Информация, которую нельзя раскрывать по телефону 1

Персональные данные

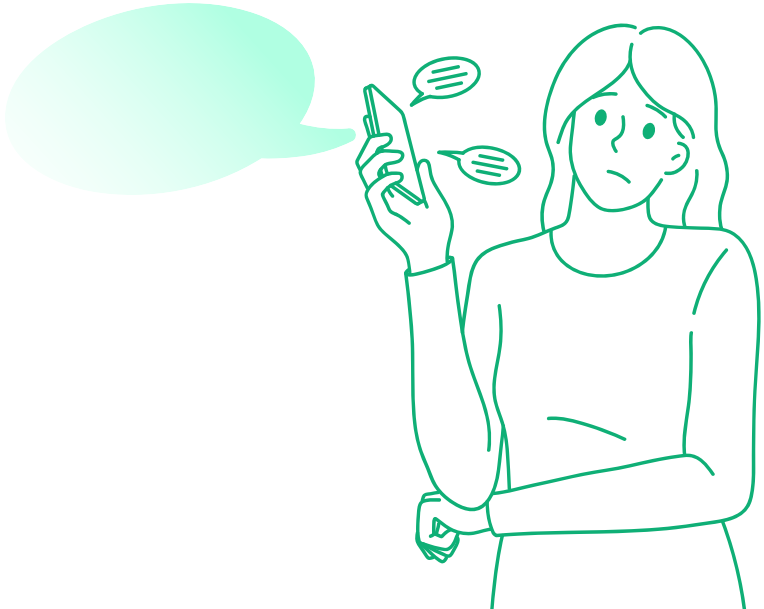
- ФИО
- Адрес регистрации или проживания
- Данные документов: паспорта, СНИЛС, ИНН

Банковские данные

- Номер карты
- Три цифры на обороте (CVV-код)
- Список последних операций по карте
- Коды из смс- и пуш-уведомлений
- Кодовое слово
- Остаток на счёте

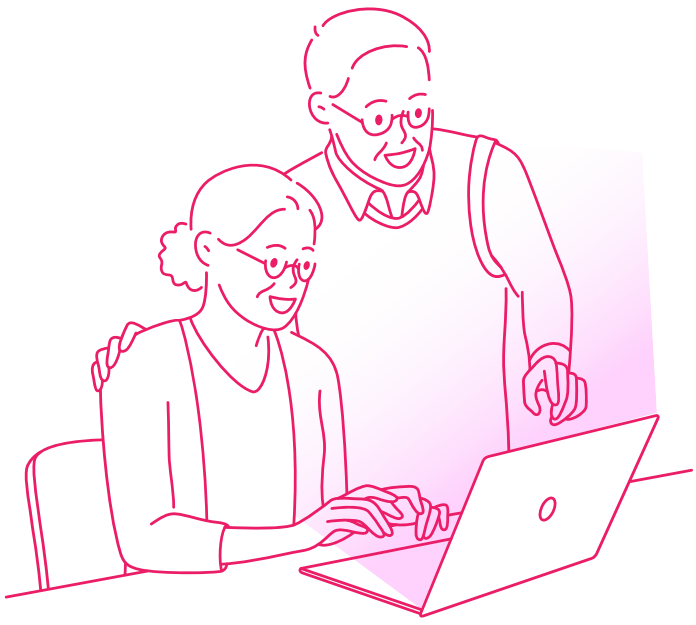
Фразы, которые говорят только мошенники 2

- Назовите номер вашей карты
- Назовите код из смс от вашего банка
- В каких банках вы ещё обслуживаетесь?
- Сколько средств у вас на счёте?
- Рядом с вами сейчас находится кто-то? Для банка они являются третьими лицами и не допускаются к операции
- Назовите ваш логин и пароль
- Какое у вас кодовое слово?
- Ваш сын попал в беду, а вы бросаете трубку. Вы не хотите ему помочь?



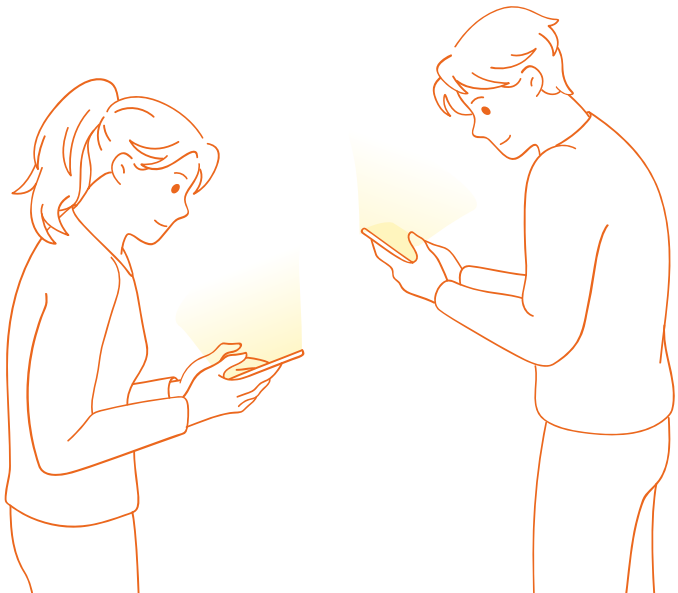
Как создать надёжный пароль 3

- Задайте пароль длиной 12 и более символов
- Используйте верхний и нижний регистр, числа и специальные символы
- Используйте случайные комбинации
- Откажитесь от простых комбинаций букв и чисел — qwe123
- Не берите за основу публичную информацию: девичью фамилию матери или дату рождения
- Используйте фразу, которая связана с жизненной ситуацией и легко запоминается, например «Я_обожаю_эклеры_с 10_лет!»



Как защитить мобильное устройство 4

- Настройте блокировку экрана
- Установите программу для удалённой блокировки устройства
- Используйте антивирус
- Обновляйте операционную систему и приложения
- Не устанавливайте приложения из непроверенных источников
- Не переходите по подозрительным ссылкам
- Не давайте приложениям разрешения, которые им не нужны для нормальной работы
- При подключении к бесплатному вайфаю не пользуйтесь критически важными приложениями, например Госуслугами, банковскими приложениями, почтой, соцсетями



Советы для юных пользователей интернета

5

- Используйте уникальные и надёжные пароли
- Включите двухфакторную аутентификацию для защиты аккаунтов, например по смс
- Настройте приватность в соцсетях
- Блокируйте пользователей, которые преследуют вас негативными комментариями
- Не публикуйте в соцсетях информацию, которая может быть полезна преступникам
- Не общайтесь с незнакомыми людьми в интернете
- При подключении к бесплатному вайфаю не пользуйтесь критически важными приложениями, например почтой и соцсетями
- Не провоцируйте других и не отвечайте на агрессию в интернете

Как не стать жертвой фишинга 6

- Внимательно проверяйте адрес отправителя
- Ищите информацию об акциях или выплатах на официальных сайтах компаний и ведомств
- Изменяйте учётные данные, только когда самостоятельно заходите на сайт, а не по ссылке из письма
- Не переходите по подозрительным ссылкам
- Не устанавливайте приложения из непроверенных источников
- Не переходите по подозрительным ссылкам
- Не открывайте присланные файлы, если не уверены в отправителе
- Не устанавливайте приложения из сомнительных источников
- Будьте бдительны и повышайте киберграмотность