



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ



Академия
МИНПРОСВЕЩЕНИЯ РОССИИ



Информационные угрозы:

ФИШИНГ



Шпион в овечьей шкуре

ФИШИНГ - вид интернет-мошенничества, цель которого — получить данные пользователей

Механизмы работы:

поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные перейдя по ссылке в электронном письме



Немного статистики

92%

Электронная почта

самый популярный инструмент как для распространения вредоносного ПО (92%), так и для фишинга (96%)

* Расследования утечки данных Verizon 2018

56%

Руководителей служб

информационной безопасности (далее ИБ) считают защиту электронной почты своей ключевой профессиональной задачей

* Опрос CISCO

36%

Респондентов

потеряли важные данные в результате фишинговых атак

* Опрос CISCO

Прогнозы

в 2022 году

Фишинг становится более индивидуальным, атака всё чаще осуществляется через мессенджеры и социальные сети

POSITIVE TECHNOLOGIES

Фишинг: при чём тут инженерия?



Психология

не менее важный инструмент киберпреступников, чем коддинг и веб-дизайн

Удачный фишинг -

это как правило результат успешного манипулирования. Ниточки, за которые дёргают мошенники, — это не только доверчивость, невнимательность или жадность. Это сострадание, зависть, доброта и даже лень. Объединяет их одно - бдительность жертвы усыпляется общественно одобряемым ритуалом

Это и есть социальная инженерия

Мы пользуемся ей сотни раз каждый день. Любое взаимодействие, которое не рефлексится нами, потому что «так принято», — элемент социальной инженерии. Из таких взаимодействий во многом состоит наша жизнь

Но когда мы говорим о киберпреступности, **социальная инженерия** — это совокупность психологических методик и мошеннических приёмов для создания условий, при которых манипулировать человеческим сознанием и поведением становится значительно проще

Механизм работы



Самопроверка: увидим ли мы угрозы?

I

Шаг 1

Изучаем каждый ресурс
в течение 3-5 секунд
и определяем признаки
фишинга

II

Шаг 2

Проверяем ответ



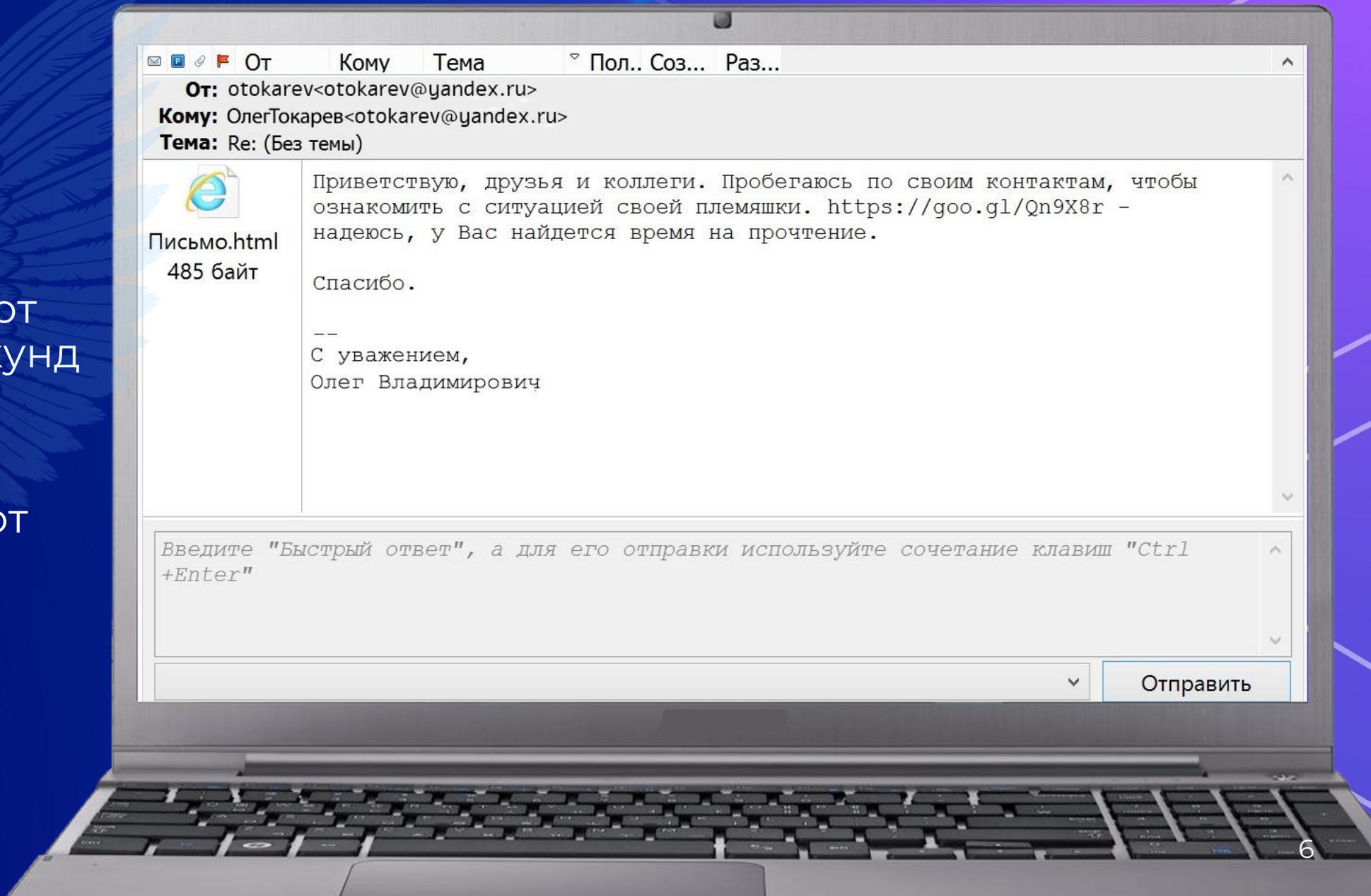
3 секунды

в среднем тратит
пользователь на решение
перейти по ссылке
в письме или на сайте

Ресурс 1

Изучите скриншот
в течение 3-5 секунд

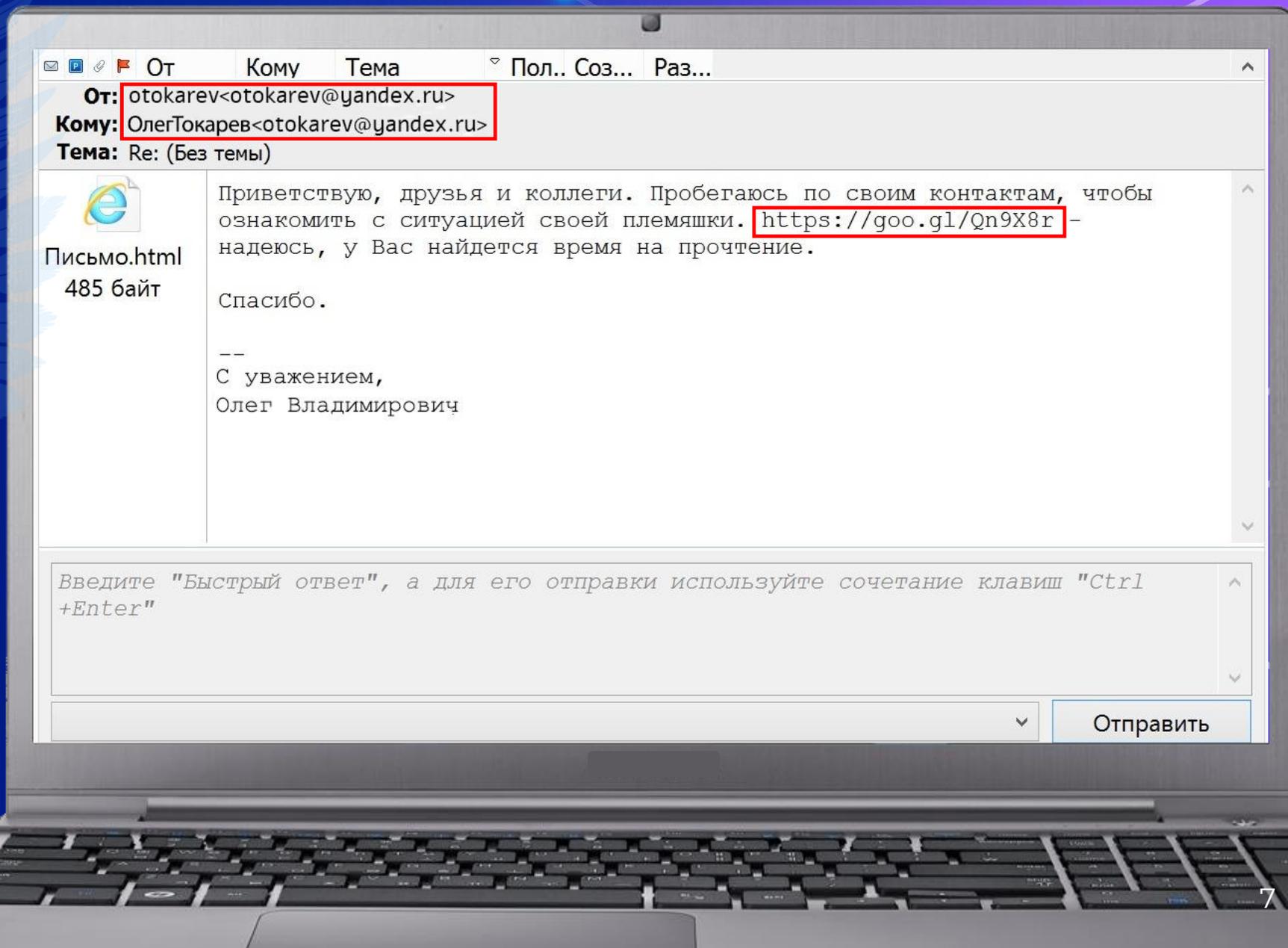
Как вам кажется,
безопасен ли этот
ресурс?



