# Противодействие IT-преступлениям

# Основные виды дистанционных хищений

# Социальная инженерия

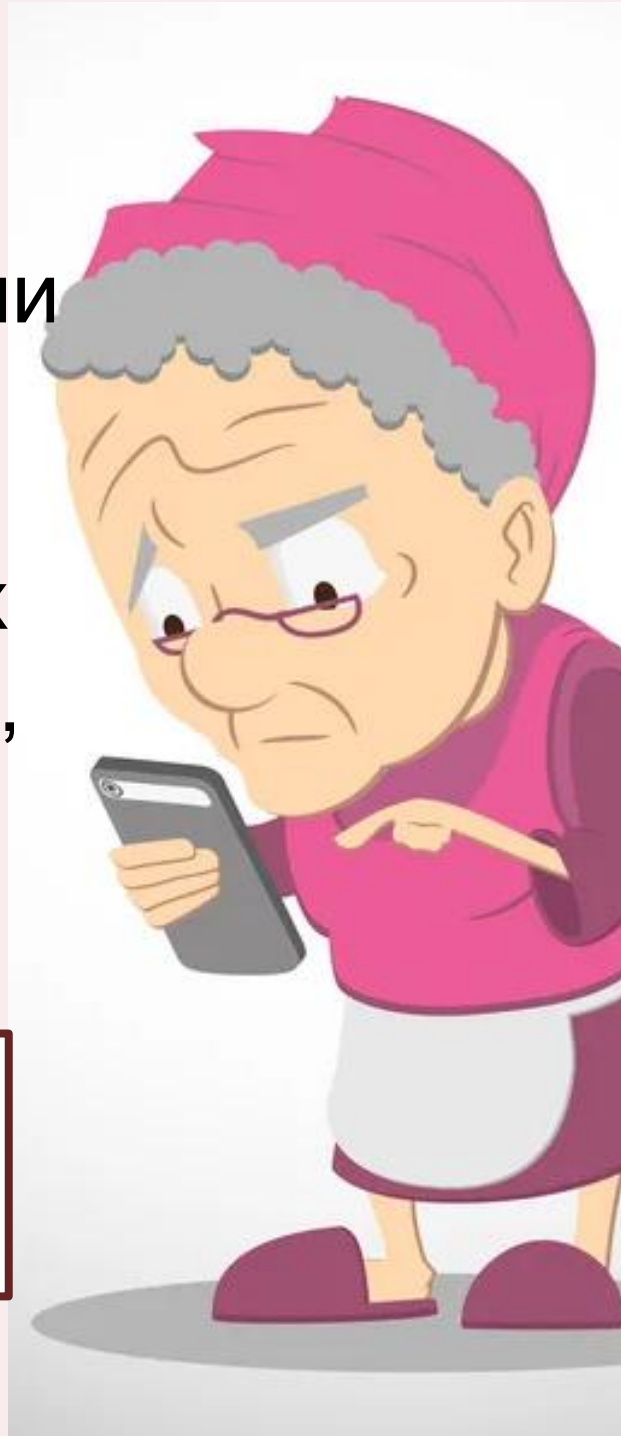
Социальная инженерия-обман на доверии

Злоумышленник вводит в заблуждение жертву и та выполняет его инструкции, сама отдает ему деньги либо пароль от личного кабинета в онлайн-банк

**НЕ ОТКРЫВАЙТЕ ДВЕРЬ**

незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д.

Перезвоните и уточните, направляли ли к Вам этого специалиста!



**НЕ ДОВЕРЯЙТЕ**, если Вам звонят и сообщают, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства – в общем откупиться.

**Это ОБМАН!**

# СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ

Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на вашу квартиру!

Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким «льготным» ценам?

