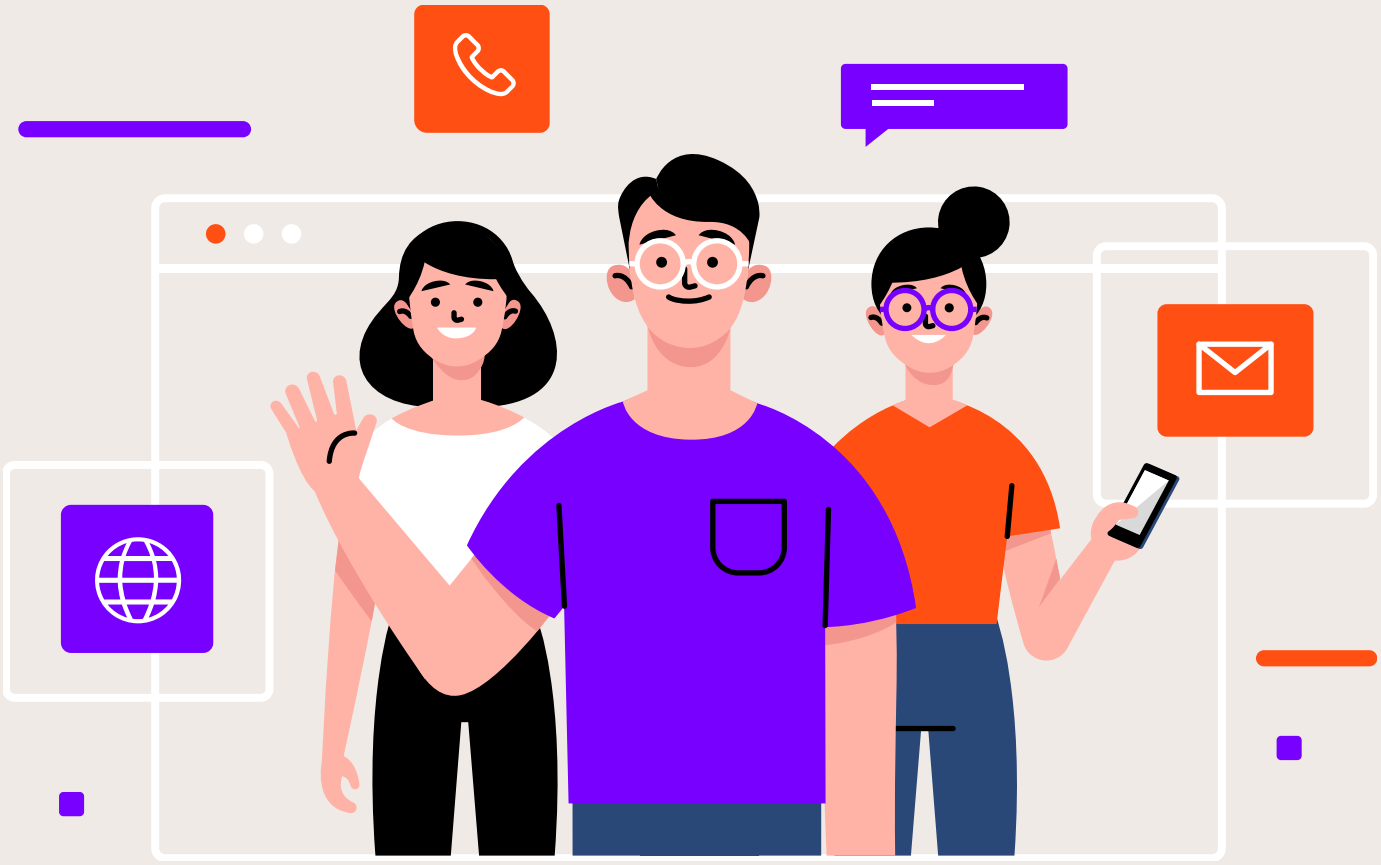
Ростелеком

Кибермошенничество

– сложная, но очень злободневная тема

Особенно сейчас, когда мошенники научились действовать повсеместно, стараясь застать врасплох и используя наши эмоции.



В этой брошюре мы постарались просто и кратко рассказать вам о том, как обезопасить свои данные и финансы, и не попасть в ловушки, расставленные хакерами в интернете.

Мошенничество с помощью смс

Наверняка вам часто приходят сообщения на телефон с незнакомых номеров с предложением перейти по ссылке.
Это может быть выигрыш в лотерею, большие скидки на товары, бесплатная диспансеризация — все то, что заставит вас на эмоциях открыть сайт и выполнить действия.

Мошенники точно знают, на какие болевые точки надавить и какие темы затронуть, поэтому призываем вас быть бдительными и внимательными.

Только представьте, в среднем на одного человека в месяц приходится 41 спам-сообщение.

Как вас могут обмануть?

На ваш телефон могут приходить смс-сообщения с таким текстом:

Что делать в таком случае?