Ответ 1

Отправитель
и получатель – один
и тот же адрес. Это
явный признак
фишинга

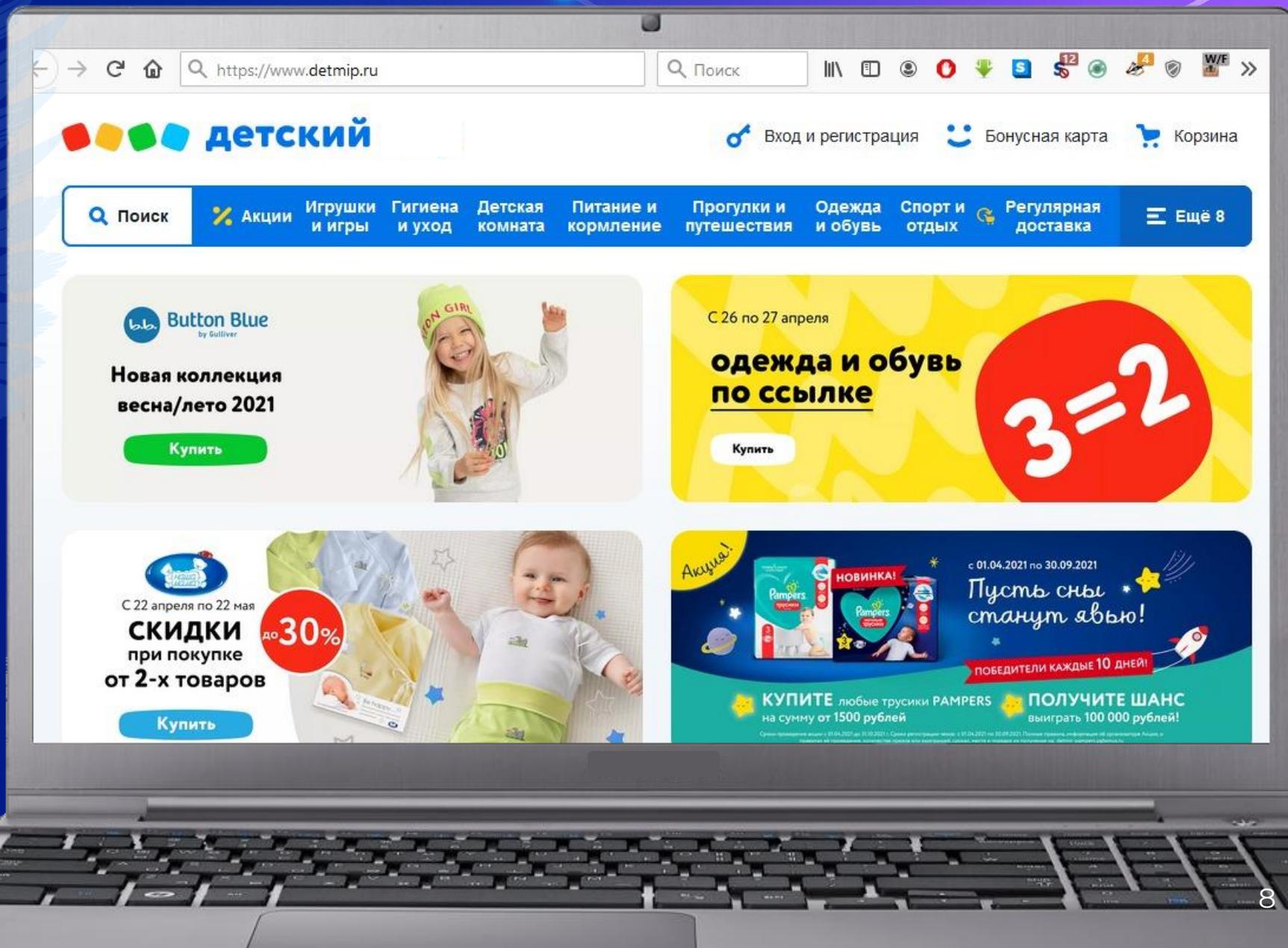
Опасным является
переход по ссылке
из письма



