

Профилактика мошенничества с использованием цифровых технологий

С использованием материалов Министерства
общественной безопасности Челябинской области
<https://minob.gov74.ru/minob/activity/zashhita/obman.htm>

Цифровая гигиена

Как защититься от телефонных и
кибермошенников?

2

ВАША КАРТА ЗАБЛОКИРОВАНА

Для разблокировки
перезвоните сотруднику
безопасности Банка –
Петру Иванову
8-910-***-**-**

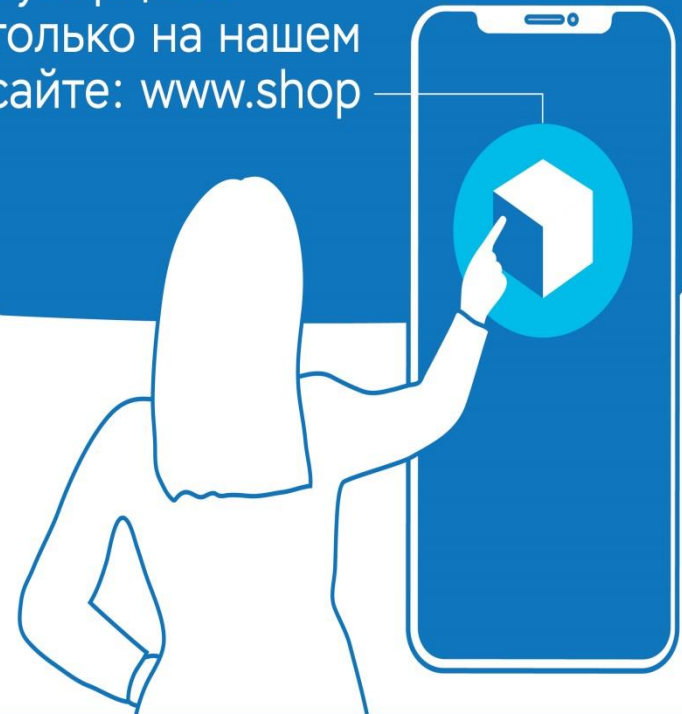


Получив любое тревожное сообщение или звонок из банка, не поддерживайте переписку или разговор. Немедленно позвоните в банк сами – вручную наберите номер, указанный на обороте банковской карты или на официальном сайте.

3

СКИДКИ ОТ 70%!

Суперцены
только на нашем
сайте: www.shop

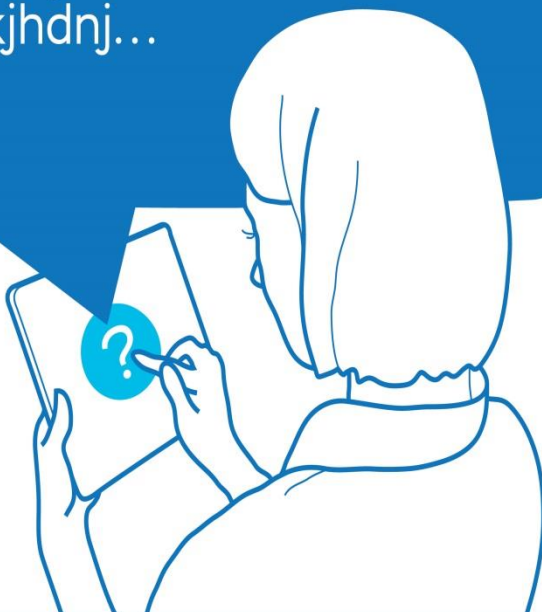


«Выгодные предложения» могут оказаться уловкой. С их помощью мошенники привлекают пользователей в свои фальшивые интернет-магазины. Это фишинг – попытка выманить реквизиты вашей банковской карты, чтобы украсть с нее деньги. Всегда проверяйте адрес сайта и не вводите данные на сомнительных страницах.

4

ВАША ПОСЫЛКА ДОСТАВЛЕНА
В ПУНКТ ВЫДАЧИ ЗАКАЗОВ

Вы можете заказать
доставку на дом по ссылке:
www.kjhdnj...



