Как защитить себя и близких от киберзлодеев. Инструкция от Сбера

Во втором квартале 2023 года банки отразили больше 6,5 млн атак на счета клиентов и спасли 911 млрд руб. Но все же мошенники смогли похитить 3,6 млрд.

Вместе со специалистами Сбера подготовили инструкцию по кибербезопасности: рассказываем, как защитить себя и близких от кибермошенников, как заблокировать спам и проверить подозрительный телефон, куда жаловаться, если вас атакуют злоумышленники.

Как проверить, кто вам звонил

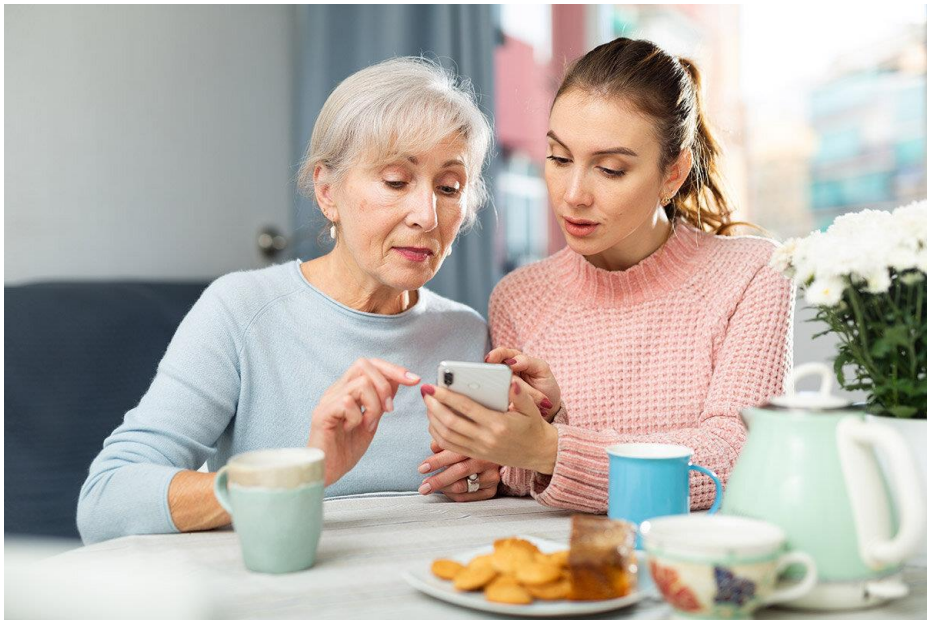
Мошенники обычно представляются сотрудниками банков или силовых структур, ссылаются на статьи законов. Могут угрожать потерей денег, торопят, создают эффект паники. Вот типичные фразы, которые вы можете услышать от мошенника по телефону:

- Продиктуйте код для отмены мошеннической операции.
- С вашего счета хотят перевести деньги в другом городе.
- Зафиксирована попытка войти в Ваш личный кабинет.
- На вас хотят оформить кредит, нужно перевести деньги на безопасный счет.

Все это — фразы, которые никогда не произнесут реальные сотрудники. Лучший способ защититься от таких мошенников — сразу класть трубку и самостоятельно перезвонить на номер своего банка (в Сбере это 900), реальные сотрудники подскажут, что делать.

На звонки злоумышленников можно и не отвечать — подключите бесплатный определитель номера в приложении «СберБанк Онлайн». Если номер есть в базе банка, вы увидите предупреждение. Или проверяйте номер по нашей онлайн-базе вручную.

Как защитить близких



Мошенников в первую очередь интересуют некомпетентные или невнимательные люди, которых легко напугать специальными юридическими терминами. Под прицелом в первую очередь пожилые.

Понятно, что мы не можем быть с близкими постоянно. Зато можем подключить сервис «Проверка переводов близкого» от Сбера — например, если родной человек захочет перевести кому-то деньги, банк пришлет вам уведомление. Вы сможете подтвердить или отклонить перевод, если он показался вам подозрительным.

Как проверить себя по базам известных утечек

Мошенники берут наши номера или адрес электронной почты не из воздуха — обычно это они используют утечки баз данных в разных сервисах.

Через СберБанк Онлайн можно узнать, есть ли ваши контакты в таких базах. На главном экране приложения найдите «Безопасность» → «Проверка номера и почты». Для проверки используются основной телефон и адрес электронной почты из профиля СберБанк Онлайн.