Ресурс 2

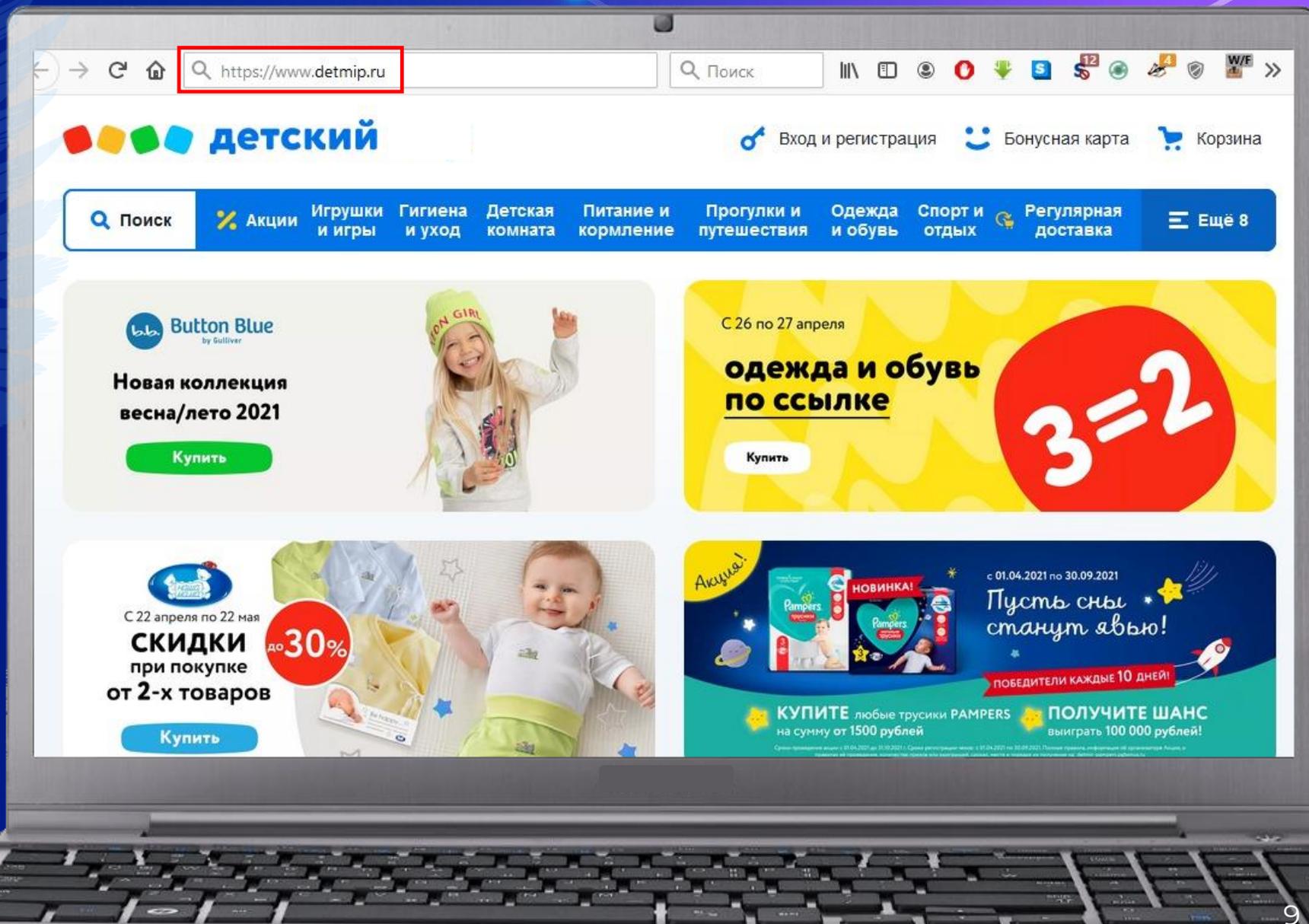
Изучите скриншот в течение 3-5 секунд

Как вам кажется, безопасен ли этот ресурс?



Ответ 2

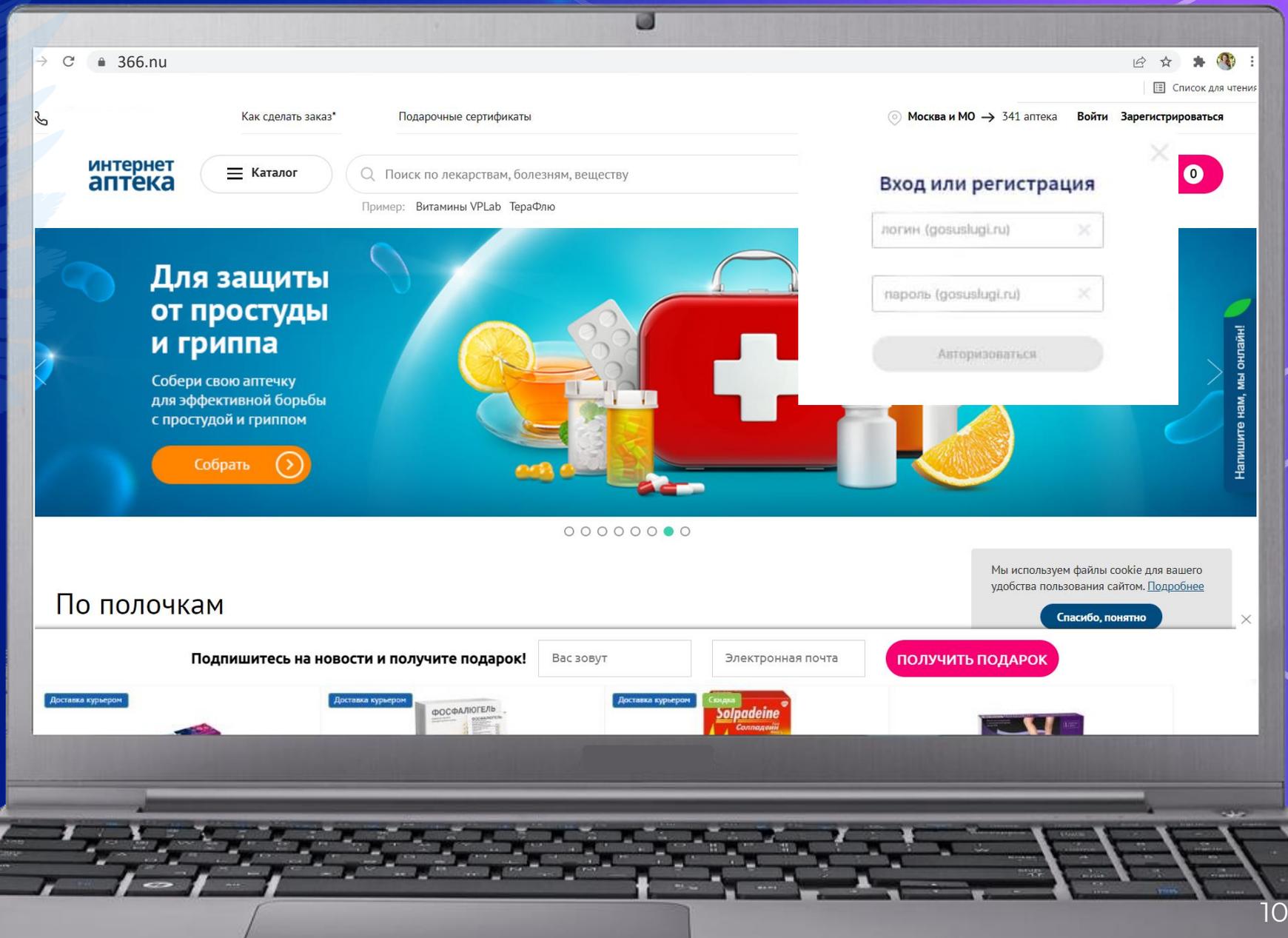
Ошибка в адресной строке – «detmip» вместо «detmir». Это явный признак фишинга



Ресурс 3

Изучите скриншот
в течение 3-5 секунд

Как вам кажется,
безопасен ли этот
ресурс?