- Запомните: переходить по неизвестным ссылкам из смс очень опасно.
- Если хотите проверить реальность выигрыша, помочь другу в беде или убедиться, что с банковского счета ничего не украдено, делайте это другим способом: сами позвоните в банк или знакомому, поищите информацию и отзывы об организаторе лотереи и т.п.
- Помните, что мошенник провоцирует вас на немедленные, а потому – необдуманные действия. Отложите телефон, сделайте глубокий вдох. Позвоните родным и посоветуйтесь, как отреагировать на «заманчивое» предложение или волнующее СМС.

Осторожно, вам звонит мошенник!

Вымогательство денег по телефону — один из самых популярных и эффективных методов обогащения для мошенников.

Почему мы до сих пор не можем противостоять обману? → **Потому что преступники очень хорошо знают наши слабые места.**

Как вас могут обмануть?

- Испугав списаниями с вашей карты, заставят перевести пенсию на «безопасный счет»

- Под предлогом государственных выплат попытаются узнать информацию, необходимую для вывода денег: код из СМС, PIN и CVV/CVC коды от банковской карты

- Вам позвонят, чтобы обрадовать: задержана преступная группировка по продаже некачественных лекарств, а вы как один из пострадавших покупателей должны получить компенсацию — **200 тысяч рублей**. Чтобы застраховать перевод, вам предложат оплатить небольшую сумму, **32 тысячи**.

- Если вы автовладелец, с вами могут связаться подставные агенты страховых компаний и предложить через них приобрести страховку. После перевода средств окажется, что документ уже оформлен на другого человека.

Как происходит обман

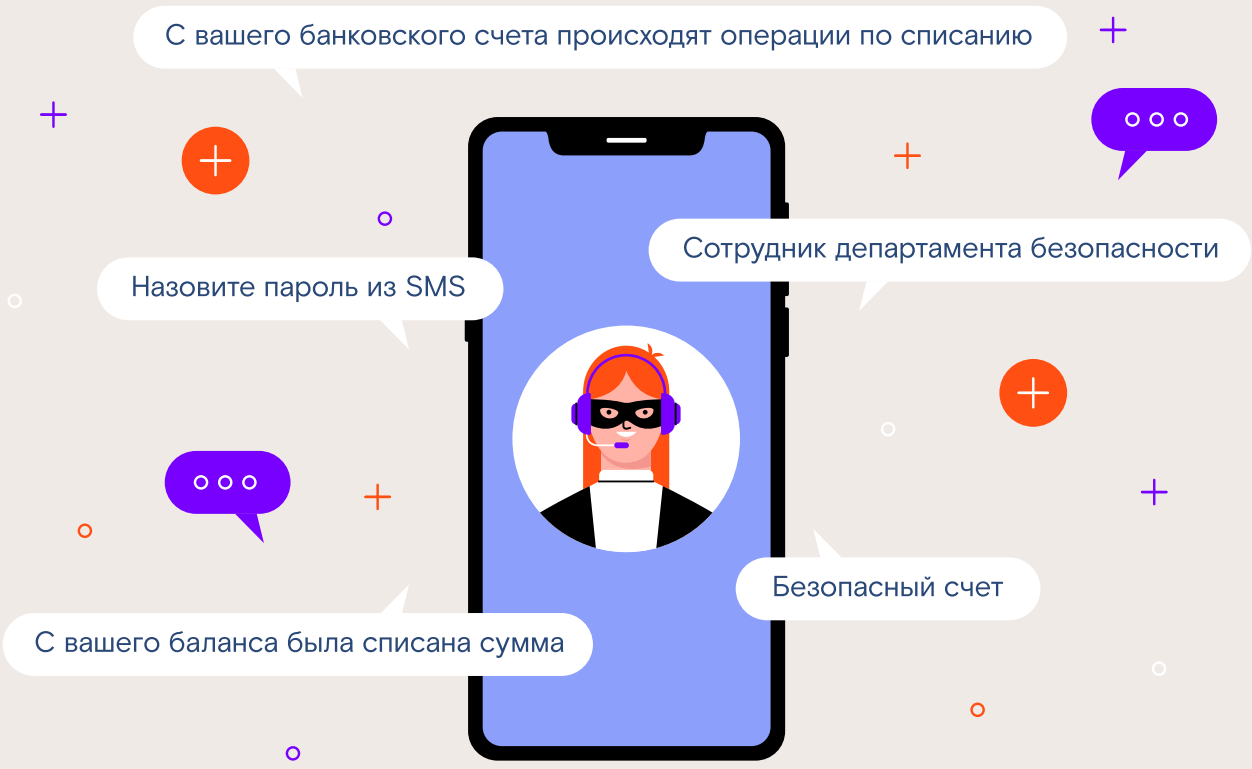
Вам могут звонить мошенники, которые представляются сотрудниками служб безопасности банков, сотрудниками прокуратуры, следователями, представителями Центрального банка и т.п.

