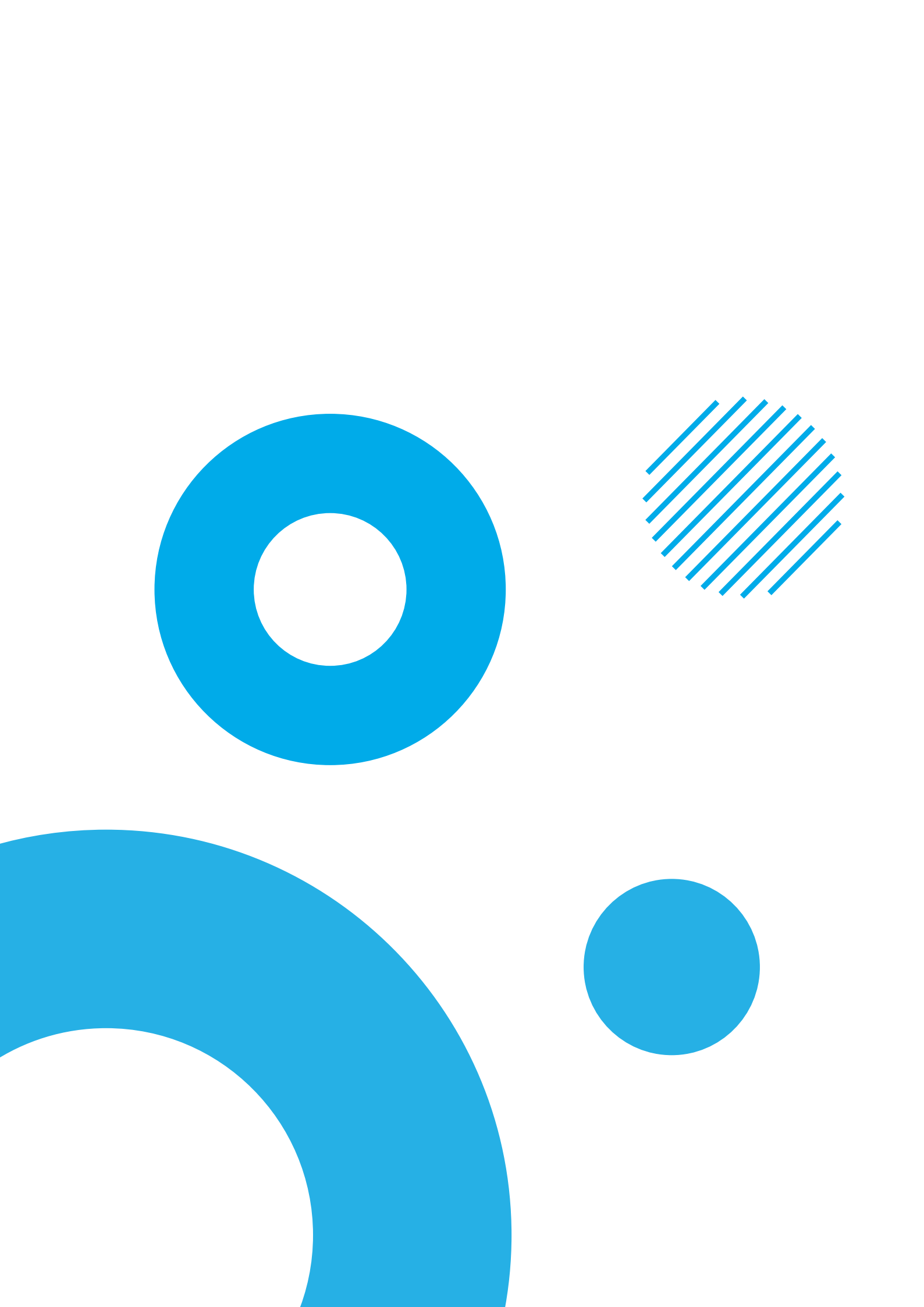
ПОБЕДИМ ТЕЛЕФОННЫХ МОШЕННИКОВ!

Когда мошенники звонят жертве, они пытаются обманом, манипуляцией или запугиванием заставить человека сделать то, что им нужно – перевести деньги или передать свои персональные данные. Почти все жители России хотя бы раз в своей жизни сталкивались с телефонным мошенничеством. По данным ВЦИОМ , в 2022 году 83% россиян столкнулись со звонками или смс-сообщениями от мошенников. Это на 7% больше, чем в 2021 году.

Персональные данные человека сами по себе представляют большую ценность!