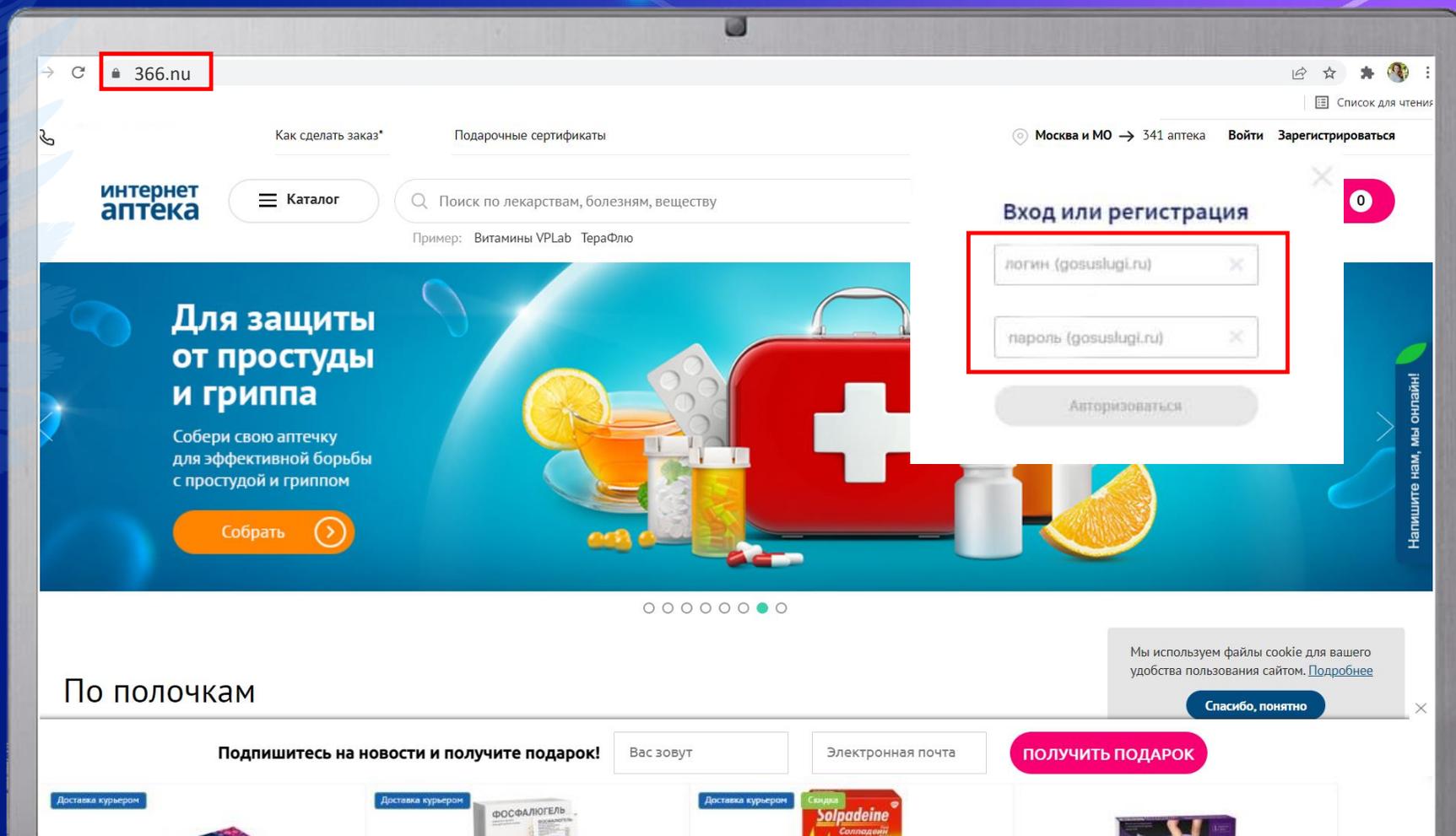


Ответ 3

Ошибка в адресной строке – «**nu**» вместо «**ru**»

Ресурс просит ввести учётные данные от портала Госуслуг

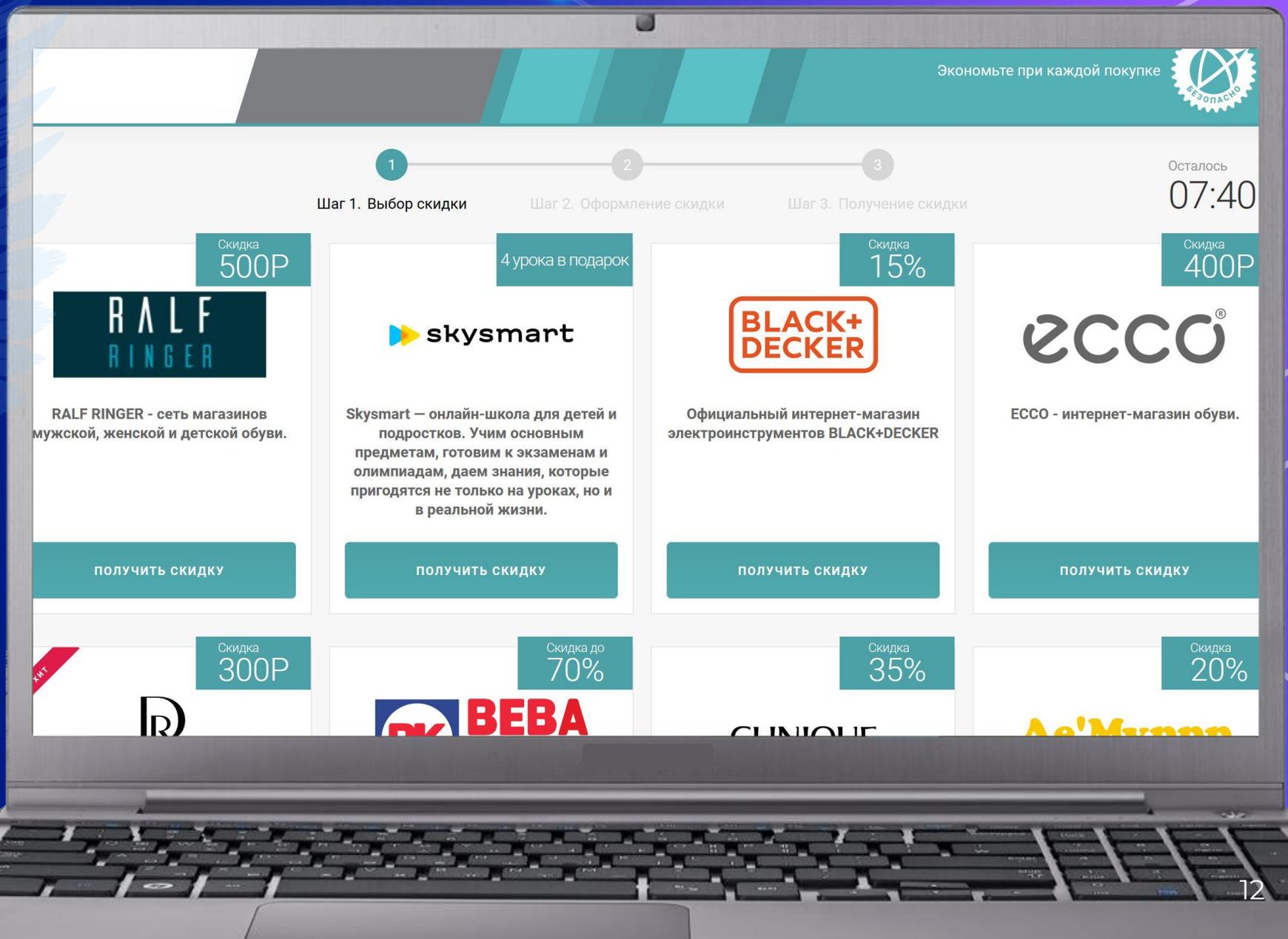
Это явные признаки фишинга



Ресурс 4

Изучите скриншот в течение 3-5 секунд

Как вам кажется, безопасен ли этот ресурс?



Ответ 4

Этот ресурс **безопасен**, признаков фишинга на нём нет

Экономьте при каждой покупке

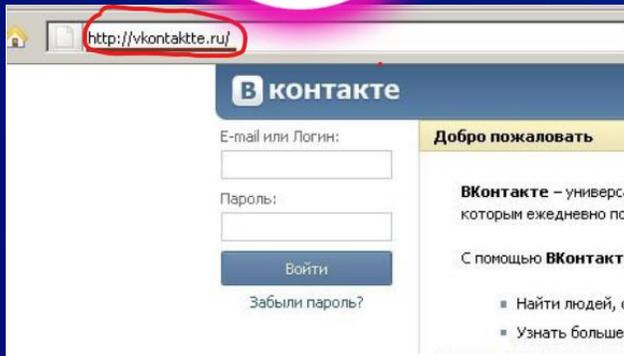
Осталось 07:40

Шаг 1. Выбор скидки Шаг 2. Оформление скидки Шаг 3. Получение скидки

Скидка	Бренд	Описание	Кнопка
Скидка 500Р	RALF RINGER	RALF RINGER - сеть магазинов мужской, женской и детской обуви.	получить скидку
4 урока в подарок	skysmart	Skysmart — онлайн-школа для детей и подростков. Учим основным предметам, готовим к экзаменам и олимпиадам, даем знания, которые пригодятся не только на уроках, но и в реальной жизни.	получить скидку
Скидка 15%	BLACK+DECKER	Официальный интернет-магазин электроинструментов BLACK+DECKER	получить скидку
Скидка 400Р	ECCO	ECCO - интернет-магазин обуви.	получить скидку
Скидка 300Р	DR		
Скидка до 70%	BEBA		
Скидка 35%	CLINIQUE		
Скидка 20%	Ac'Mirra		

Как происходит фишинговая кража

Переход по ссылке



Шаг 1

Ссылка ведёт на фишинговый сайт

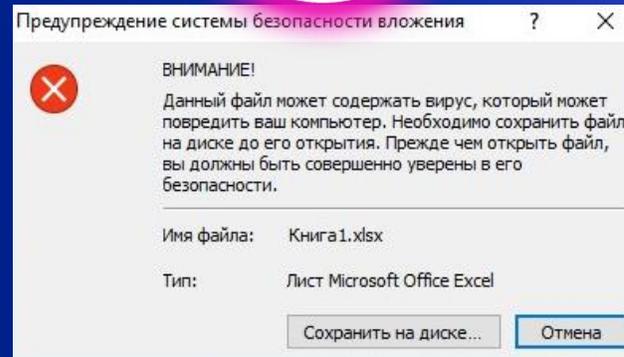
Шаг 2

Пользователь вводит логин/пароль

Результат

Преступник получает учетные данные пользователя и доступ к сервису, от которого они получены

