# ДЕНЬГИ ДЛЯ МОШЕННИКОВ

## ОНЛАЙН-ОФОРМЛЕНИЕ КРЕДИТА ПО ПРОСЬБЕ НЕИЗВЕСТНОГО

потребуются только данные банковской карты и смс-пароли

сумма определяется в ходе разговора

заемные средства перечисляете на номера мошенников

кредит оплачиваете вы, а тратят мошенники

**ЯКУТЯНЕ ЕЖЕДНЕВНО ДАРЯТ МОШЕННИКАМ 870 ТЫСЯЧ РУБЛЕЙ**

помните, аферисты всегда рядом

# Учебная банковская карта

Можно говорить

Нельзя говорить

1234 5678 9012 3456

Номер из 16 цифр

MONTH/YEAR
VALID THRU 12/99

Срок действия

IVAN IVANOV

Имя, фамилия

*Для оплаты в сети и перевода средств **ВСЕГДА** достаточно номера карты или телефона, к которому она привязана*

Перевести средства на резервный счет- **уловка МОШЕННИКОВ!**

# ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

## БАНКИ НЕ ЗВОНЯТ!

123 ! Код безопасности. Позволяет подтвердить онлайн сделку. Если о нем узнают другие лица они получат доступ к управлению счетом!

**ВНИМАНИЕ:** не сообщайте фамилию, имя держателя карты, код безопасности и комбинации цифр, приходящие по смс. Не переводите предоплату незнакомым лицам, каким бы выгодным не были их предложения. Совершайте интернет-покупки только через **НАДЕЖНЫЕ САЙТЫ!**

**Запомните!** Нельзя никому и никогда сообщать код из смс от банка.

# Мы хотим все ваши деньги

Мошенники всегда рядом

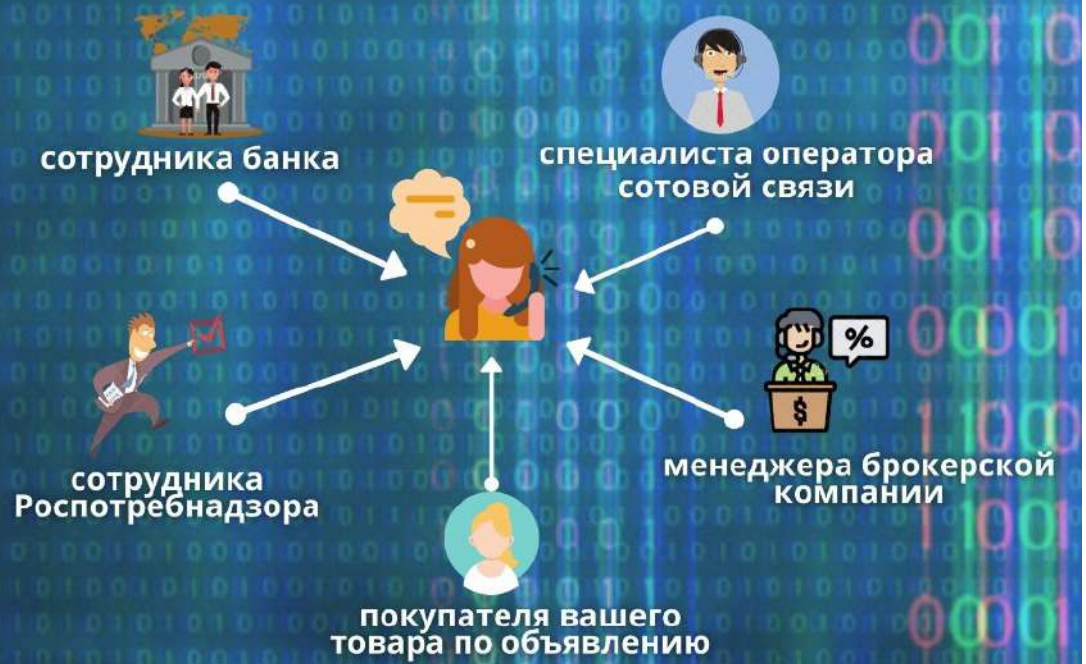
Управление экономической безопасности
и противодействия коррупции
МВД по Республике Саха (Якутия)

# МВД по Республике Саха (Якутия) предупреждает:

## Мошенничество в сфере онлайн-инвестиций

# ВИШИНГ - это вид мошенничества с использованием социальной инженерии

**Если вам поступил телефонный звонок от:**




**то ни в коем случае не раскрывайте данные ваших банковских карт, а именно:**

# Учебная БАНКОВСКАЯ КАРТА

Можно говорить

Нельзя говорить

1234 5678 9012 3456

Номер из 16 цифр

MONTH/YEAR
VALID THRU 12/99

Срок действия

IVAN IVANOV

Имя, фамилия

Для оплаты в сети и перевода средств **ВСЕГДА** достаточно номера карты или телефона, к которому она привязана

Перевести средства на резервный счет- **уловка МОШЕННИКОВ!**

# ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

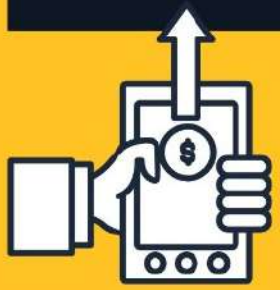
## БАНКИ НЕ ЗВОНЯТ!

