Ростелеком

Кибербезопасность:

Вопросы, ответы, полезные советы

О чем говорят цифры?

300 млрд

рублей украли
кибермошенники
у россиян в 2024 году

20 %

пострадавших от
кибермошенников –
люди старшего поколения

>80 %

инцидентов, связанных
с кибербезопасностью,
начинается с фишинга
fishing англ. = рыбалка

Ростелеком

Методы социальной инженерии

83 % успешных атак реализованы при помощи методов социальной инженерии – психологического манипулирования людьми с целью совершения определенных действий или разглашения конфиденциальной информации. В **75%** атак используются технологии **ИИ**

ИНФОРМАЦИЯ – самая ценная валюта

Ростелеком

Самые «популярные» сценарии

«Вам полагается прибавка к пенсии» – неучтенный стаж – звонок из Социального фонда России

«Получите новые льготы» – ЖКУ – запись на прием в МФЦ

«Срочно переводите все на безопасный счет» – звонок из «банка», «МВД», «ФСБ»

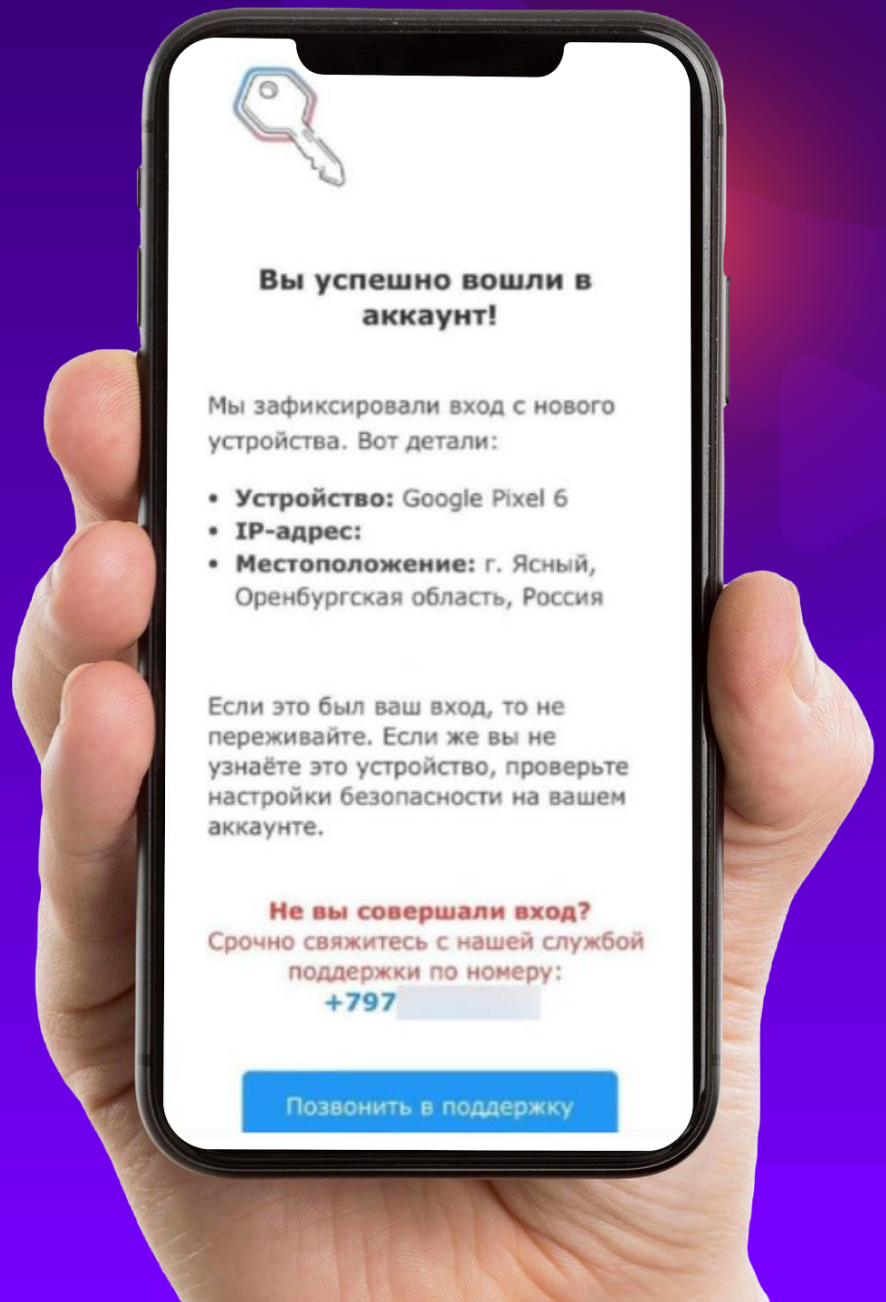
«Новый полис ОМС» «Провайдер ускорит Интернет» «Выгодные инвестиции» «Истекает срок действия SIM карты» «QR код домового чата» «Мама, я попал в аварию»