Открытие файла



Шаг 1

Пользователь получает в письме исполняемый (.exe) либо ассоциированный (xls, rtf, doc, msi) файл

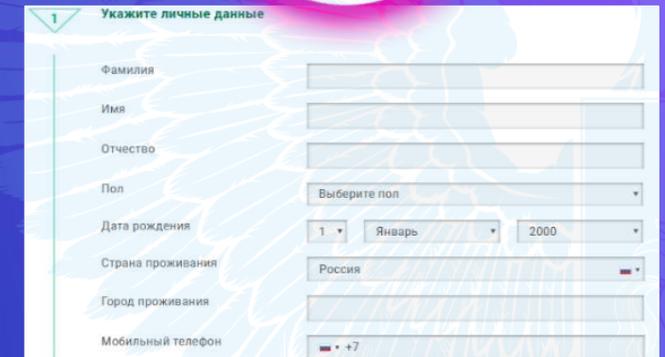
Шаг 2

Двойной клик по файлу приводит к его открытию и запуску

Результат

Преступник получает удаленный доступ к устройству/внедряет логгер

Заполнение формы



Шаг 1

Пользователь вводит конфиденциальные данные

Шаг 2

Нажимает на кнопку «Отправить»

Результат

Преступник получает то, что отправил пользователь

Некоторые примеры фишинга



рассылки от «государственных структур»



рассылки от «банков» и «финансовых организаций»



рассылки от «интернет-магазинов», предложения услуг, личные письма



фишинг через смс, мессенджеры и звонки



взлом сайта, на котором вы были зарегистрированы

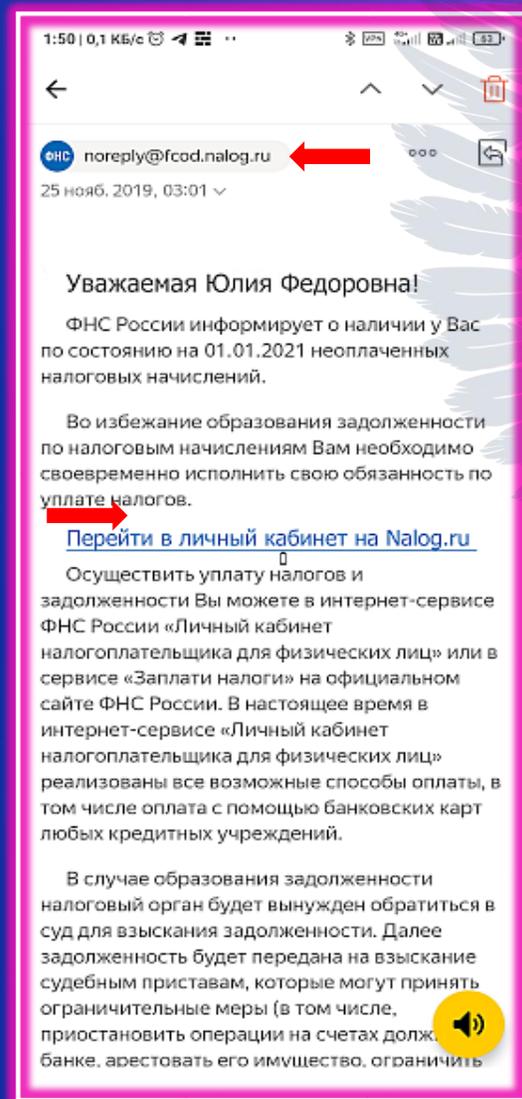
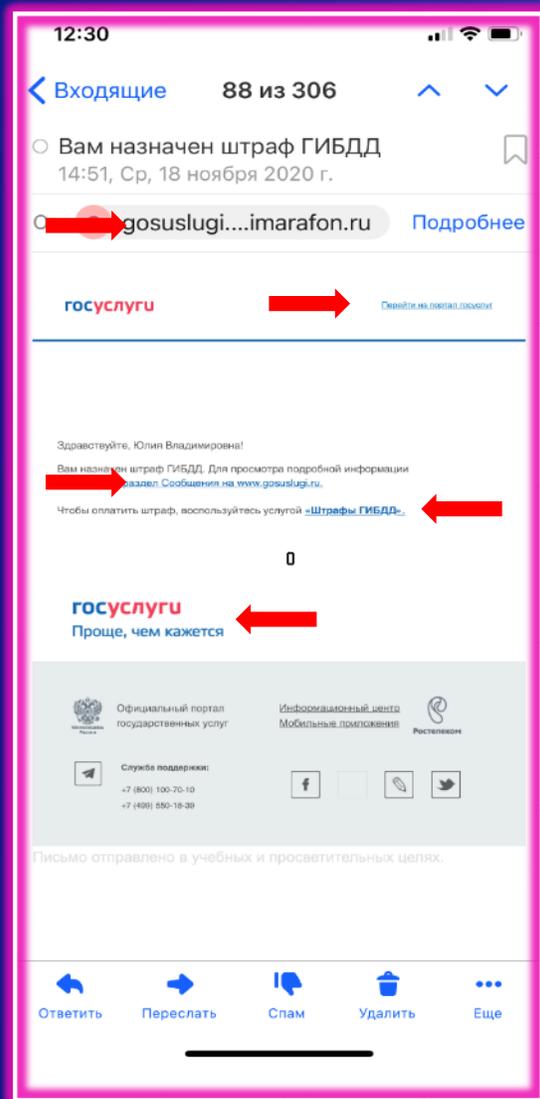
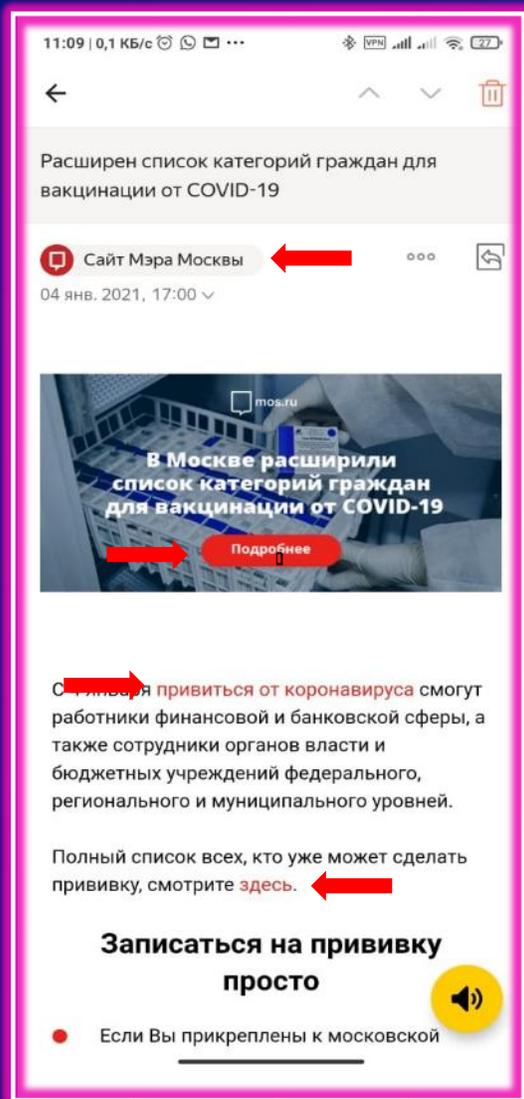


Мошенники – хорошие психологи и прекрасно знают, какое влияние на пользователя оказывает получение таких писем или звонков

Чувство тревоги, неизвестности, желание побыстрее разобраться с проблемой влияют на получателя такого письма и заставляют совершать **необдуманные поступки**

Пример фишинга: рассылки от «Госструктур»