Преступники часто рассылают письма от имени популярных сервисов. Адрес отправителя может отличаться от настоящего всего парой символов. Ссылки в этих сообщениях ведут на фишинговые сайты или содержат вирусы, крадущие платежные данные с устройств. Не переходите по ним – сразу удаляйте подозрительные письма.

5

ВАШ АНАЛИЗ НА COVID-19 ГОТОВ

Результат по ссылке:
www.##2%%&#

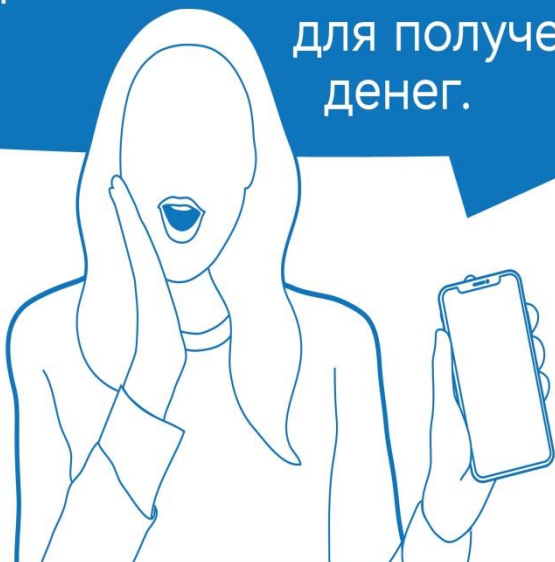


Вирусные и фишинговые рассылки обычно касаются самых популярных тем. Даже если вы сдавали анализ и ждете результат, не спешите следовать инструкциям незнакомого отправителя. Сначала проверьте адрес лаборатории на ее официальном сайте.

6

ПЕНСИОННЫЙ ФОНД

Вам полагается
компенсационная выплата
за несовершеннолетнего
ребенка. Заполните анкету
для получения
денег.

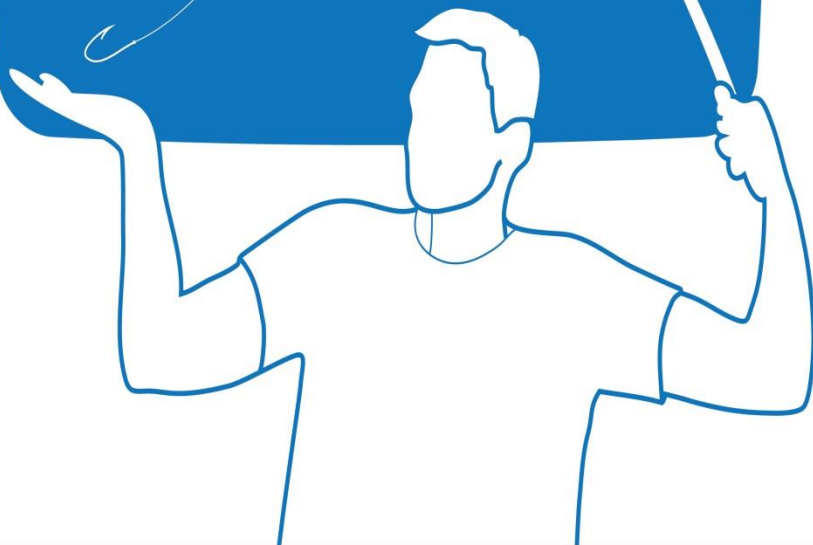


«Письма счастья» о государственных выплатах могут оказаться уловкой мошенников. Не вводите данные банковской карты на сомнительных страницах. Всегда перепроверяйте информацию о субсидиях и компенсациях в деловых СМИ или на сайтах ведомств. А еще лучше – найдите и сами прочитайте законы, указы или постановления.