Ростелеком

«Свеженькое»

Звонок от сотрудников Федеральной налоговой службы. Вы не подали сведения о доходах за 2024 год в форме 3-НДФЛ. Для записи на прием требуют сообщить либо паспортные данные, либо ИНН.

Письма от «Госуслуг» о попытках входа в аккаунт с других устройств.
В сообщениях указан поддельный номер телефона службы поддержки.



«Свеженькое»

Мошенники представляются сотрудниками «жилищной инспекции» и угрожают изъятием домашних животных, если не будет переведен деньги. Они выясняют количество питомцев и требуют оплату за «разрешение» на их содержание. Злоумышленники отправляют ссылки на поддельные «Госуслуги», чтобы украсть личные данные.

Аферисты представляясь инженерами оператора связи, и под предлогом «проверки телефонной линии» просят набрать комбинации вроде #90, #09 или других. «Нажатие этих цифр передает управление сим-картой аферистам, что позволяет им совершать звонки за ваш счет и получать доступ к банковским приложениям»

Ростелеком

Что объединяет эти схемы?

1. Звонок или СМС с незнакомого номера
2. Запрос ваших персональных данных
3. Просьба сообщить код из СМС
4. Просьба скачать, установить, приложение по ссылке
5. Возможны все варианты

Ростелеком

«Выудить» информацию можно по разному

Фишинг
в интернете

Фишинг
в почте

Фишинг в
мессенджерах

Вишинг по
телефону

Ростелеком

Как распознать фишинговый ресурс (сайт)?

