

МОШЕННИКИ В ЦИФРОВОМ МИРЕ

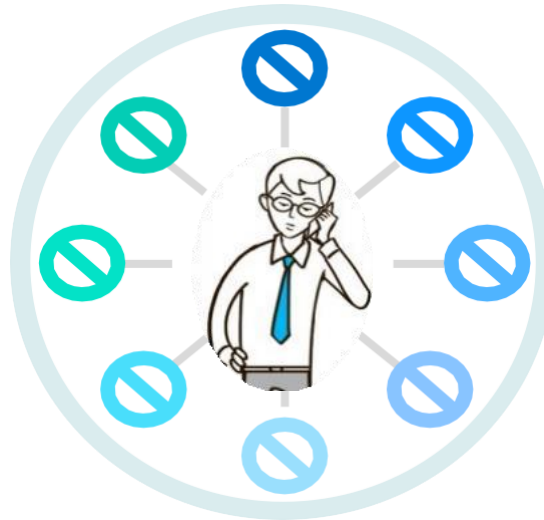
КАК СБЕРЕЧЬ СВОИ ДЕНЬГИ?



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО И IP-ТЕЛЕФОНИЯ

Звонки с целью кражи ваших средств, выманивания реквизитов банковских карт и одноразовых паролей

- ✓ **звонки по размещенным объявлениям** о продаже личного имущества через сайты «Авито», «Юла» якобы для приобретения товара
- ✓ **Звонки из социальных служб** (мошенники сообщают о необходимости получить материальные компенсации за неиспользованные льготы; могут попросить сделать якобы возвратный «идентификационный» платеж)
- ✓ **звонки с номеров телефонов банка** (мошенники представляются работниками службы безопасности банка и сообщают клиенту о якобы проведенных операциях по его карте и необходимости их отмены)



- ✓ **звонки из налоговой** (мошенники представляются работниками налоговых служб и предлагают вернуть НДС, ссылаясь на фейковое постановление о праве на получение денежной компенсации затрат на оплату товаров иностранного производства, и просят оплатить ряд услуг: консультацию юриста, заполнение анкеты и др.)
- ✓ **звонки от «представителя сотового оператора»** (мошенники предлагают перерегистрировать SIM-карту, пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного списываются деньги)

❖ **МОШЕННИЧЕСТВО ЧЕРЕЗ IP-ТЕЛЕФОНИЮ***: номера мошенников могут отражаться как номера телефонов банка или любого номера из вашей телефонной книжки



РАБОТАЕТ ТОЛЬКО НА ВХОДЯЩИЕ ЗВОНКИ - ЧТОБЫ РАЗВЕЯТЬ СОМНЕНИЯ, НУЖНО ПЕРЕЗВОНИТЬ

❖ **СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИЮ О БАНКОВСКИХ СЧЕТАХ И КАРТАХ, А ТАКЖЕ КОНТАКТЫ РОДНЫХ И БЛИЗКИХ ЛЮДЕЙ НЕЛЬЗЯ ПРЕДОСТАВЛЯТЬ НИКОМУ!**

SMS-МОШЕННИЧЕСТВО

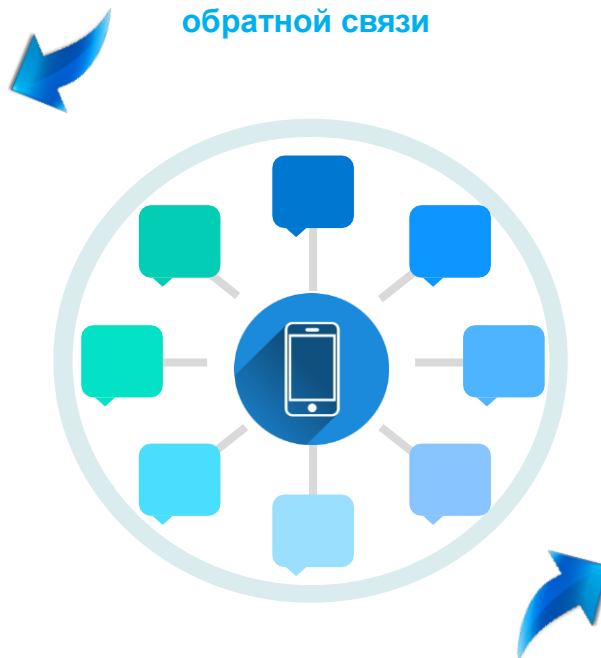
◆ Напоминаем о необходимости погасить задолженность по кредиту. Ц.Б.Р.Ф.
Информация 8 800 XXX
XX XX

◆ Оплата на сайте Ozon.ru на сумму 3500 руб. успешно зарезервирована. Если не совершали операцию, необходимо перезвонить по номеру 8800-511-51-36

◆ Ваша карта заблокирована в целях безопасности. Для уточнения информации необходимо перезвонить по определившемуся номеру. +79961763523

◆ Поздравляем!!! Пополнение Вашего телефона через карты Visa, MasterCard вошел в число призовых! Вы выиграли 100000 руб.! Информация по тел. 8-800-511-3725 или Giperkassa.ru

Рассылка SMS-сообщений с указанием номера телефона для обратной связи



Рассылка SMS-сообщений, нацеленная на вынуждение жертвы перевести деньги на счета и телефоны мошенников

◆ Мама, пополни счет на этот номер на 1000 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!