Внимательно изучите скриншоты, обращая особое внимание на места, отмеченные стрелками



Пример фишинга: рассылки от «Госструктур»

Технология фишинга: «Проверка»

Несуществующий адрес

Отправителя можно проверить на сайте госорганов

Вредоносная ссылка

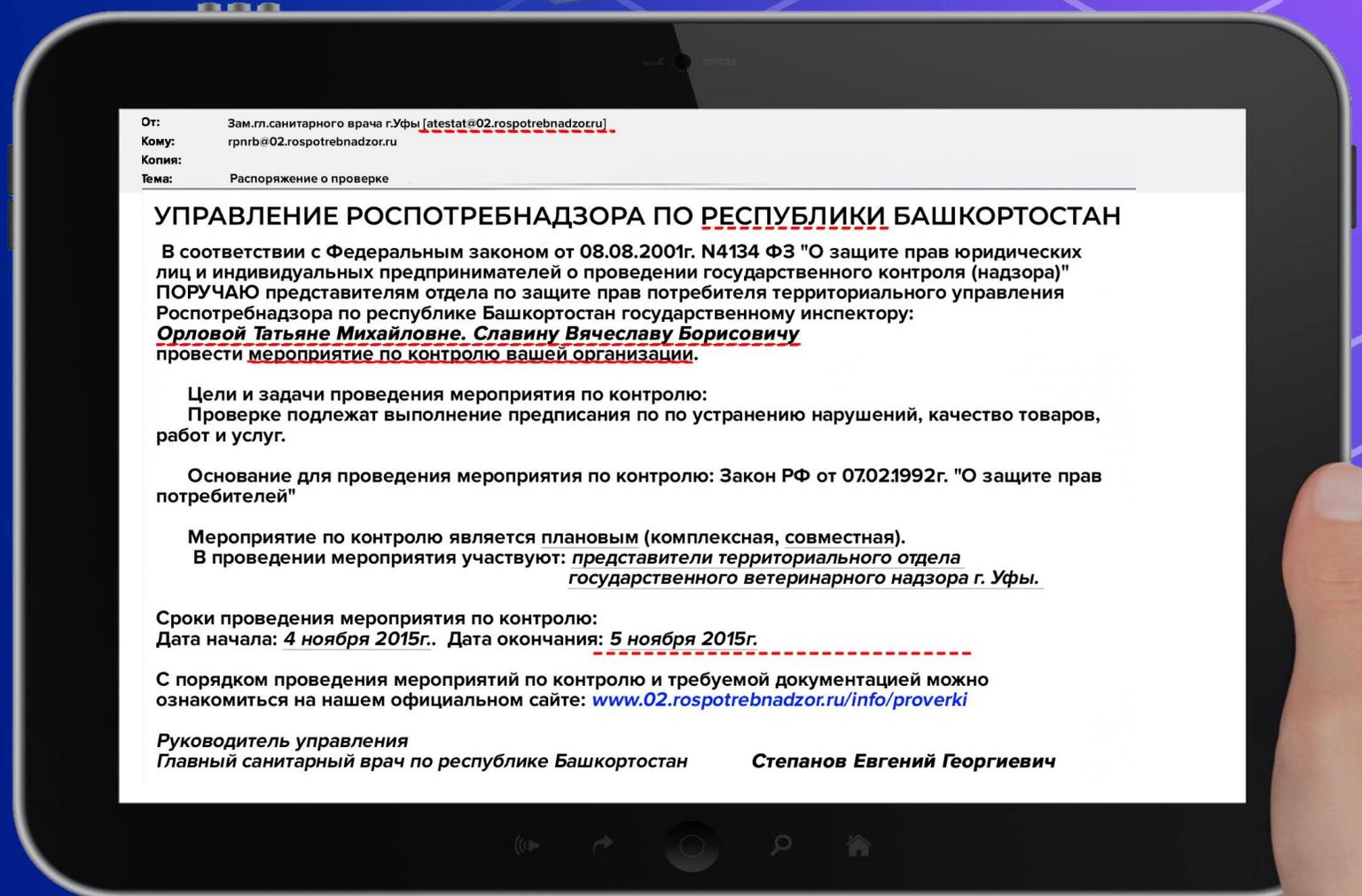
Правильную ссылку также можно посмотреть на сайте госорганов

Чувство тревоги

Текст письма побуждает к немедленным действиям

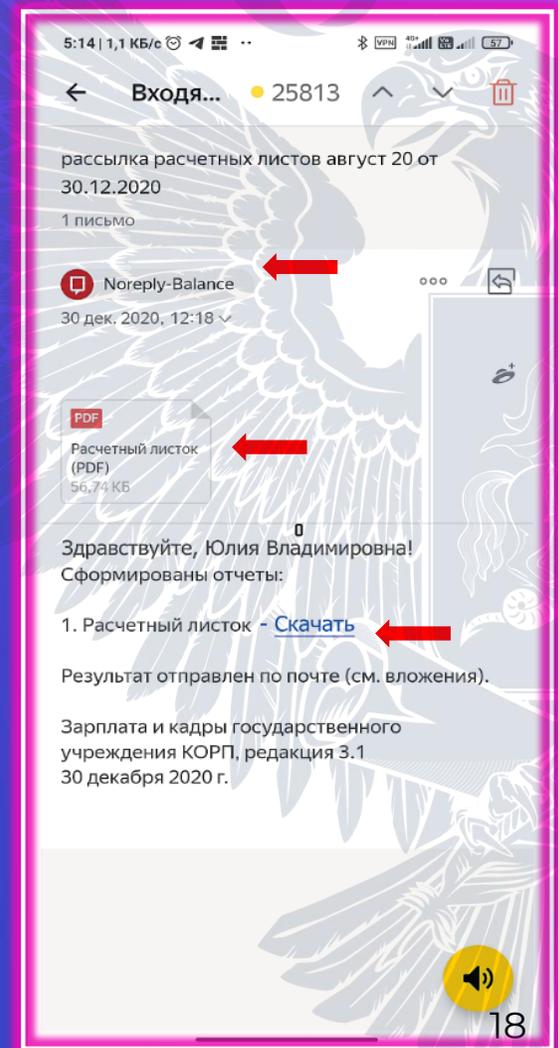
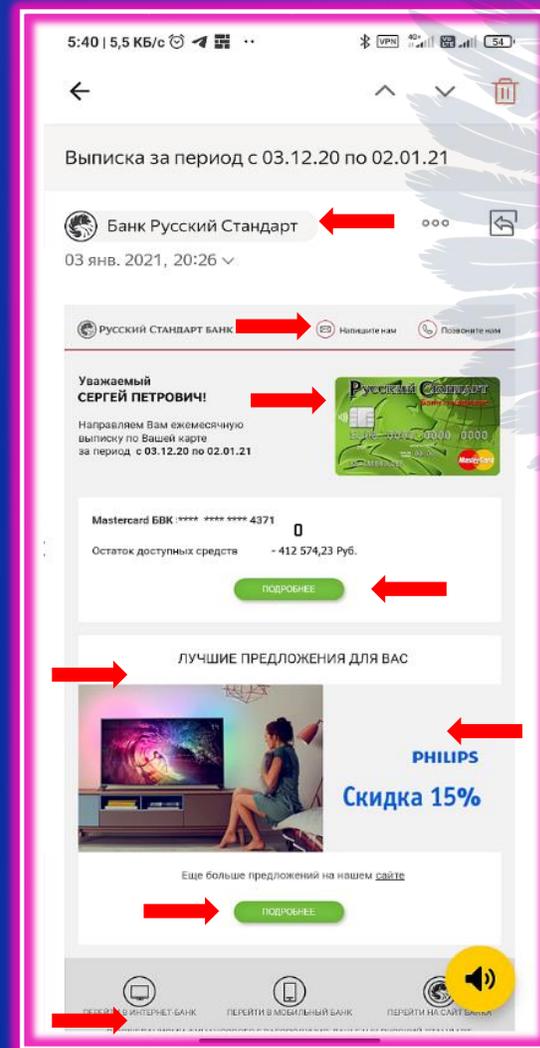
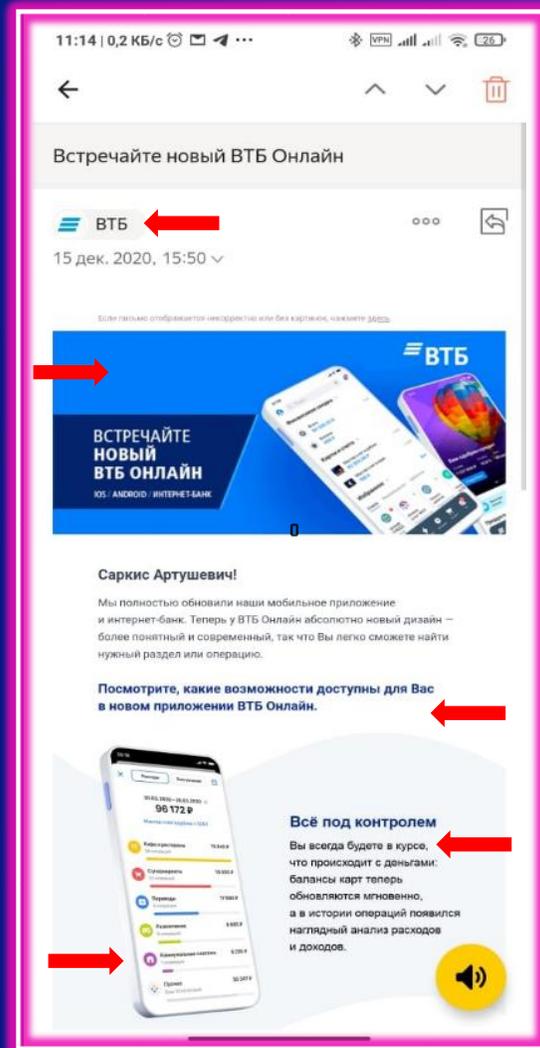
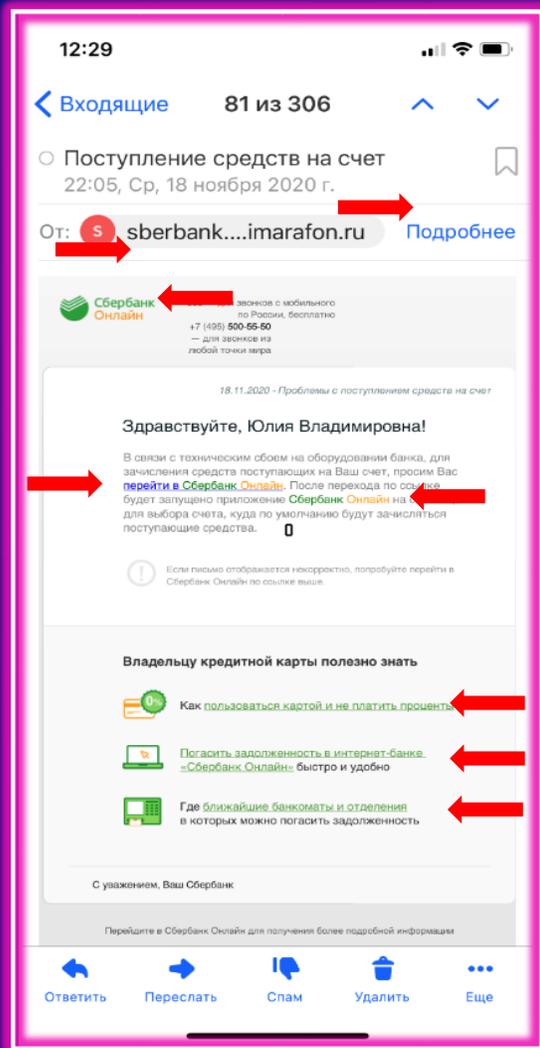
Несуществующие сотрудники