01 Зайти на сайт и сделать заказ. Если он не пришел – значит обман

02 Зарегистрироваться на сайте

03 Проверить Интернет-адрес сайта и замочек в адресной строке

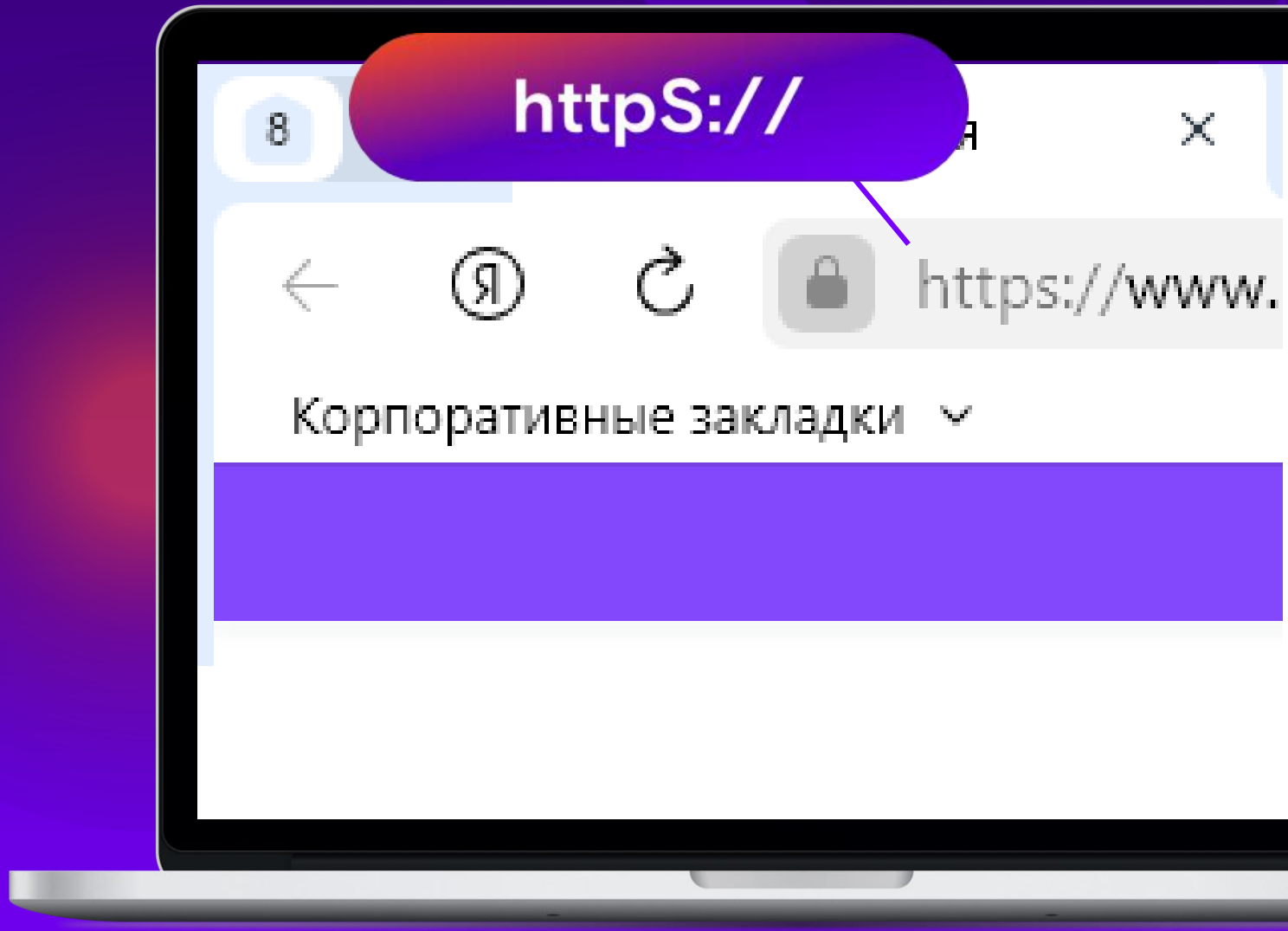
04 Написать администратору ресурса «Вы не мошенники?»

Ростелеком

Как распознать фишинговый ресурс?

Правильный ответ:
Проверить Интернет-адрес сайта и замочек в адресной строке

За **2025 год** специалисты Роскомнадзора **заблокировали** более 12 000 **фишинговых ресурсов** и более 60 сайтов, на которых распространялось вредоносное программное обеспечение: https://portal.noc.gov.ru/ru/news/



Ростелеком

Какой адрес Портала государственных услуг РФ верный?

01

gosuslugi.ru

02

gosuslugi.com

03

gosyslugi.ru

04

gosusllugi.ru

Ростелеком

Вам поступает СМС: "Вы не оплатили коммунальные услуги, завтра вам отключат свет! Срочно переведите деньги". Ваши действия?

01

Заплачу сразу – не хочу остаться без света

02

Проверю задолженность на сайте по ссылке из этого СМС

03

Проверю задолженность на официальном сайте или в личном кабинете поставщика услуг

04

Попрошу назвать мой лицевой счёт и сверю его с квитанцией

Ростелеком

На почту пришло письмо от знакомого с вложенным файлом и текстом «Посмотри срочно!». Как вы поступите?

01

Сразу открою файл — вдруг там что-то важное

02

Напишу знакомому и уточню, действительно ли он мне это отправил

03

Перешлю письмо подруге, чтобы она тоже посмотрела

Ростелеком

Д’Артаньян

Королева просила привезти подвески

Бэкингем

Хорошо, сударь, но лучше я лично уточню ее запрос

Вам звонят из органов правопорядка, предлагают перевести деньги на безопасный счет. Ваши действия?

01

Попросить к телефону Глеба Жиглова

02

Не вовлекаться в разговор и прекратить звонок

03

Попытаться перевоспитать мошенников взывая к совести

Ростелеком

Простые правила

Не торопиться переходить по ссылкам в почте и смс

Не торопиться скачивать вложенные файлы

Не вводите никакие данные в предлагаемые формы и не сообщайте их по телефону

Не отвечайте на сомнительное письмо или звонок с незнакомого номера

Не пересылать письмо другим

Удалить из почтового ящика и почистить корзину

Ростелеком

Как защитить свой аккаунт в мессенджерах? Ваши действия?