Обратите внимание: аферисты могут называть ваши паспортные данные, номер счета и другую конфиденциальную информацию, но это не должно сбить вас с толку.

Что делать в таком случае?

- Если вас запугивают «сотрудники» каких-либо компаний или государственных органов, завершите звонок и свяжитесь с ведомством самостоятельно.
- Ни в коем случае не звоните на номер, с которого вам только что поступил тревожный звонок. Найдите официальный номер банка или компании.
- Помните, что страх и необходимость моментального решения — две стихии мошенников. Если звонящий торопит вас и запугивает ужасными последствиями, завершайте разговор без сожалений.

Задумайтесь, если вы услышали по телефону эти слова. Скорее всего, это мошенники:



Купить в интернете и не разориться

Покупать в интернете — это экономия времени и сил. Но делать это нужно с осторожностью.

Как вас могут обмануть?

1. Рассылки, баннеры, контекстная реклама и многое другое

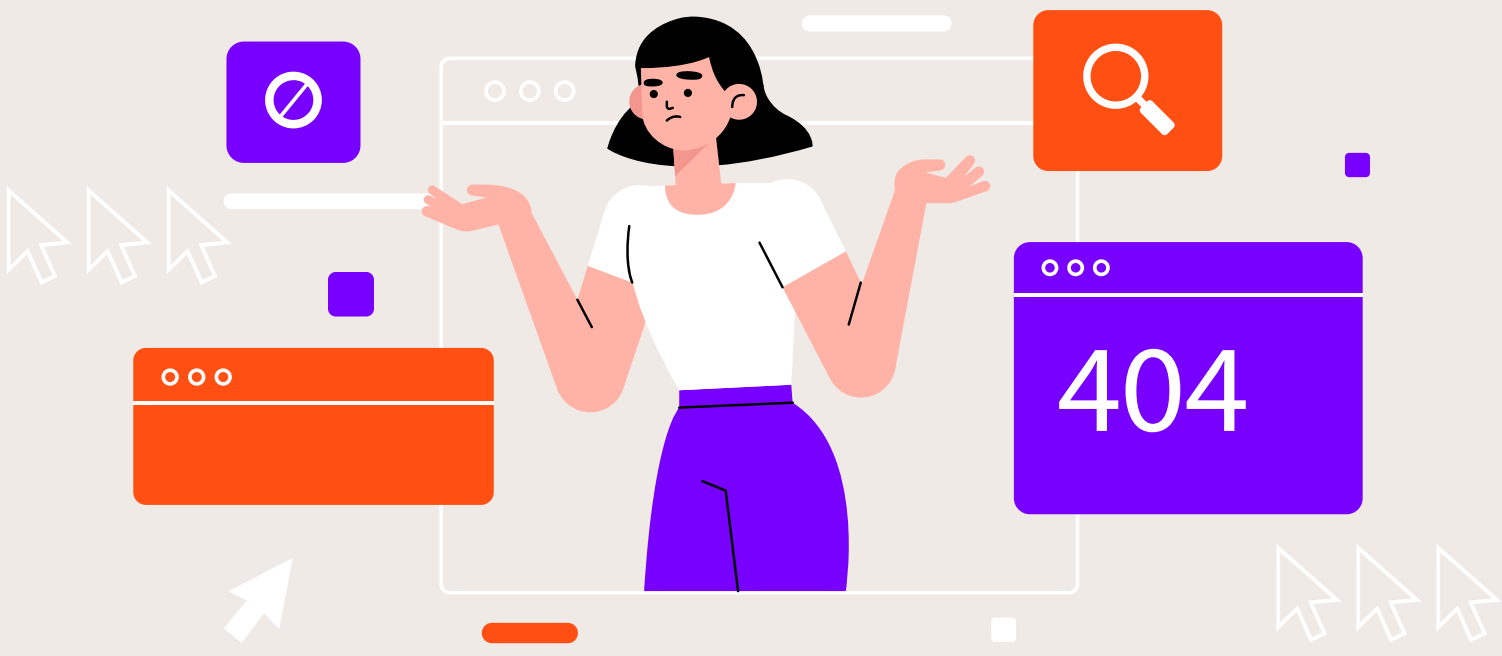
Мошенники рекламирую товары по выгодным ценам. Это может быть одежда или бытовая техника, которую вы совсем недавно сами искали в интернет-магазине. Цены приятно поражают, стоимость ниже в несколько раз. Вы радуетесь и переходите по ссылке из рекламного сообщения.

2. Смешные цены

Онлайн-страница пестрит дешевыми товарами. Вы выбираете товары и переходите к оплате.