◆ Извините, по ошибке положила вам 500 руб. Прошу вернуть на этот номер

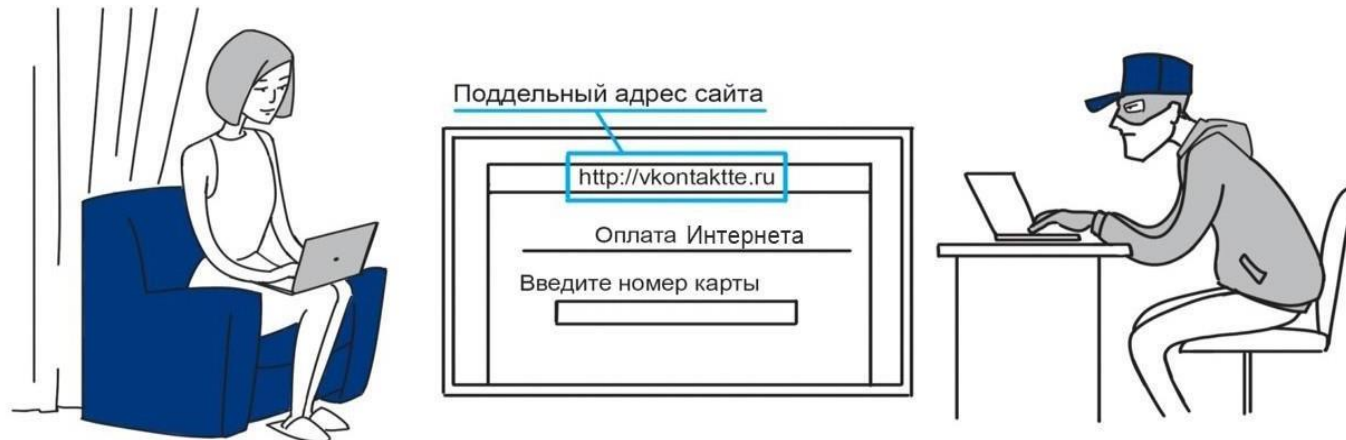
◆ Чтобы перейти на более выгодный тариф, отправьте смс на короткий номер XXXX

◆ Иванова Ирина Викторовна. Согласно геолокации, вами был нарушен режим карантина согласно ст. 20.6.1 КоАП РФ. Вам необходимо оплатить штраф согласно постановлению ФСИН №168-322 от 09-04-2020года в размере 4000 рублей на номер 8 800 XXX XX XX

❖ НЕ ПЕРЕЗВАНИВАЙТЕ ПО ТЕЛЕФОНАМ, УКАЗАННЫМ В SMS, И НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ SMS

❖ НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫЕ СООБЩЕНИЯ — ЭТО РИСК ПОДПИСАТЬСЯ НА ПЛАТНУЮ УСЛУГУ

ФИШИНГ



ФИШИНГ

Цель мошенничества — получение доступа к логинам, паролям и ПИН-кодам при помощи спама, SMS и фишинговых сайтов

КАК СЕБЯ ОБЕЗОПАСИТЬ



Не пересылajte никому
пароли и логины



Используйте антивирусы
и последние версии браузеров



Проверьте, установлено ли на сайте банка
защищенное соединение

<http://abra.kadabra>

Проверяйте адрес сайта, не переходите
по подозрительным ссылкам из писем

СНИФФЕРИНГ

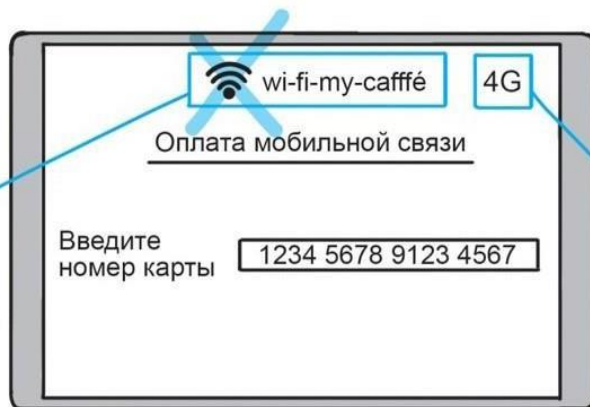


СНИФФЕРИНГ

Цель мошенничества — перехват данных мошенниками в общественных местах

КАК СЕБЯ
ОБЕЗОПАСИТЬ

Не осуществляйте платежные операции в общественных местах через незащищенные сети Wi-Fi



Убедитесь, что соединение происходит через мобильную сеть

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ



ЗАЩИТИТЕ СВОИ УСТРОЙСТВА

- обновляйте операционную систему (информационные системы и любые софты)
- используйте антивирус (следите за «свежестью» вирусных баз)
- не подключайте к своим устройствам не проверенные антивирусом новые носители информации (флешки, диски)
- создавайте резервные копии (используйте облачное хранилище или физические носители)
- следите за кибербезопасностью своего мобильного устройства (установите пароли, разделите учетные записи на личную и рабочую)



ЗАЩИТИТЕ СЕБЯ В ИНТЕРНЕТЕ

- не разглашайте личную информацию (ПИН-код, CVV/CVC, SMS-код, логин, пароль и др.)
- контролируйте содержание размещаемой информации (неразрешенное использование материала влечет гражданскую или уголовную ответственность)
- закрывайте сомнительные всплывающие окна
- используйте сложные пароли к разным ресурсам (например, с помощью менеджера паролей) и двухфакторную идентификацию
- используйте общественный Wi-Fi только в случае крайней необходимости (мобильный Интернет безопаснее)



ПРЕВЕНТИВНЫЕ МЕРЫ

- бережно храните документы, удостоверяющие личность, старайтесь не допустить их потери или кражи.
- умеете говорить «нет»! Оставляйте сканы документов только там, где этого требует закон (например, откажите охранникам, которые пытаются снять копию с паспорта, вместо того чтобы переписать данные для оформления пропуска).

**СПАСИБО ЗА
ВНИМАНИЕ!**