Как могут обмануть на сайте бесплатных объявлений

Мошенники часто притворяются продавцами и просят перевести предоплату за товар или оплатить доставку «более удобным» способом, через сторонний ресурс. Регулярно предлагают перейти общаться в мессенджеры, а там присылают ссылку на поддельную страницу оплаты за товар или доставку. Вы вводите данные своей банковской карты (имя, номер карты, срок действия, трехзначный код на обороте), и они оказываются у мошенников.

Продавцы тоже под прицелом: злоумышленники под разными предлогами будут просить данные ваших карт — имя, номер карты, срок действия, трехзначный код на обороте, код из СМС. Запомните, для перевода вам денег покупателю не нужны никакие данные, кроме номера телефона или номера карты (без срока действий и кодов).

Как быть, если «сотрудник банка» просит установить приложение или зайти на сайт

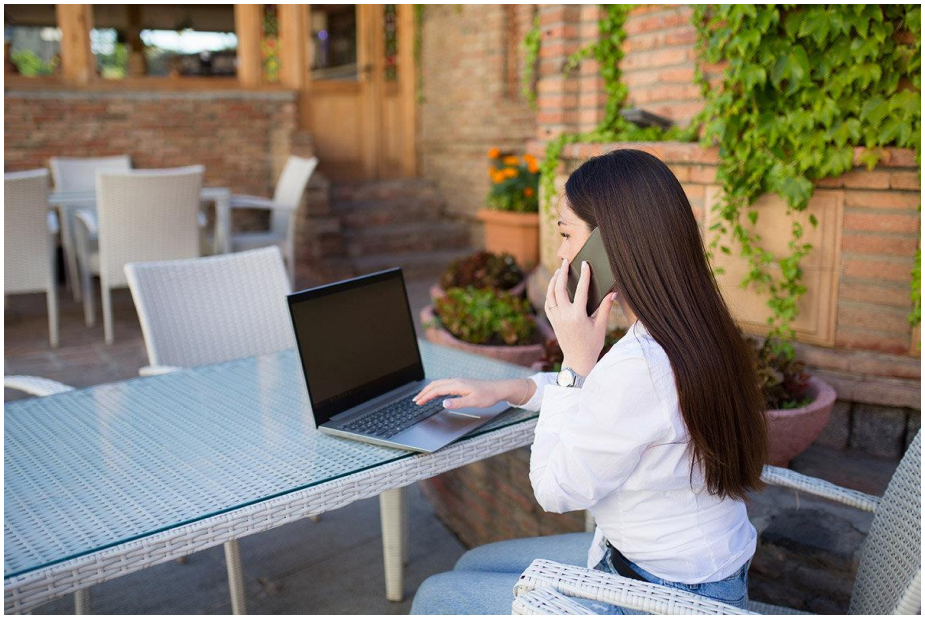
Если вам позвонил якобы сотрудник банка или робот и просит установить что-то на телефон или компьютер — это точно мошенник!

- Сразу прекращайте разговор.
- Не совершайте никаких операций и действий по инструкциям звонящего.
- Звоните в банк сами и узнавайте, что вам делать.

Сотрудник банка никогда не попросит вас установить что-то на ваше устройство, например, антивирус или программы для удаленного доступа.

Официальное приложение банка вы можете установить сами, но для этого нужно пользоваться официальным сайтом банка, на который вы перешли сами, без ссылок от якобы сотрудников. Или установите официальные приложения банка из магазинов RuStore, App Store, Google Play.

Что делать, если я выиграл приз



Мошенники могут обмануть не только через телефонные звонки, но и с помощью мессенджеров или электронной почты. Например, вам может прийти письмо якобы от банка или другой организации: «Вы выиграли приз…» или «Поздравляем с днем рождения, подготовили вам подарок». По ссылке обычно нужно ввести номер карты — якобы чтобы получить приз.

Ни в коем случае не делайте этого. Это распространенная схема мошенничества, когда от имени банка мошенники направляют информацию о предполагаемой выплате. Не переходите по подозрительным ссылкам, не вводите данные своей карты на подобных сайтах.

Как быть, если мошенники получили доступ к данным

Опасной можно считать ситуацию, если вы продиктовали мошенникам номер и другие данные карты, сообщили код из СМС, рассказали пин-код для приложения банка. Действовать нужно быстро.

Заблокируйте карты и счета через приложение, чтобы никто не смог потратить с них деньги. Зайдите на главный экран СберБанк Онлайн → «Безопасность» → «Закрыть доступ». Или позвоните по номеру 900.

Сообщите о мошеннике. Если вас попытались обмануть или вы пострадали от действий мошенников, сообщите об этом в банк. Клиенты Сбера могут позвонить на номер 900.

Как защитить себя и близких от киберзлодеев. Инструкция от Сбера

https://dzen.ru/a/ZcYSGOTpV1GGKKkd