3. «Введите реквизиты банковской карты»

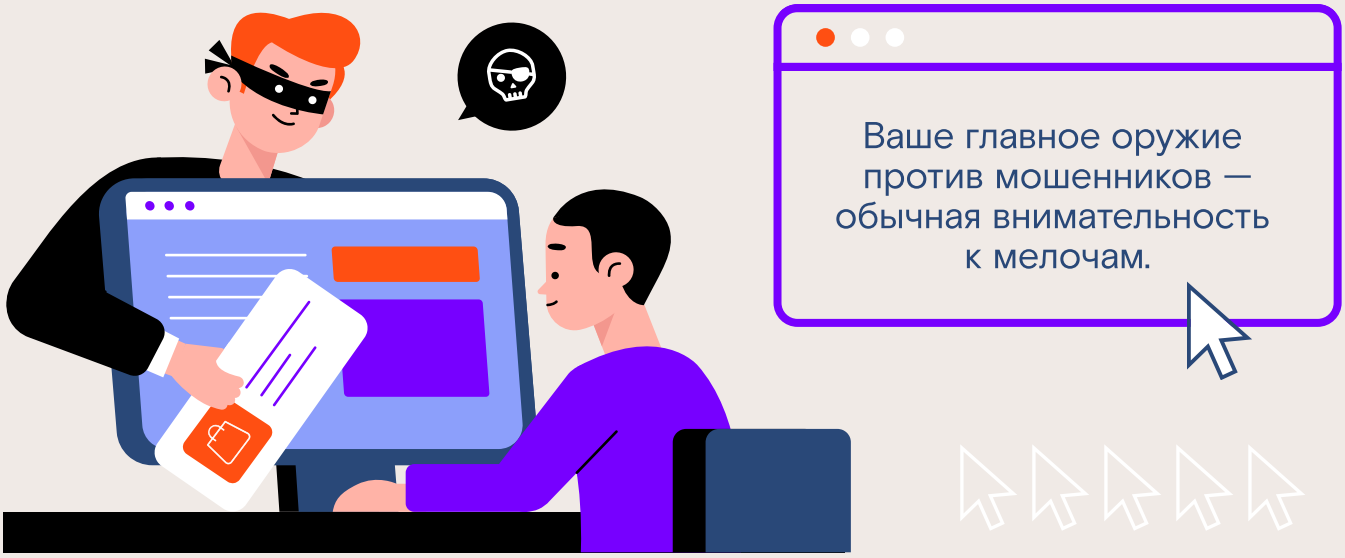
После ввода данных деньги действительно списываются, только товары никогда не придут вам, а мошеннический сайт в скором времени станет недоступен для обманутых покупателей.



Что делать в таком случае?

Не позволяйте низким ценам и выгодным предложениям обмануть вас.

Даже если вам нужно купить что-то срочно, лучше потратить 5 минут на проверку сайта. Так вы не потеряете деньги и научитесь определять вредоносные сайты быстрее.



Обратите внимание на то, как выглядит мошеннический сайт

- В адресной строке браузера отсутствует значок замка и сочетание HTTPS, а в адресе сайта есть дополнительные буквы, цифры или символы.

Настоящий сайт	Подделка
https://www.wildberries.ru/	http://wildberies.id8987.ru
https://www.ozon.ru	http://ozon.delivery.ru
https://www.mosenergosbyt.ru/	http://mozenergosdyt.ry/