7

СООБЩЕНИЕ ОТ БАНКА

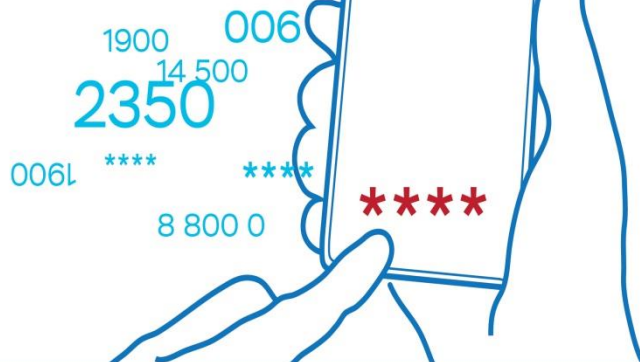
Мы проводим актуализацию
данных клиентов.
Подтвердите информацию
по ссылке: www.fdgh1j



Не переходите по ссылке – сначала позвоните в банк по официальному номеру и уточните, настоящая ли это рассылка. Аферисты рассчитывают, что вы не станете проверять информацию и выполните их инструкции. А в итоге – скачаете вирус или введете свои секретные банковские данные на поддельной странице.

ПОДОЗРИТЕЛЬНОЕ СПИСАНИЕ СРЕДСТВ С ВАШЕГО СЧЕТА

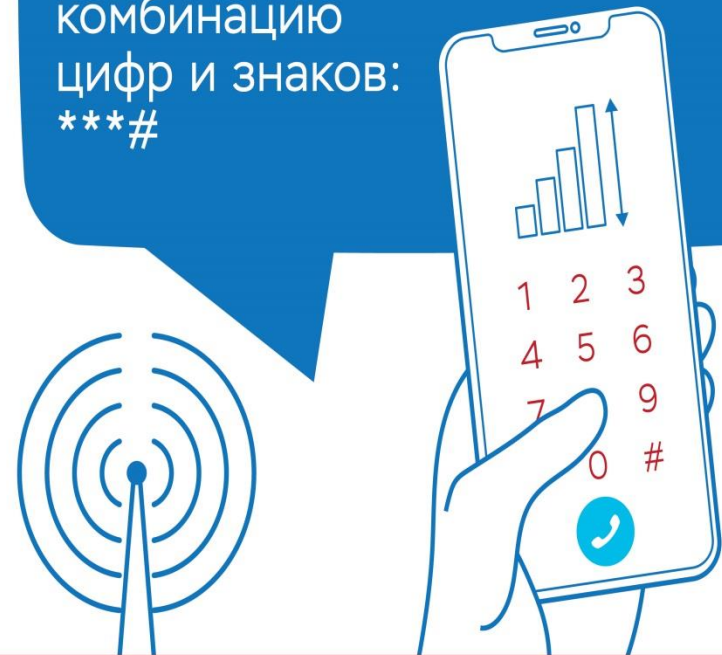
Отправьте пароль от интернет-банка ответным сообщением, чтобы отменить операцию.



Только мошенники запрашивают пароли «для отмены операции». Никому и никогда не сообщайте данные для входа в свой онлайн-банк и коды из банковских уведомлений. Также нужно держать в секрете полные реквизиты карты, включая срок действия и три цифры с оборота. В любой непонятной ситуации сами звоните в банк по официальному номеру.

ПЕРЕНАСТРОЙКА СЕТИ

Вам необходимо незамедлительно набрать комбинацию цифр и знаков:
***#



Очередная преступная схема. Любые настройки сети проходят без участия абонентов. Код, который требуют ввести на телефоне, может оказаться ключом к данным на вашем устройстве. Игнорируйте такое сообщение и передайте информацию о рассылке мошенников вашему провайдеру.

Столкнувшись с аферистами, сообщите о них в службу безопасности банка или другой организации, от имени которой они действуют.



Подробнее о том,
как защитить свои финансы,
читайте на **fincult.info**.



КАК РАСПОЗНАТЬ ТЕЛЕФОННОГО МОШЕННИКА

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

**ЕСЛИ ВАМ СООБЩИЛИ
ПО ТЕЛЕФОНУ, ЧТО:**

- ▶ необходимо пополнить баланс неизвестного номера телефона...
- ▶ ваша банковская карта заблокирована
- ▶ нужны деньги, чтобы спасти попавшего в беду родственника
- ▶ вы выиграли приз...
- ▶ вам полагается компенсация...



