновляйте их.

Никому не сообщайте персональные данные, тем более пароли и коды от банковских карт. Не храните данные карт на компьютере или в смартфоне.

Всегда проверяйте адресную строку сайта, на котором вы вводите свои платежные или личные данные. Ещё лучше – сохранить в закладках страницы, которыми вы пользуетесь, или заходить в них через проверенные приложения.

**Подключите СМС-оповещения об операциях по карте.** Если вы получили СМС с кодом подтверждения покупки, которую не совершали, или сообщение с кодом на восстановление пароля карты, сразу же созвонитесь с банком. Возможно, вам посоветуют заблокировать карту и перевыпустить её. Так же нужно поступить, если вы потеряли карту или даже просто подозреваете, что её данные стали известны посторонним людям. Если деньги с карты были действительно списаны, нужно в течение 24 часов обратиться в банк с заявлением о том, что операция была совершена без вашего согласия. Финансовая организация проведет расследование и компенсирует потерянные деньги, но при условии, что вы не передавали мошенникам данные своей карты.

Также следует обратиться в отделение полиции по месту жительства, написав заявление. Чем быстрее вы это сделаете, тем больше шансов найти преступников и вернуть деньги.

Будьте предельно внимательны и осторожны, соблюдайте правила кибергигиены. Это защитит ваши денежные средства от действий киберпреступников и телефонных мошенников.