**НЕ ВЕРЬТЕ-ЭТО МОШЕННИЧЕСТВО!**

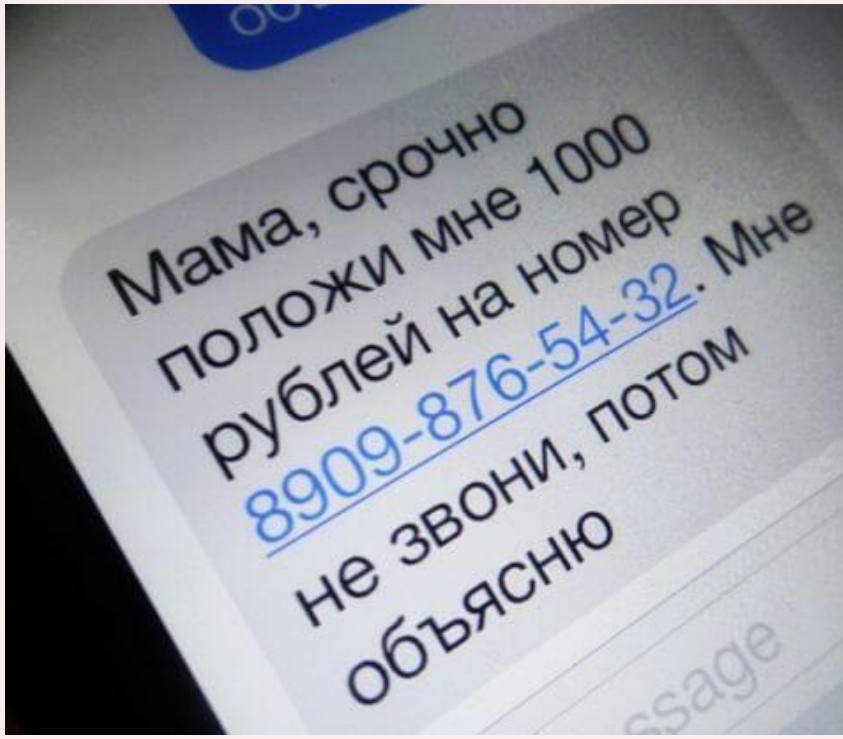
# Телефонное мошенничество

# Поступил сомнительный звонок? Вам необходимо:

- Прервать разговор и перезвонить тому, о ком идёт речь
- Если телефон отключен, связаться с его друзьями и родственниками для уточнения информации
- Если разговор происходит якобы с представителем правоохранительных органов, узнать, из какого он подразделения
- Набрать 02 и уточнить в дежурной части названного Вам подразделения, действительно ли родственник туда доставлен

# SMS, сообщения-просьба о помощи

Пожилым людям, детям и подросткам следует объяснить, что на сообщения с незнакомых номеров реагировать нельзя, это могут быть мошенники!



# Телефонный номер-грабитель

Мошенники регистрируют сервис с платным звонком без предупреждения абонента о снятии платы за звонок.

Будьте бдительны, совершая звонок по чужой просьбе!

# Выигрыш в лотерею

Необходимо помнить, что человек не может выиграть приз, не участвуя в лотереях.
**Это обман.**
Не стоит отвечать на данные сообщения, а тем более отправлять информацию о своей банковской карте и переводить денежные средства

# «Ошибочный» перевод средств

Если Вас просят перевести якобы ошибочно переведённую сумму, посоветуйте с чеком о переведённой операции обратиться в отделение банка.

Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

# Деньги за онлайн-опрос

# Бесплатный адвокат

Если Вам предлагают просто так что-то очень выгодное, то, скорее всего, это обман. Не нужно верить таким предложениям

# Компенсация от «Минздрава России»

# Компенсация от «Минфина России»

Необходимо помнить, что мошенники рассылают подобные фейковые сообщения от различных государственных органов. Не поддавайтесь на их уловки!

# Мошенничество с банковскими картами


Ни одна организация, включая банк, не вправе требовать Ваши CVC-код или ПИН-код.