ПРЕКРАТИТЕ РАЗГОВОР

ПОМНИТЕ: это орудуя телефонные мошенники!

ГУ МВД России по Челябинской области
ВСЕГДА НА СВЯЗИ
102 / 112



ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

МОШЕННИКИ:



Здравствуйте, Вера Петровна!
Я сотрудник БАНКА.

ЛОЖЬ

Добрый день! Я сотрудник правоохранительных органов. Вы приобрели некачественные БАДы, за них Вам положена КОМПЕНСАЦИЯ и мы ВЕРНЁМ ДЕНЬГИ.

ЛОЖЬ



ПРЕКРАТИТЕ РАЗГОВОР



СОВЕТ: Убедитесь в том, что Вам звонили из банка, перезвонив по НОМЕРУ, указанному на ОБОРОТЕ Вашей БАНКОВСКОЙ КАРТЫ

ТАКЖЕ СТОИТ ЗНАТЬ:



**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ НА НОМЕРА
ТЕЛЕФОНОВ ИЗ СМС-СООБЩЕНИЙ
ТАКОГО ТИПА:**

- ▲ "МАМА, У МЕНЯ ПРОБЛЕМЫ, ПОПОЛНИ СЧЕТ"
- ▲ "ВЫ ВЫИГРАЛИ ПРИЗ - ДЛЯ ЕГО ПОЛУЧЕНИЯ ОПЛАТИТЕ НАЛОГ"
- ▲ "ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО ВАШЕМУ КРЕДИТУ. ТЕЛ: ..."



**ВСЁ-ТАКИ ПЕРЕВЕЛИ
ДЕНЬГИ МОШЕННИКАМ? -
СРОЧНО ЗВОНИТЕ
В БАНК!**

Сообщить о факте мошенничества:

02 / 102

со стационарного телефона с мобильного телефона

либо обратиться в ближайший отдел полиции



ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ



ИНФОРМИРУЕТ

о наиболее распространенных способах мошенничества



**НА ТЕЛЕФОН ПОСТУПАЕТ ЗВОНОК
ОТ ЯКОБЫ «СОТРУДНИКОВ БАНКА»**

**ЗЛОУМЫШЛЕННИК СООБЩАЕТ:
«НА ВАС ПЫТАЮТСЯ ОФОРМИТЬ ОНЛАЙН-КРЕДИТ»
ЛИБО
«К ВАШЕМУ СЧЕТУ В БАНКЕ
ПЫТАЮТСЯ ПОЛУЧИТЬ ДОСТУП»**



ДАЛЕЕ НЕИЗВЕСТНЫЙ СОБЕСЕДНИК:

1. ПРОСИТ СООБЩИТЬ ДАННЫЕ ВАШЕЙ БАНКОВСКОЙ КАРТЫ
2. РЕКОМЕНДУЕТ АННУЛИРОВАТЬ ОФОРМЛЯЕМЫЙ КРЕДИТ,
ПРИ ЭТОМ ЗАКЛЮЧИВ НОВЫЙ ДОГОВОР
С КРЕДИТНОЙ ОРГАНИЗАЦИЕЙ

**ЕСЛИ ВЫ СОГЛАШАЕТЕСЬ
НА ВЫШЕУКАЗАННЫЕ ДЕЙСТВИЯ -
ВЫ ТЕРЯЕТЕ СВОИ СБЕРЕЖЕНИЯ**

КАК УБЕРЕЧЬ СЕБЯ ОТ МОШЕННИКОВ?



Незамедлительно прекратите
с неизвестным разговор по телефону.