Контактные данные проверяются звонком по телефону



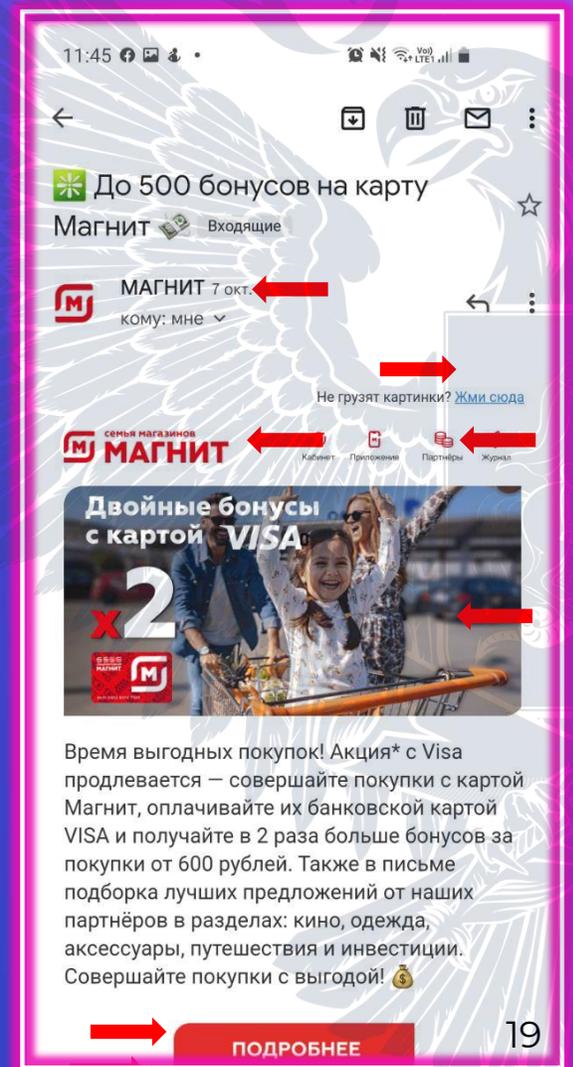
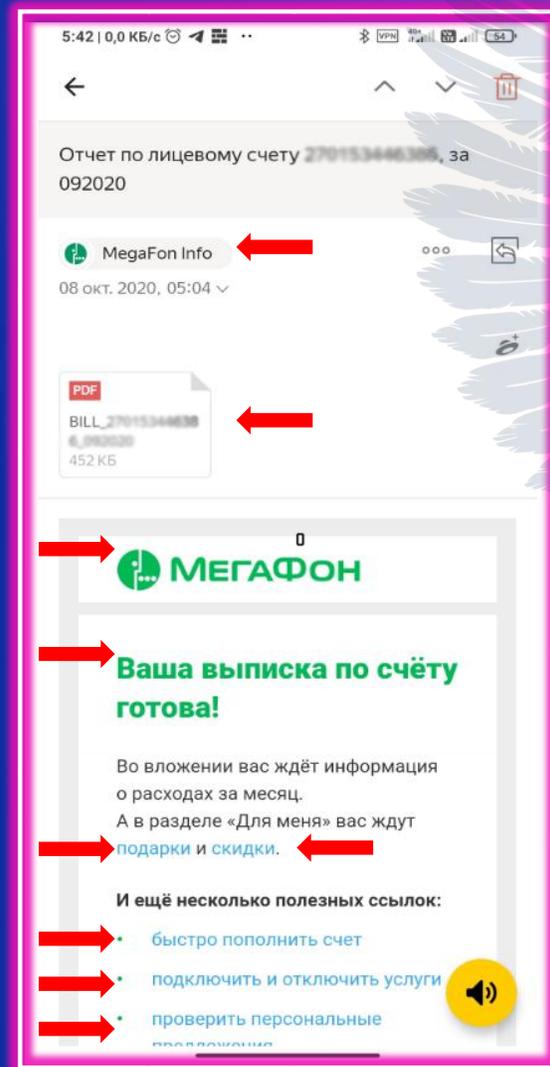
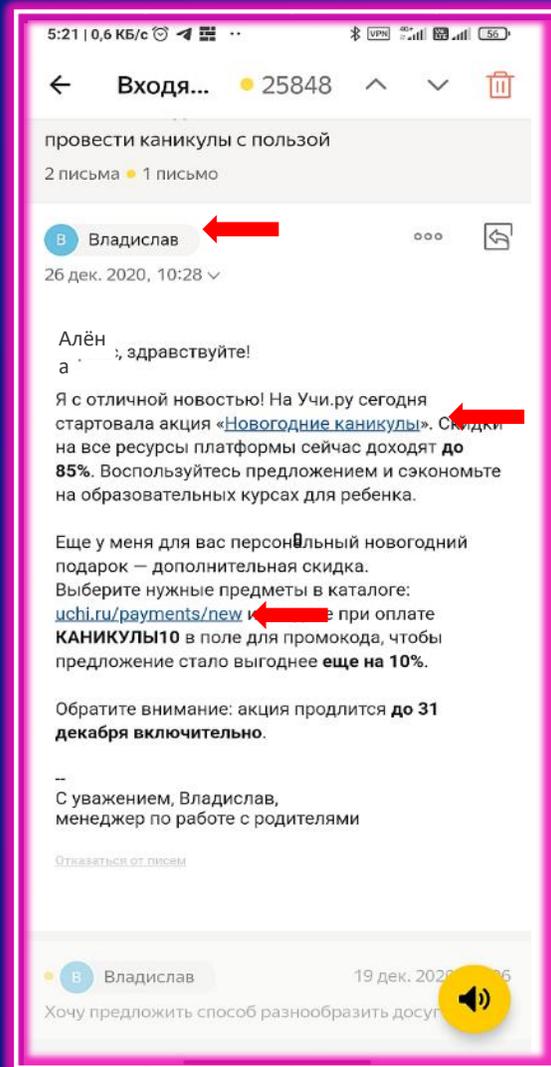
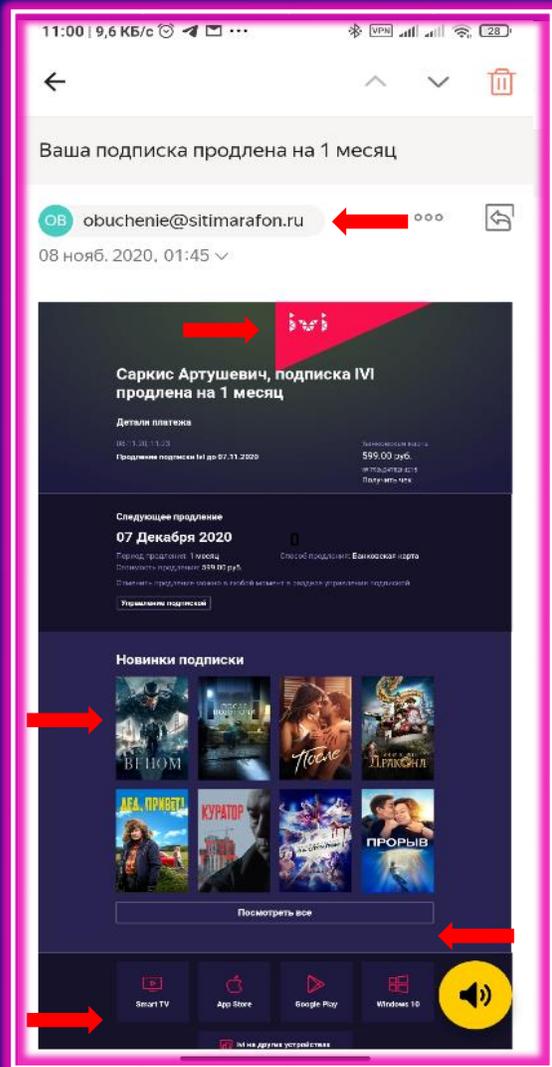
Пример фишинга: рассылки «от банков»