01

Выставить корректные настройки приватности и конфиденциальности

02

Использовать защищенный мессенджер

03

Вести переписку с нескольких аккаунтов и разных телефонов, что бы запутать мошенников

Ростелеком

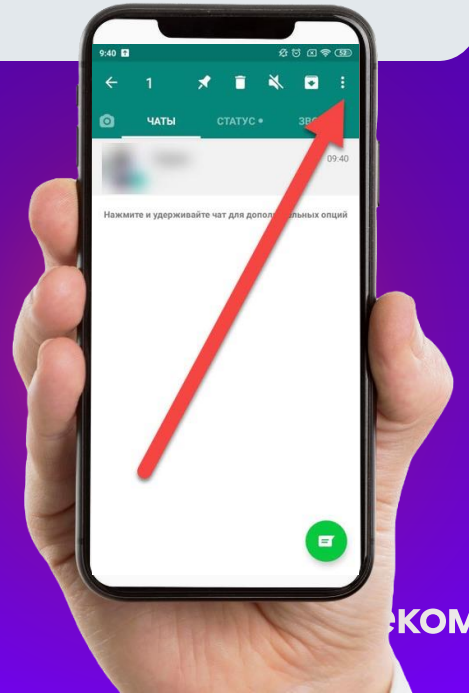
Несколько советов по настройкам безопасности WhatsApp

Включаем двухшаговую проверку и указываем свой адрес электронной почты на случай, если забудем PIN-код

Включаем двухшаговую проверку и указываем свой адрес электронной почты на случай, если забудем PIN-код

Закрываемся от добавления в посторонние группы Конфиденциальность – Группы – Мои контакты

Отключаем звонки с неизвестных номеров Настройки - Конфиденциальность – Звонки



Регулярно проверяем связанные устройства. Три точки - Связанные устройства

Устанавливаем код устройства на случай кражи устройства

Для продвинутых Конфиденциальность – Расширенные настройки и Проверка конфиденциальности

Несколько советов по настройкам безопасности Телеграм:

Регулярно проверяем, на каких устройствах активен ваш аккаунт. Настройки –> Устройства (если находим аномалии – сразу удаляем подозрительный сеанс)

Включаем код-пароль. Настройки –> Конфиденциальность –> Код-пароль (включаем и не забываем) можно облачный пароль включить

Скрываем свой номер телефона. Настройки –> Конфиденциальность –> Номер телефона (настраиваем так, чтобы его никто не видел)

Скрываем свои фото. Настройки –> Конфиденциальность –> Фотографии профиля (настраиваем так, чтобы их никто не видел)

Запрещаем себя добавлять в групповые чаты и каналы. Настройки –> Конфиденциальность –> Приглашения (настраиваем так, чтобы никто не мог приглашать)

Запрещаем звонить посторонним. Настройки –> Конфиденциальность –> Звонки. PEER-TO-PEER (анонимные звонки) вообще отключаем, а обычные – по своему усмотрению, но точно не «для всех»

Как вы думаете в будущем фишинг?

01 Станет законным

02 Перестанет быть прибыльным

03 Станет еще опаснее

04 Останется на текущем уровне

Ростелеком

Фишинг станет еще опаснее

В РФ за I квартал 2025 года выявили более **60** уникальных дипфейков

Дипфейк (от deep learning — «глубокое обучение» и fake — «подделка») — синтез правдоподобных поддельных изображений, видео и звука при помощи искусственного интеллекта

Что делать?

Перечислили деньги:

заявление в банк
и в полицию

Угнали аккаунт, взломали почту:

сменить пароль, а лучше создать новые

Сняли деньги с карты без вашего ведома:

перевыпустить карту, заблокировав старую

Потеряли смартфон:

смените пароль на учетке google, удалите куки и историю в браузере, заблокируйте и перевыпустите банковские карты, сбросьте настройки до заводских

Сходите в МФЦ

и напишите заявление на отказ от сделок без вашего присутствия

Установите запрет на Госуслугах

на получение кредитов
и займов

Ростелеком

Полезное

Дополнительный текст

Договоритесь о кодовом слове известном только вашим близким

Рассказывайте о кибербезопасности

Будьте внимательны к себе и близким

Не бойтесь прекратить телефонный разговор

Узнавайте новое

Будьте бережнее к себе и окружающим


Всегда на связи
Ростелеком