Для того, чтобы проверить поступившую информации о блокировке карты, следует позвонить в клиентскую службу поддержки банка

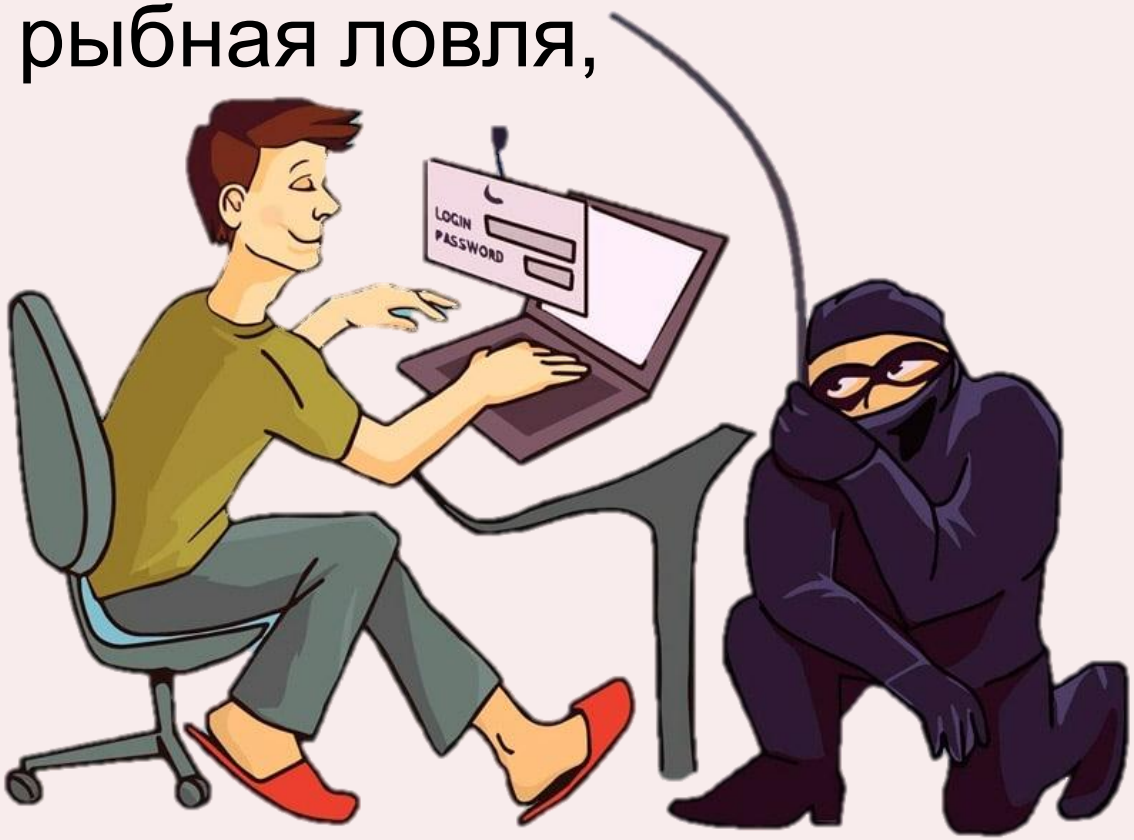
# Правила безопасности при обращении с банковскими картами

НЕЛЬЗЯ:

