ГАЗПРОМБАНК

ЧЕК-ЛИСТ

Как распознать мошенника?

О попытке мошенничества вы можете сообщить по телефону **8 800 100 07 01** (бесплатно по России) или **400** (бесплатно с мобильных для всех городов России).

Номер телефона не вызывает подозрений

Раньше мошенники звонили со скрытых номеров — уже так можно было определить злоумышленника. Банковские сотрудники всегда звонят с официальных номеров, указанных на сайте. Но сейчас мошенники используют айпи-телефонию и подставляют **любые номера** — банков, ФСБ, следственных органов.

Что делать?

Кладите трубку и перезванивайте по официальным номерам. Вы попадете к специалистам и узнаете, были ли звонки.

Мошенник не отвечает на вопросы

Как работает банковский сотрудник? У него есть вся информация о вашем счете в банке. Он может назвать номер карты (последние 4 цифры), ваши имя и фамилию, сумму, которую вы снимали последней, и в каком городе это было. Он уточняет данные и **никогда не спросит** секретной информации.

Как работает мошенник?

Мошенник может знать ваше ФИО и другие данные, украденные из разных источников, но всей информации у него нет, поэтому он спрашивает номер вашей карты и CVV-код. Он не знает точно, сколько у вас денег на карте и какие операции были за последние сутки.

Создание тревоги и спешки

Мошенник **всегда будет вас торопить**. Даже в СМС-сообщениях от мошенников всегда есть спешка: «Срочно! Быстро! Нельзя терять время!»

Мошенники нагнетают обстановку и пугают штрафами и потерей еще больших денег.

Что делать?

Не спешить. Несколько минут ничего не решают. Вешайте трубку и перезванивайте в банк. Настоящий сотрудник банка никогда не будет вас торопить.

Быстрая выгода

Мошенники **всегда обещают доход**, ради которого не нужно предпринимать усилий. Например: выигрыш в лотерею, беспроигрышный конкурс, кредит с хорошей ставкой, работа с высокой зарплатой, куда можно устроиться, просто заплатив «за регистрацию в системе».

Так мошенники пытаются взять у вас предоплату или данные карты, чтобы якобы перевести деньги.

Низкая грамотность

Читайте внимательнее сообщения: мошенники присылают СМС и емейлы. У банков есть команда редакторов, вычитывающих каждую строчку, которая будет отправлена клиенту. А вот мошенники за грамотностью не следят, поэтому в их текстах обязательно будут опечатки, пунктуационные ошибки, несогласованные предложения.

Интерактивное голосовое меню

Мошенники могут переключить вас на IVR — интерактивное голосовое меню. Это делается для создания иллюзии безопасности. Кажется, что если диктуешь данные роботу, то никто ничего не узнает. Но на самом деле это не так.

Банк **никогда не попросит озвучить секретную информацию** по телефону и не переведет вас на голосовое меню, если с вашим счетом действительно что-то случилось.

Поймаем мошенника вместе

Мошенники представляются сотрудниками внутренней службы безопасности, полиции, ФСБ и просят вас помочь найти нечестных сотрудников.

Сразу вешайте трубку!

Во-первых, вы не обязаны помогать ловить злоумышленников. А во-вторых, службы безопасности не привлекают клиентов банков к таким операциям.

Общие рекомендации

1. При подозрительных звонках сразу кладите трубку и перезванивайте на официальные номера банка, указанные на сайте.
2. Не платите вперед.
3. Не отправляйте фотографии паспорта и других документов неизвестным людям.
4. Проверяйте домен сайта, прежде чем совершать оплату.
5. Внимательно читайте сообщения: если есть ошибки, то это с большой вероятностью злоумышленники.
6. Не переходите по ссылкам с неизвестных номеров.
7. Установите антивирус на компьютер и мобильные устройства.