Популярные схемы мошенничества:

1. **Звонок от имени сотрудника банка,** службы безопасности, бюро кредитных историй, оператора сотовой связи, правоохранительных органов, Центробанка или любой другой уполномоченной организации. Прикрываясь именем организации, люди убеждают клиентов в необходимости совершения определенных действий – выдаче данных карты, переводе денег, сообщении пароля или кода из СМС.
2. **СМС с просьбой о помощи.** Обычно СМС приходит от имени человека, который вам хорошо знаком – сестры или брата, ребенка или родителя, другого родственника. Вместо СМС мошенники могут позвонить, сказав, что ваш родственник попал в беду. Предлоги разные: попал в аварию, задержан за преступление, которого не совершал и оказался в полицейском участке. В этом случае мошенники просят деньги, например, чтобы выпустить вашего родственника «под залог» или чтобы его положили в больницу. Мошенники рассчитывают, что напуганная жертва не будет перепроверять информацию и не догадается перезвонить своему родственнику, чтобы уточнить, правда ли это.
3. **Сообщение с просьбой перезвонить.** На телефон приходит СМС, сообщение в мессенджере или даже письмо на почту от имени какой-либо организации. Такое сообщение может выглядеть как настоящее уведомление от банка или государственных органов. В нем будет написано о подозрительных операциях на вашем счете, снятии денег с карты, взломе личного кабинета и так далее. Также в сообщении будет указан номер телефона самого банка или другой организации, по которому вам нужно позвонить, чтобы разобраться в произошедшем, вернуть деньги или отменить операцию. Если жертва позвонит по указанному номеру, то вместо банка попадет к мошенникам.

Внимание!

Звонки, как и сообщения, могут поступить абсолютно с любого номера – настоящего номера банка, полиции, организации. Сегодня с помощью специальных программ можно подделать абсолютно любой номер.

Чего мошенники добиваются звонками:

1. **Пытаются обманом заставить перевести деньги.** Мошенники могут рассказать вам, что ваши средства в опасности, а для того, чтобы защитить их, необходимо перевести все на некий «резервный» счет, который откроют специально для вас. Разумеется, никакого резервного счета не существует. Если согласиться и сделать перевод, деньги отправятся к мошенникам.
2. **Пытаются получить персональные данные** и другую ценную информацию. Вместо того чтобы заставить человека перевести деньги, мошенники могут узнать его банковские реквизиты и перевести все деньги самостоятельно. Помните, что даже незначительная, на ваш взгляд, информация, может представлять ценность для мошенников. Если они не смогут украсть с ее помощью карты сейчас, то в будущем используют ее для подбора другой схемы. Такой информацией может быть даже запись вашего голоса. Конечно, мошенники не смогут оформить кредит на ваше имя, просто записав, как вы произносите «Да», «Согласен» или «Подтверждаю», но это может помочь им обойти защиту банка и получить доступ к вашему личному кабинету.
3. **Пытаются получить доступ в мобильный банк.** С этой целью мошенники могут, например, отправить вам СМС с кодом доступа и попросить вас сообщить его под любым предлогом.
4. **Обманом пытаются заставить установить вирусную программу,** которая или будет шпионить за вашим устройством, или вообще предоставит мошенникам полный доступ к устройству.

К сведению!

На современных телефонах Android присутствует встроенная бесплатная защита от спама. Чтобы включить ее, откройте приложение «Телефон», нажмите на значок «Еще» (выглядит как три точки), выберите пункт «Настройки», затем «АОН и спам». Включите пункт «Фильтровать спам-вызовы». На телефонах «Apple» встроенной защиты от спама нет, однако можно загрузить приложения для фильтрации мошеннических и спам-звонков.

Как можно обезопасить себя от телефонных мошенников?

1. **С осторожностью относитесь к звонкам с незнакомых номеров.** Если есть возможность, лучше вообще не отвечать на них. Чаще всего, такие звонки – либо спам, либо мошенники.
2. **Будьте внимательны и с осторожностью относитесь к тому, что вам говорят по телефону незнакомые люди.** Независимо от того, кем представляется собеседник и что он вам говорит. Мошенник может открыть сайт МВД и найти там имя настоящего сотрудника, чтобы представиться им. Он может рассказывать вам что угодно, что вы могли стать свидетелем преступления, что нужна ваша помощь для поимки мошенников, что у вас хотят украсть деньги со счета.
3. **Не ведите с мошенниками разговоров.** Если думаете, что вам позвонили мошенники – вешайте трубку и блокируйте номер. Многие мошенники являются опытными манипуляторами. Чем дольше вы с ними разговариваете, тем сильнее рискуете случайно выдать какую-нибудь важную информацию. Даже если вам кажется, что в этом нет ничего страшного и эта информация бесполезна, для мошенника она может оказаться очень ценной.
4. **Подключите функцию защиты от спама на телефон.** Рекомендуем сделать это в том случае, если подобные звонки происходят слишком часто. В магазинах приложений Play Market (для Android) и App Store (для iOS) вы можете найти приложения, как платные, так и бесплатные, которые фильтруют ваши входящие звонки, определяет среди них спам или мошенников. Лучше всего обратиться к приложениям от известных и крупных организаций. В любом случае, такое приложение будет получать доступ к списку ваших звонков. Если его разработчик надежен, то это значит, что ваши данные с меньшей вероятностью подвергнутся утечке.

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт ligainternet.ru