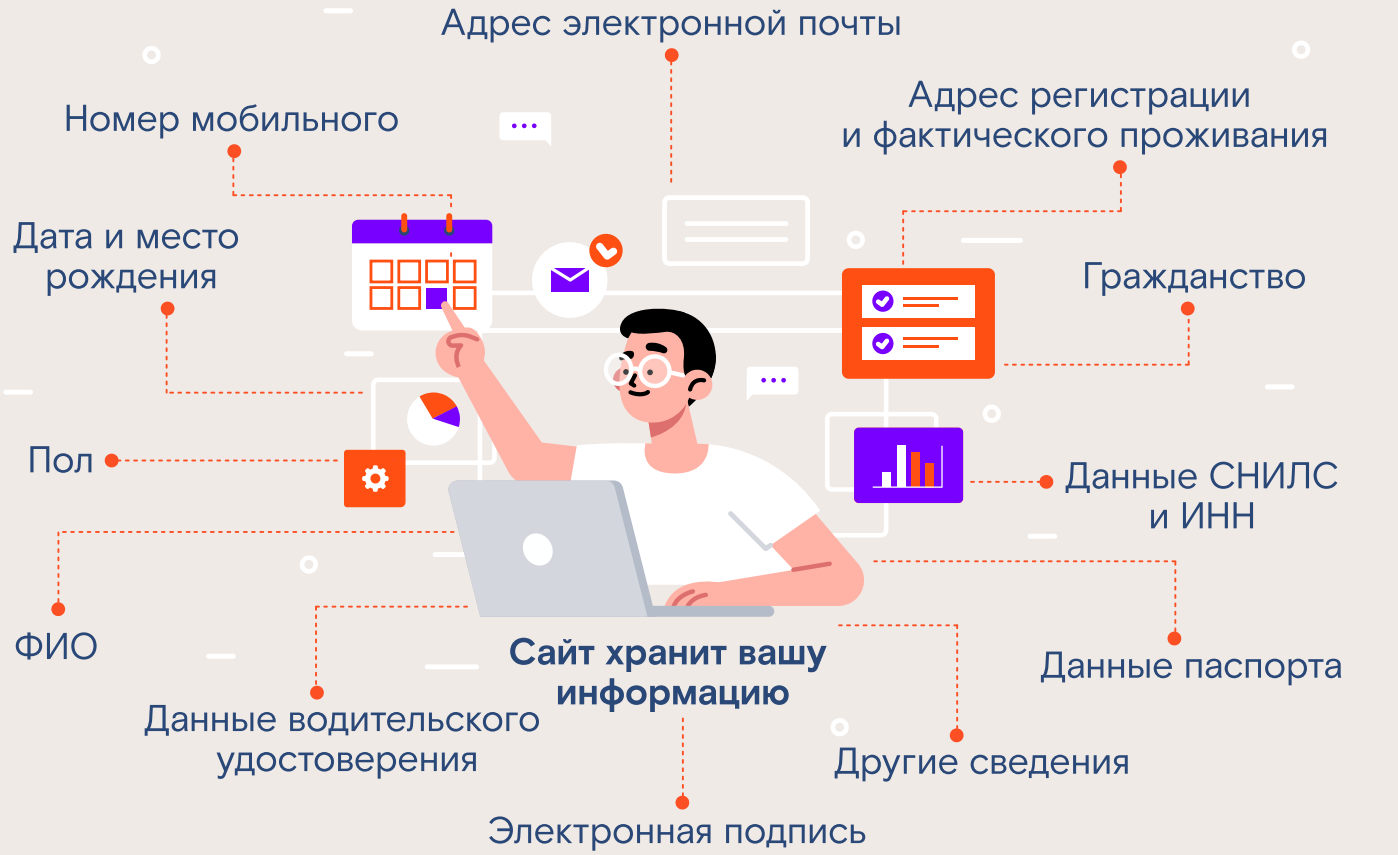
- Внешний вид вызывает подозрения. Замыленный логотип, опечатки, отсутствие ключевой информации (реквизиты, контакты, ИНН, юридический адрес).
- На сайте отсутствуют ключевые документы: Политика конфиденциальности данных, Пользовательское соглашение и Политика использования cookie-файлов.
- Нет информации о том, сколько сайту лет. Эту графу следует искать в «подвале», самом конце страницы. Например, интернет-магазин одежды Wildberries существует с 2004 года.

«Госуслуги» под замком

Госуслуги» — это не просто портал с уникальной возможностью быстро заказать ряд услуг, а настоящий «банк», который хранит не сбережения, а ваши цифровые документы

Если ваш аккаунт подтвержден сотрудником МФЦ, вы — полноценный пользователь «Госуслуг».

Что хранят «Госуслуги»



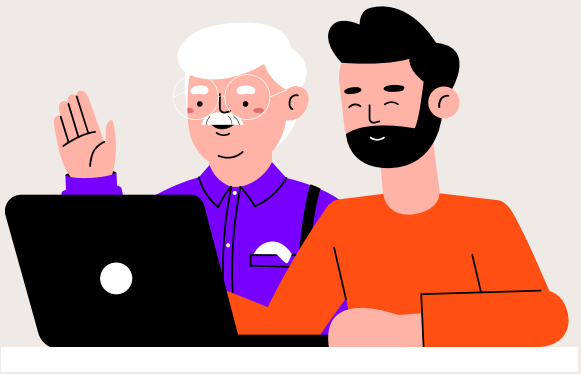
Как вас могут обмануть?

- По паспортным данным мошенники могут: оформить на вас микрокредиты и рассрочки, открыть ООО и ИП для вывода украденных средств, зарегистрировать подставные электронные кошельки и SIM-карты для телефонного мошенничества.
- По СНИЛС оформить онлайн-заявление о переводе средств гражданина в какой-нибудь негосударственный пенсионный фонд.
- При помощи электронной подписи оформить договор дарения вашей недвижимости третьему лицу.
- Получив доступ ко вкладке «Банковские карты и счета», мошенники способны перевести все ваши денежные средства на электронный кошелек.

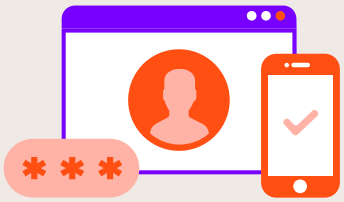
Что делать в таком случае?

Чтобы пользоваться «Госулугами» без страха, необходимо подключить настройки безопасности.

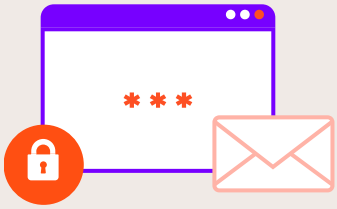
Вы сможете сделать это самостоятельно. Но если вам не просто разобраться с этим, попросите родственников о помощи.



Основные защитные функции находятся во вкладке «Профиль», далее перейдите в раздел «Безопасность».