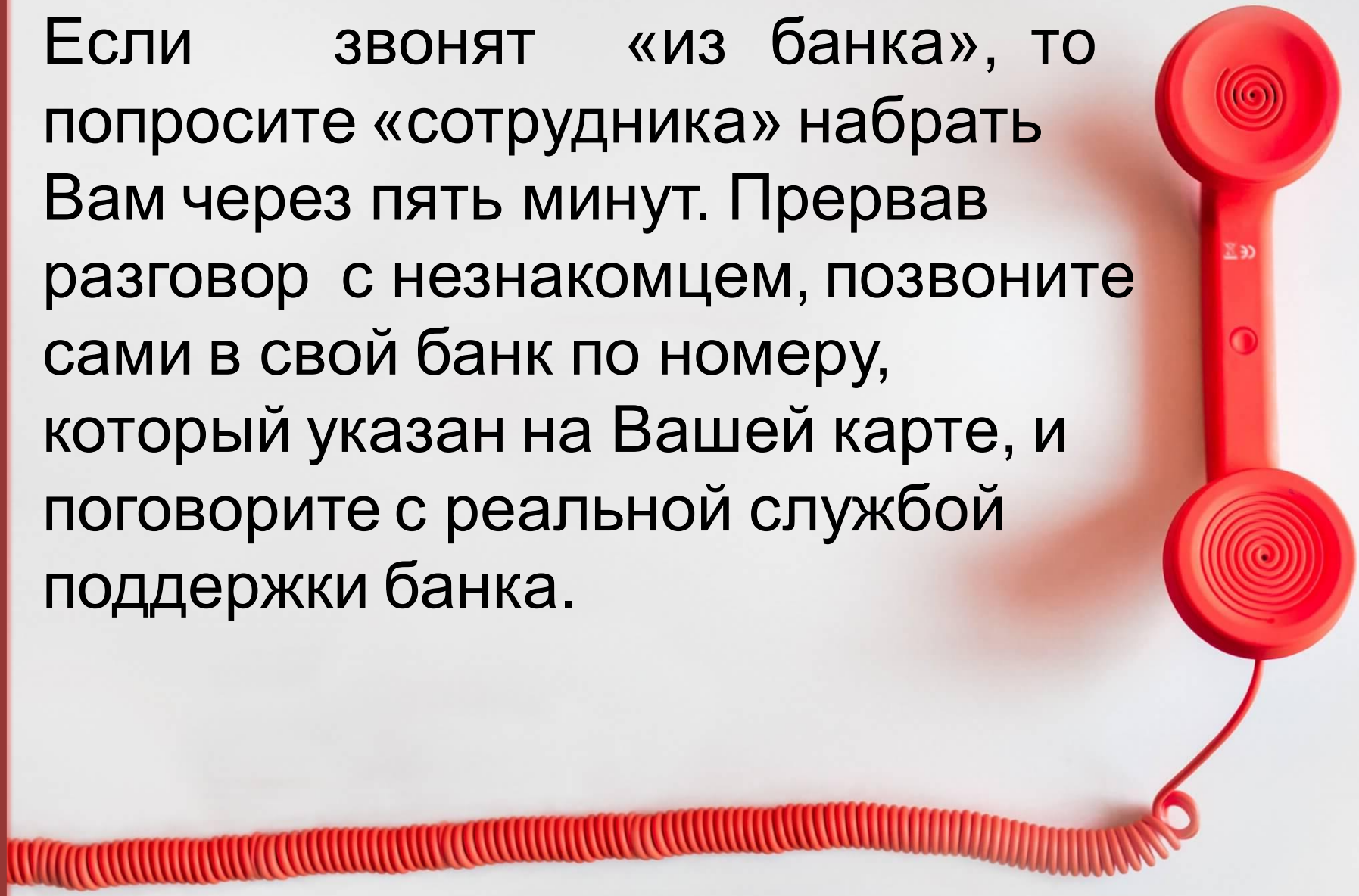
- Хранить ПИН-код рядом с картой, записывать его на бумаге
- Прибегать к помощи третьих лиц при проведении операции с банковской картой в банкоматах
- Позволять посторонним лицам использовать Вашу пластиковую карту

# Фишинг

Вид интернет-мошенничества, цель которого – получить Ваши персональные данные, получил название **фишинг** (от англ. fishing – рыбная ловля, выуживание).



Если звонят «из банка», то попросите «сотрудника» набрать Вам через пять минут. Прервав разговор с незнакомцем, позвоните сами в свой банк по номеру, который указан на Вашей карте, и поговорите с реальной службой поддержки банка.



# Следует помнить:

- банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой о предоставлении своих данных;
- сотрудники банка располагают достаточной информацией о своих клиентах;
- сотрудники банка могут у Вас спросить кодовое слово в том случае, если Вы им сами позвонили.

# Вредоносные программы и тактика борьбы с ними

**Вредоносные программы-** любое программное обеспечение, которое предназначено для скрытного (несанкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а так же для нанесения ущерба, связанного с его использованием

# Общие рекомендации по обеспечению безопасной работы в сети Интернет

- Установите антивирусное ПО с последними обновлениями антивирусной базы
- Регулярно обновляйте антивирусные программы
- Не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников- скачанные с неизвестных веб-сайтов, присланные по электронной почте
- По возможности не сохраняйте в системе пароли и периодически меняйте их