123

Код безопасности. Позволяет подтвердить онлайн сделку. Если о нем узнают другие лица они получат доступ к управлению счетом!

**ВНИМАНИЕ:** не сообщайте фамилию, имя держателя карты, код безопасности и комбинации цифр, приходящие по смс. Не переводите предоплату незнакомым лицам, каким бы выгодным не были их предложения. Совершайте интернет-покупки только через **НАДЕЖНЫЕ САЙТЫ!**

**Запомните!** Нельзя никому и никогда сообщать код из смс от банка.



# ВИШИНГ: НОВЫЙ ВИД МОШЕННИЧЕСТВА НАБИРАЕТ ОБОРОТЫ

## ЧТО ТАКОЕ ВИШИНГ?

(англ. vishing — от voice phishing)

Это вид мошенничества, когда аферисты используют телефонную связь, представляются кем-либо (например, сотрудниками банков, сотовых операторов) и выманивают у владельцев банковских карт конфиденциальную информацию.

## КАК ЭТОМУ ПРОТИВОСТОЯТЬ?

Вам позвонил сотрудник банка и сказал, что мошенники пытаются похитить ваши деньги? Без паники! Просто:

**КЛАДИТЕ ТРУБКУ. Это и есть МОШЕННИКИ!**

Незнакомцы просят назвать код из смс-сообщений? Прочитайте внимательно СМС. В СМС написано "НИКОМУ НЕ НАЗЫВАЙТЕ КОД". Не нарушайте это правило, чтобы сохранить свои деньги.

**БУДЬТЕ УМНЕЕ АФЕРИСТОВ!**

# Мошенник


ПОПРОСИТ КОД ИЗ СМС

# Работник банка


НЕ ПОПРОСИТ **НИЧЕГО**

#visa × nepereputai

# Мошенник

# Работник банка


ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ НА "БЕЗОПАСНЫЙ" СЧЁТ

ЗАЩИЩАЕТ ВАШИ ДЕНЬГИ САМ

#visa × neperetutai

# Мошенник

# Работник банка



НЕ ЗНАЕТ ДЕТАЛЕЙ

ВЛАДЕЕТ ВСЕЙ ИНФОРМАЦИЕЙ

#visa × nepereputai

# Мошенник

# Работник банка


ПЫТАЕТСЯ ПРОДОЛЖИТЬ РАЗГОВОР


**НЕ** НАВЯЗЫВАЕТСЯ

#visa × nepereputai


Мошенник
Работник банка
СРОЧНО! ИНАЧЕ ЗАБЛОКИРУЮТ!
СЕЙЧАС ВО ВСЁМ РАЗБЕРЁМСЯ
МОРАЛЬНО ДАВИТ
ПОДДЕРЖИВАЕТ
#visa × nepereputai

Министерство внутренних дел по Республике Саха (Якутия)

# КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

# ВНИМАНИЕ!!!

**Чтобы не стать жертвой телефонных и интернет мошенников следует придерживаться ПРОСТЫХ, но очень важных правил в повседневной жизни**

**НЕ ПЕРЕДАВАЙТЕ** свою банковскую карту посторонним лицам

**НЕ СООБЩАЙТЕ НИКОМУ** реквизиты своей банковской карты и ее ПИН-код


**НЕ СООБЩАЙТЕ** какие-либо СМС коды, даже сотруднику банка

**НЕ ПОДТВЕРЖДАЙТЕ** банковские операции, которые вы не производили

## С БАНКОВ НЕ ЗВОНЯТ!!!

**не верьте человеку, представившимся сотрудником банка, который напугает Вас тем, что с Вашего счета пытаются списать или уже списали деньги и предложит вам отменить или заблокировать данную операцию**

- НЕ верьте людям, представляющимися сотрудниками правоохранительных органов, которые сообщают, что ваш родственник совершил преступление и предлагают свою помощь за деньги
- НЕ производите никаких действий по просьбам, полученным по телефону от посторонних лиц
- НЕ верьте информации о выигранных призах, если не принимали участия в их розыгрыше
- НЕ верьте объявлениям в соц. сетях в оказании помощи в получении кредита
- НЕ переводите деньги неизвестным лицам через анонимные платежные системы
- НЕ соглашайтесь на предоплату при покупке, либо продаже имущества через бесплатные интернет порталы
- НЕ пользуйтесь сомнительными программами в компьютере и телефоне

**ПОМНИТЕ!!!** Что во всех случаях звонящий будет обращаться к ВАМ по имени отчеству и ему могут быть известны Ваши последние операции по карте. Таким образом, мошенники входят к Вам в доверие, убеждая Вас, что они те за кого себя выдают.