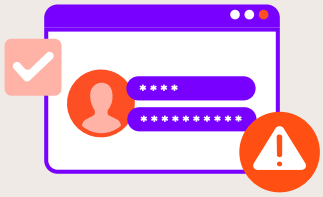


1. Выберите вход с подтверждением по SMS.



2. Подключите функцию «Оповещение на электронную почту».

3. Замените пароль на более сложный и надежный. Например, сочетание L3zqnf%7{ хоть и сложно запомнить, но также сложно подобрать для взлома. Меняйте пароль раз в год. Не сообщайте логин и пароль никому и не храните информацию об учетной записи на виду.



4. Не заходите в личный кабинет с компьютеров и телефонов третьих лиц.

5. Установите приложение «Госключ» и получите усиленную квалификационную электронную подпись.

Недостоверная информация: как ее проверить

Информация в интернете и средствах массовой информации распространяется быстрее, чем соседские сплетни. Иногда бывает сложно отделить достоверные факты от провокации. Давайте разберемся, что такое фальшивые новости, почему они существуют и как научиться их распознавать.

А вы видели эту информацию? Это примеры фальшивых новостей.

Мобилизация	«Вторая волна мобилизации начнется с Калининграда в начале февраля»
Скоростной интернет	«Вышки 5G устанавливают, чтобы облучить людей высокими дозами радиации»
Пробники духов	«В России появился новый вид убийства! Дают понюхать пробник от духов, после чего человек сразу умирает»

На какую реакцию рассчитаны эти новости

Вы продолжите распространять недостоверную информацию.

На пике эмоций все мы действуем необдуманно, делимся «новостью» с родственниками и друзьями, продолжая сеять панику. Авторы таких новостей знают: чем больше людей поверит в легенду, тем сложнее будет доказать ее надуманность.

Вы измените свое отношение к событию/человеку/организации.

Изменить мнение людей просто. Никто не будет испытывать симпатию к человеку, которого назвали живодером или коррумпированным политиком. Ложные обвинения способны уничтожить репутацию любого человека, компании или организации.

Для чего их распространяют

- Дестабилизировать ситуацию в стране, обострить социальные конфликты.
- Спровоцировать эмоциональный отклик у аудитории и заставить совершать необдуманные поступки (покинуть страну, купить всю гречку в магазине).
- Повысить посещаемость и популярность интернет-ресурса при помощи кричащих заголовков и провокационных материалов.

ТОП-10 советов по безопасности

Потеря телефона или непредвиденное списание денег с карты — это стресс, и в такие моменты нельзя медлить. Вот несколько полезных советов для ситуаций, когда нужно действовать быстро.

1. Что делать, если мне пришло сообщение о списании денежных средств, а я ничего не покупал(а)?

- Не паникуйте. Вам могли отправить смс-сообщение мошенники, чтобы заставить вас перейти на вредоносный сайт.
- Позвоните в банк чтобы удостовериться о наличии операции.
- Заблокируйте карту, если информация об операции подтвердится.
- Посетите отделение банка и напишите заявление о несогласии с операцией, возможно, вам еще успеют вернуть украденную сумму.

2. Что делать, если в соцсетях мои знакомые получают сообщения с просьбой одолжить денег?

- Первое: измените пароль от аккаунта на более надежный и совершите выход из аккаунта на всех устройствах.
- Второе: просмотрите личные сообщения. Если хакер успел написать кому-либо, сообщите этим людям, что вас взломали.
- Третье: свяжитесь с техподдержкой платформы и сообщите об инциденте.

3. Что делать, если сотрудник банка просит назвать данные карты и перевести деньги на безопасный счет?

Здесь может быть только один ответ: вам позвонили мошенники, сбросьте звонок как можно быстрее.