ОБРАТИТЕСЬ В ПОЛИЦИЮ

**ВСЕГДА НА СВЯЗИ
102 / 112**



**ПОЛИЦИЯ
ЧЕЛЯБИНСКОЙ ОБЛАСТИ
ПРЕДУПРЕЖДАЕТ**



**ОСТОРОЖНО,
МОШЕННИКИ!**

**ЕСЛИ ВАМ ПОСТУПАЮТ СОМНИТЕЛЬНЫЕ ЗВОНКИ
ИЗ КРЕДИТНЫХ УЧРЕЖДЕНИЙ -**

ПОЛОЖИТЕ ТРУБКУ!

**ПРИЗНАКИ ЗВОНКА
ОТ ЛЖЕСОТРУДНИКА БАНКА:**

- сообщение о попытке хищения
денежных средств
- предложение перевести деньги
на «безопасный» счет
- просьба назвать реквизиты карты,
код и пароли

НИКОГДА НЕ СООБЩАЙТЕ
СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ,
ОСОБЕННО ИНФОРМАЦИЮ
ПО БАНКОВСКИМ КАРТАМ
(CVV, ПИН, КОДОВОЕ СЛОВО И Т.Д.)

НИКОГДА НЕ ПЕРЕХОДИТЕ
ПО ССЫЛКЕ, УКАЗАННОЙ
В СМС-СООБЩЕНИИ
ОТ НЕИЗВЕСТНЫХ ЛИЦ!

ГУ МВД РОССИИ ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ
ВСЕГДА НА СВЯЗИ
102 / 112

ОСТОРОЖНО, МОШЕННИКИ!

ВАША КАРТА ЗАБЛОКИРОВАНА

Требуют сообщить
3 цифры CVV-кода?

**ПРЕКРАТИТЕ
РАЗГОВОР!**

РОДСТВЕННИК В БЕДЕ

Сообщают, что
родственник попал
в сложную
ситуацию?

**ПЕРЕЗВОНИТЕ
РОДСТВЕННИКУ!**



В СОЦИАЛЬНЫХ СЕТЯХ ПРОСЯТ ДЕНЬГИ

Приходят сообщения
с требованием
срочно перевести
в долг деньги?

**ПОЗВОНИТЕ ЛИЧНО
ВЛАДЕЛЬЦУ
АККАУНТА!**

ВЫПЛАТЫ

Якобы сотрудник
сообщает, что
вам положена
компенсация?

**НЕ ПРЕДОСТАВЛЯЙТЕ
ЕМУ ПЕРСОНАЛЬНЫЕ
ДАННЫЕ!**

ВЫИГРЫШ

Вам сообщили, что
вы победили
в розыгрыше, нужно
перевести деньги
за доставку?

ЭТО ОБМАН!

БУДЬТЕ БДИТЕЛЬНЫ!



ГУ МВД РОССИИ ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ВСЕГДА НА СВЯЗИ

102 / 112

КОМПЕНСАЦИЯ

Вам сообщили
о выплате за
некачественный
товар?

ЭТО УЛОВКА!



1

Незнакомец неожиданно связывается с вами

Например, от имени банка, полиции, магазина. Способы могут быть разные - звонок, СМС или ссылка в мессенджере.

Общее у них одно - кто-то сам вышел на связь с вами. Значит ему что-то нужно.

2

С вами говорят о деньгах

Основная задача мошенников - получить доступ к чужим деньгам. Вам помогут предложить:

- Перевести все деньги на "безопасный счет".
 - Оплатить "страховку" для получения "кредита".
 - "Очень выгодно" инвестировать в свои сбережения.
- И многое другое. Главное: речь всегда будет идти о деньгах.

3

Вас просят сообщить данные



Назовите код из СМС

Сообщите 3-значный код на обороте вашей карты

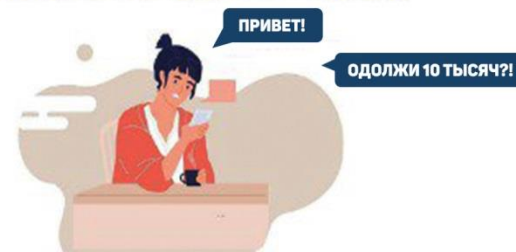
4



Вас выводят из равновесия

5

На вас давят



**5 примет,
по которым
можно вычислить
мошенников**

Интернет-мошенничество - памятка для граждан

СИТУАЦИЯ 1



Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

СИТУАЦИЯ 2

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

БЕЗОПАСНОСТЬ



Apple iPhone 5s 16Gb (серебристый)
47000 руб. ~~15000 руб.~~



Поделиться:



