



Как узнать телефонных мошенников

Как осуществляется атака кибермошенников по телефону?



Уточняют информацию о наличии продуктов, деталях операций, пробуют выманить данные карт.



Угрожают потерей денег, данных, наступлением для вас кредитной или уголовной ответственности.



Торопят, создают эффект паники, подталкивают к быстрым действиям.



Используют специальную терминологию, ссылаются на статьи закона.

Как защититься

- 1 Запишите в контакты телефон своего банка
- 2 При первых признаках мошенничества прекратите разговор
- 3 Не совершайте никаких операций по инструкциям звонящего
- 4 Не перезванивайте на незнакомые номера
- 5 Отказывайтесь. Уверенно говорите «нет»
- 6 Включите в СберБанк Онлайн проверку телефонных номеров

Запомните распространённые фразы мошенников

- Голосовой помощник: «Сообщите СМС-код»
- Продиктуйте код для отмены мошеннической операции...
- Примите участие в расследовании. Никому о нём не рассказывайте. Помогите поймать нечестного сотрудника...
- Для сохранности ваших денежных средств мы откроем специальную ячейку, на которую будут переведены ваши деньги на время проведения расследования...
- В каких ещё банках у вас открыты счета?
- С вашего счёта хотят перевести деньги в другом городе...
- Робот: «Ваша карта заблокирована, перезвоните, пожалуйста, по номеру...»
- Ваши средства находятся в опасности. Чтобы избежать финансовых потерь, необходимо перевести сбережения на безопасный счёт
- На вас оформили кредит...
- Зафиксирована попытка войти в ваш личный кабинет...
- Давайте уточним остаток средств на вашей карте...
- Надо установить специальное мобильное приложение, которое поможет ликвидировать вирусы и защитит ваши средства...

Что изучить ещё



Узнайте больше о существующих схемах обмана



Больше информации — в библиотеке знаний по кибербезопасности «Кибрарий»