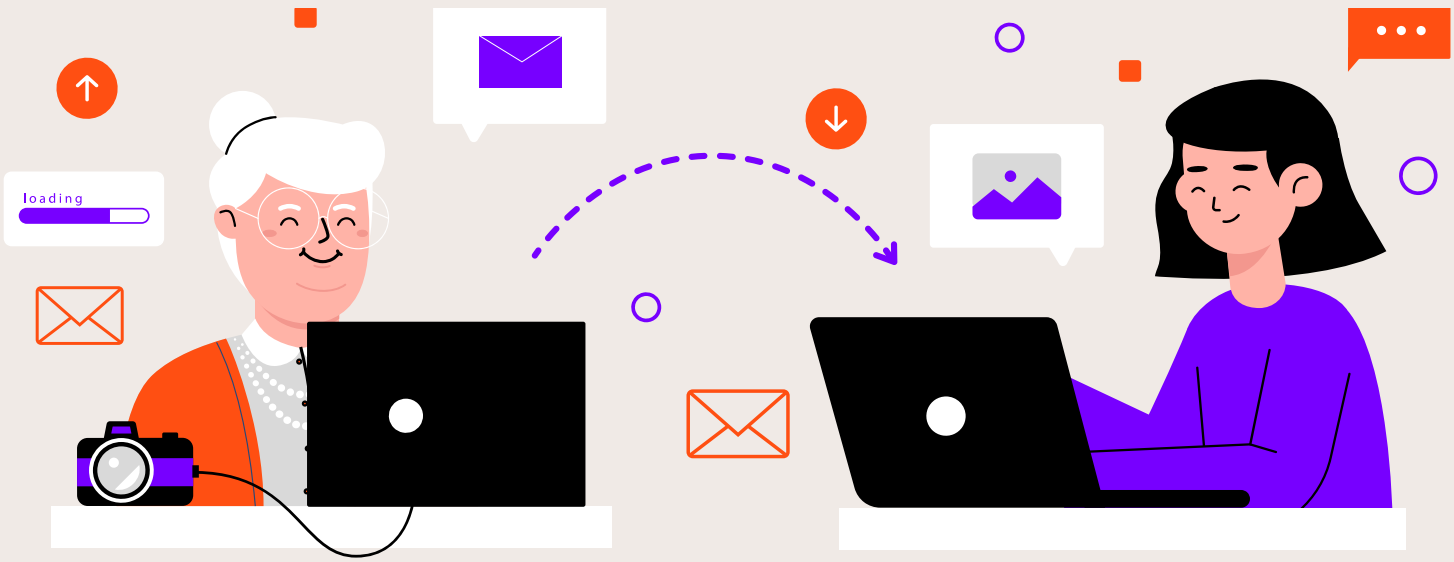
- Сотрудники банка не вправе запрашивать у клиентов конфиденциальную информацию.
- Безопасных счетов для сохранности денежных средств не существует.

4. Что делать, если у меня потерялся телефон или его украли?

- Сначала свяжитесь с сотовым оператором и попросите заблокировать SIM-карту, чтобы не дать злоумышленнику возможность оплатить покупку через интернет или войти в банковские приложения, «Госуслуги».
- Позвоните в банк(и) и попросите заблокировать карты.
- Сообщите родственникам и друзьям об инциденте. Предупредите их, что мошенники могут попросить денег от вашего лица.
- Обратитесь в полицию и напишите заявление.
- Смените пароли на всех аккаунтах, в электронной почте, социальных сетях и других сервисах.
- Посетите салон сотового оператора, чтобы перевыпустить SIM-карту.

5. Что делать, если хочу отправить фотографию паспорта?

- Не отправляйте фото (скан) документа через социальные сети, мессенджеры или в смс-сообщении.
- Если необходимо, отправьте данные документа в текстовом виде, а изображение — по почте в файле с паролем.

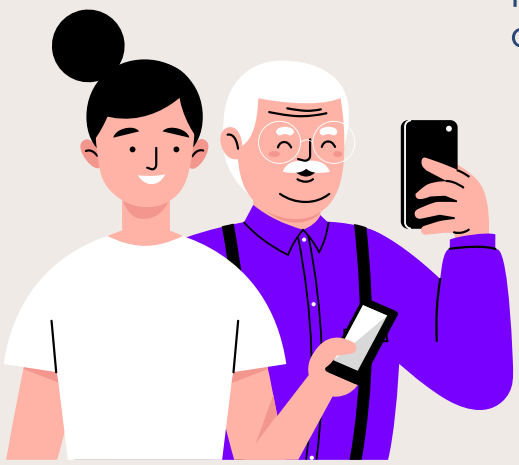


6. Что делать, если меня просят дать согласие на обработку данных на сайте?

Это стандартная процедура, которая означает, что вы соглашаетесь передать свои персональные данные интернет-ресурсу. С этого момента администраторы сайта имеют право собирать, хранить, передавать сведения о вас в рекламных и других целях. Но также это означает, что администраторы ресурса несут ответственность за безопасность персональных данных пользователей.

- Соглашайтесь на обработку ПДн только на тех сайтах, которым можно доверять.

7. Что делать, если дети подарили умное устройство, а я не знаю, как им пользоваться?



Прежде чем расстраиваться, познакомьтесь с гаджетом.

- Посмотрите информационные ролики, они подскажут что умеет устройство, для каких целей его используют и как оно работает.
- Попросите детей разобраться вместе.
- Прочтите несколько статей об аппарате и не забудьте поинтересоваться, как устроена его безопасность.

8. Что делать, если мошенники названивают мне несколько раз в день?