Изготовлено по заказу Министерства по делам молодежи и социальным коммуникациям в рамках реализации государственной программы Республики Саха (Якутия) «Профилактика правонарушений в Республике Саха (Якутия) на 2020 – 2024 годы»

# Банки не звонят!* Зато это делают МОШЕННИКИ

*ЗА ИСКЛЮЧЕНИЕМ РЕКЛАМНЫХ ПРЕДЛОЖЕНИЙ

## Соблюдайте правила безопасности

Если вам позвонили из банка, лучше завершите разговор и самостоятельно перезвоните по телефону "горячей линии", указанному на вашей карте.

Никому не сообщайте данные карты и разовые коды из смс-сообщений.

Не переходите по ссылкам из смс или e-mail. Набирайте интернет-адреса вручную, не пользуясь "поисковиком".

Помните, что никакие серьезные финансовые операции (выдача компенсации, отмена транзакции) не проводятся по телефону.

## Как распознать кибераферист?

В основном мошенники звонят с номеров с московским кодом "8 (495)" и с номеров других регионов.

Лжесотрудник службы безопасности банка задает много вопросов, например, "какую последнюю операцию проводили?", "картами каких банков пользуетесь?" и т.д.

Разговаривает вежливо, но с нажимом, убеждает, что надо действовать немедленно, не давая времени на раздумье.

Сотрудники банка не спрашивают CVV/CVC-код и одноразовые смс-коды, а также не просят установить приложение «Team Viewer».

## Завершите разговор, если...

- Неизвестный сообщает о попытке хищения денег с карты;
- Звонящий настойчиво просит назвать данные карты, в том числе CVV/CVC-код, смс-коды, реквизиты.

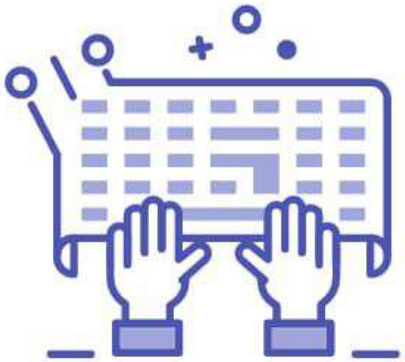
МВД ПО РЕСПУБЛИКЕ САХА (ЯКУТИЯ)

## Расскажите родителям

Пожилые люди доверчивы, не привыкли все время быть начеку и плохо осведомлены о современных способах мошенничества.

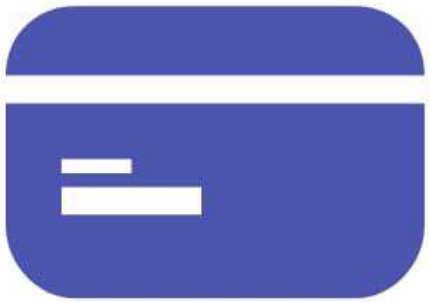
## Сомневаетесь? Кладите трубку!