Оплата и доставка

1. Перевод на QIWI кошелёк номер [redacted]
2. Удобрение денег на счет [redacted]
3. Перевод на карту
Ис карты [redacted]
Владелец карты [redacted]
Срок действия карты [redacted]
4. РБК Money кошелёк номер [redacted]



СИТУАЦИЯ 3



Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

СИТУАЦИЯ 4

На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.

Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.



СИТУАЦИЯ 5

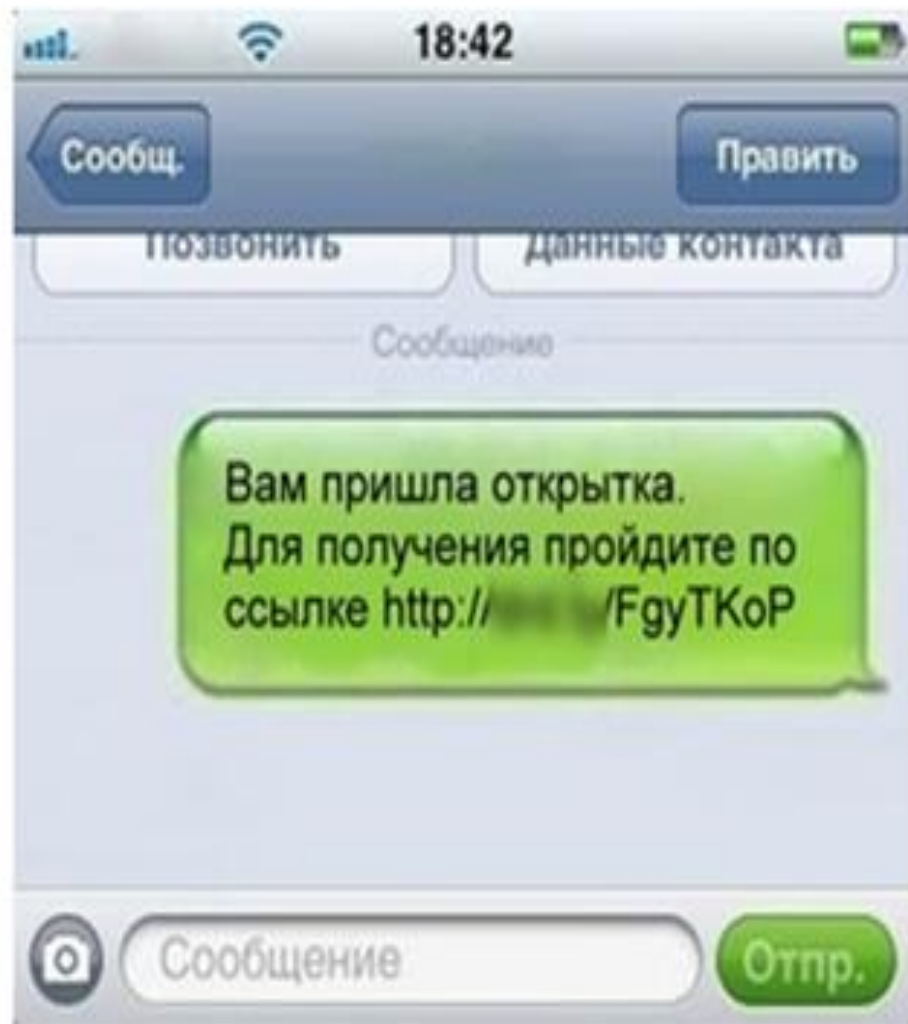


Вы хотите приобрести авиабилеты через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.

Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.

СИТУАЦИЯ 6



Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

НИКОГДА не переходите по ссылке, указанной в сообщении.

Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.