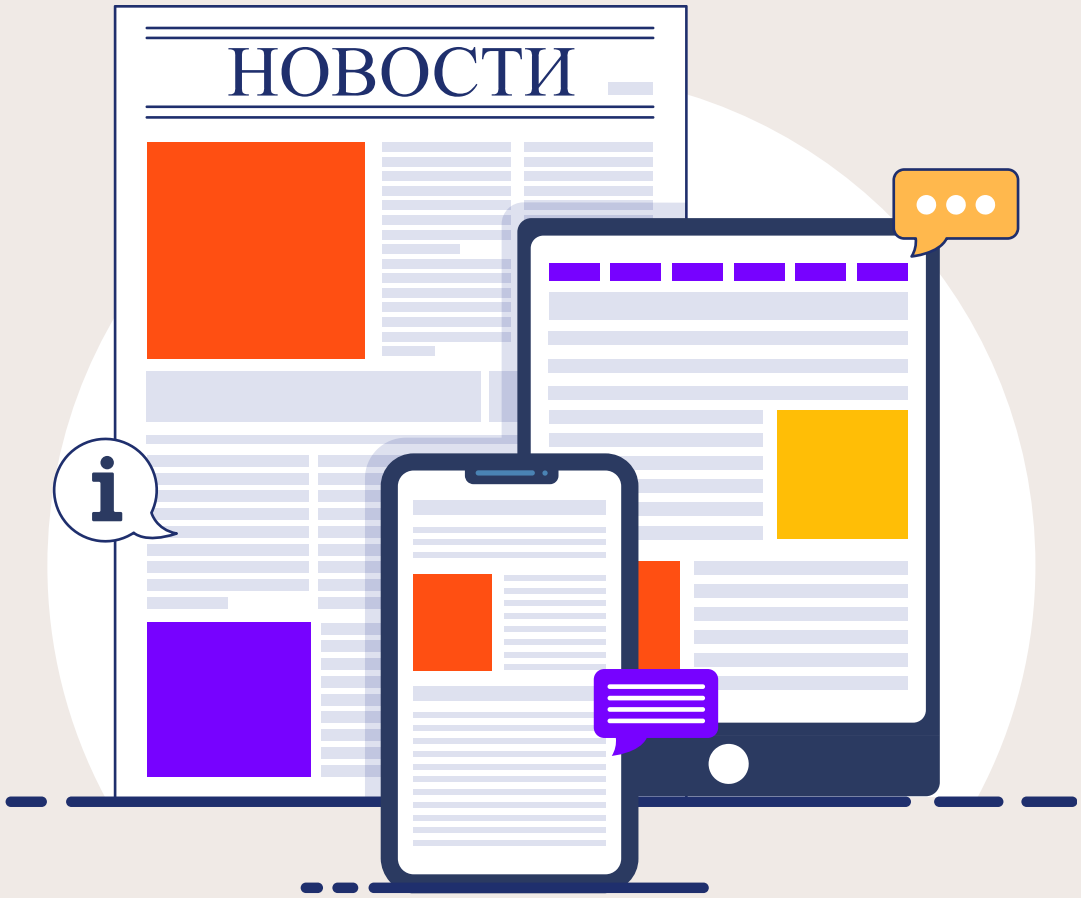
- Не реагируйте на провокации и завершайте звонки.
- Добавьте номер(а) в черный список.
- Свяжитесь с сотовым оператором и попросите подключить функцию «Определитель номера».

9. Что делать, если телефон ведет себя странно?

- Если на экране появились незнакомые приложения или на телефон приходят сообщения с нечитаемыми символами, а зарядка садится быстрее чем обычно, то ваше устройство скорее всего заражено вирусом или взломано.
- Установите на телефон антивирусное приложение.
- Проведите сканирование на наличие вирусов.
- Удалите незнакомые приложения.
- Обновите программное обеспечение до последней версии (функцию можно найти в предустановленном приложении «Настройки»).

10. Что делать, если вы сомневаетесь в достоверности источника информации?

- Проверить достоверность информации можно только на интернет-ресурсах авторитетных СМИ.
- Убедитесь, что другие авторитетные СМИ подтвердили и опубликовали эту же новость. Появление только в одном источнике информации говорит о том, что сенсацию еще не успели подтвердить или опровергнуть.
- Удостоверьтесь, что текст не подталкивает вас к действиям. Например, перейти на другой сайт или оставить гневный комментарий.



Что делать при обмане

1. Обратиться в полицию

- По телефону горячей линии МВД 8-800-222-74-47
- На сайте МВД
- В отделении полиции по месту жительства

2. Обратиться в банк

По закону банки обязаны вернуть клиенту незаконно списанные средства, если не докажут, что клиент сам нарушил правила использования карты.

- Позвоните в банк, сообщите о проблеме и заблокируйте карту.
- Попробуйте отменить транзакцию в личном кабинете банка или в мобильном приложении.
- Запросите подробную выписку со счёта, где будет указано, куда переведены деньги.
- Если банк отказывается решать ваш вопрос, попросите письменный отказ с указанием причин. Напишите жалобу на сайте Банка России.

Если вы лично раскрыли мошеннику конфиденциальную информацию — например, дали пин-код от карты или сказали CVV-код — банк не обязан возвращать деньги. Этот платёж считается добровольным, банк не имеет права отменять его и списывать деньги со счёта получателя. Банки не вмешиваются в договорные отношения клиентов, все претензии между плательщиком и получателям решаются без участия банка