СПОСОБЫ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА



# ЗВОНОК ОТ СОТРУДНИКА БАНКА

**МОШЕННИК ОТ ИМЕНИ РАБОТНИКА БАНКА СООБЩАЕТ, ЧТО НА ВАШЕ ИМЯ ОФОРМЛЕН КРЕДИТ И ПРОСИТ СЛЕДОВАТЬ ИНСТРУКЦИЯМ**

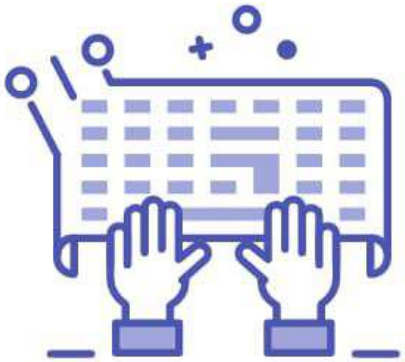


**НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ С НЕИЗВЕСТНЫХ НОМЕРОВ**

**НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ БАНКОВСКОЙ КАРТЫ И СМС-КОДЫ**

14.МВД.РФ

СПОСОБЫ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА



# ИНВЕСТИЦИИ

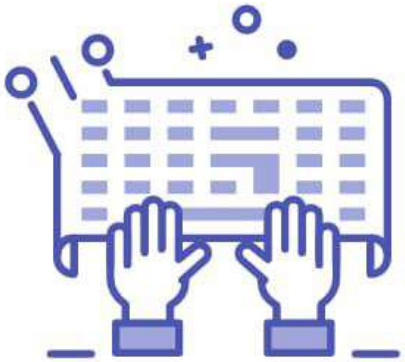
## АФЕРИСТ ПОД ВИДОМ БРОКЕРА УБЕЖДАЕТ ВНОСИТЬ ДЕНЬГИ В ФОНДОВУЮ БИРЖУ

**НЕ ВЕРЬТЕ РЕКЛАМЕ, ОБЕЩАЮЩЕЙ ПРИБЫЛЬ**

**НЕ ЗАПОЛНЯЙТЕ АНКЕТЫ НА СОМНИТЕЛЬНЫХ САЙТАХ**

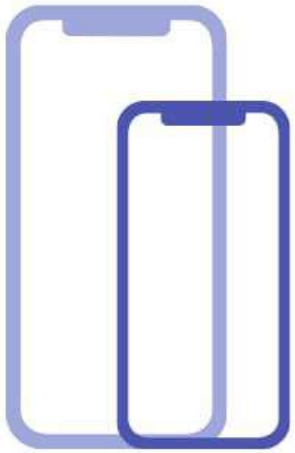
14.МВД.РФ

СПОСОБЫ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА



# ПОКУПКА И ПРОДАЖА В ИНТЕРНЕТЕ

**ДЛЯ ОПЛАТЫ ТОВАРА МОШЕННИК ОТПРАВЛЯЕТ ФЕЙКОВУЮ ССЫЛКУ, ГДЕ НУЖНО НАПИСАТЬ ДАННЫЕ КАРТЫ**



**НЕ ОБЩАЙТЕСЬ С ПОКУПАТЕЛЕМ В СТОРОННЕМ МЕССЕНДЖЕРЕ**

**НЕ ВНОСИТЕ ПРЕДОПЛАТУ**

14.МВД.РФ

# ПРАВИЛА ОБЩЕНИЯ С МОШЕННИКАМИ

## ИЛИ КАК СОХРАНИТЬ СВОИ ДЕНЬГИ

Помните, телефонные мошенники прекрасные психологи, умеют манипулировать и легко войти в доверие. Они делают свою жертву соучастником его же собственного провала.

### ДОБАВЬТЕ НОМЕР БАНКА В СПИСОК КОНТАКТОВ

Известно, что с помощью специальных программ мошенники могут подменять любые номера. На пропущенные звонки с подозрительных номеров перезванивать не стоит.

### НЕ ПОДДАВАЙТЕСЬ ЭМОЦИЯМ

Это очень важный аспект. Аферисты звонят, чтобы якобы предупредить вас о мошеннических операциях со счётом. Так они нагоняют страх, играют вашими эмоциями, оценивают психологическое состояние жертвы.

### ВНИМАТЕЛЬНО ВЫСЛУШАЙТЕ

во время разговора злоумышленник наверняка себя выдаст, употребляя финансовые термины неправильно. Они стараются получить нужную им информацию или выудить совершить какие-либо операции с картой.

### ЗАДАВАЙТЕ ВСТРЕЧНЫЕ ВОПРОСЫ

эти вопросы помогут распознать мошенника, например уточните ФИО, должность сотрудника, номер своего паспорта, номер договора при открытии банковской карты.

### НЕ ДУМАЙТЕ, ЧТО ЭТО ВАС НЕ КОСНЕТСЯ

многие потерпевшие уверены, что мошенники им не позвонят, хотя знали о способах и схемах обмана.

### ПРЕРВИТЕ РАЗГОВОР

Лучше всего не поддерживать разговор и прервать звонок. В случае необходимости проверьте неизвестный номер в интернете и перезвоните в банк по официальному номеру.

14.МВД.РФ

# ОПАСНЫЕ ВХОДЯЩИЕ С «ОФИЦИАЛЬНЫХ НОМЕРОВ»

МОШЕННИК

SIP (SESSION INITIATION PROTOCOL)
— ЭТО ОДИН ИЗ ВИДОВ ИНТЕРНЕТ-ПРОТОКОЛА IP ,
ПОЗВОЛЯЮЩИЙ ПОДМЕНЯТЬ НОМЕРА.

SIP

ПРЕДСТАВИТЕЛЬ РОСПОТРЕБНАДЗОРА

ОПЕРАТОР СВЯЗИ

СОТРУДНИК БАНКА

ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ

МЕНЕДЖЕР ОНЛАЙН-МАГАЗИНА

14.МВД.РФ