Внимательно изучите скриншоты, обращая особое внимание на места, отмеченные стрелками



Пример фишинга: рассылки от «интернет-магазинов» и предложения услуг, личные письма

Внимательно изучите скриншоты, обращая особое внимание на места, отмеченные стрелками



Пример фишинга: личные письма

Технология фишинга: шантаж

Вынуждение к немедленным действиям

Текст письма побуждает к немедленным действиям

Нет конкретики

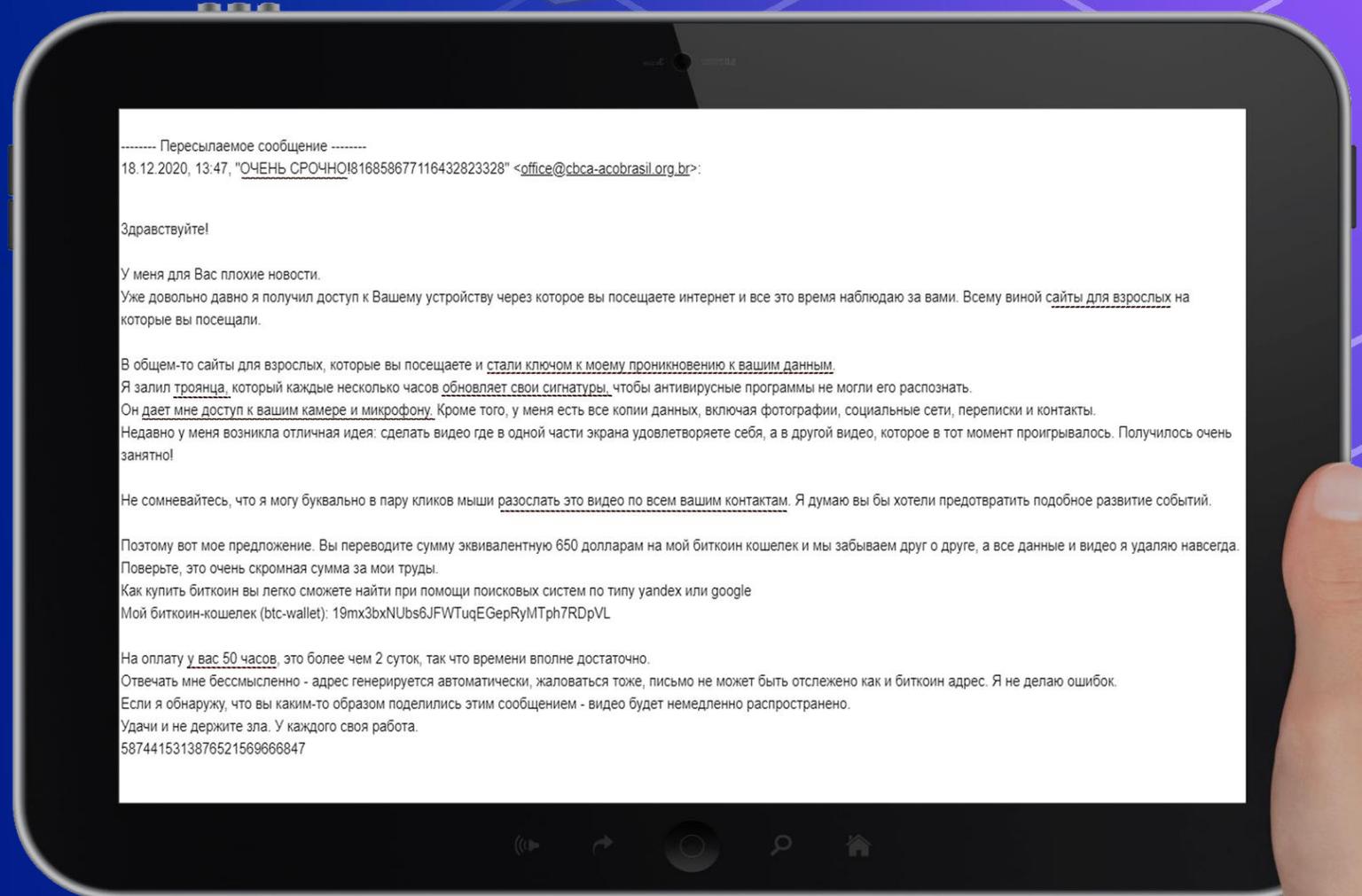
Шантажист не даёт вообще никакой конкретики – он классически пытается запугать

Универсальность темы

Универсальная тема, рассчитанная на массового получателя

Техническая безграмотность

Троянец - это агент внутри совершенно работоспособной оболочки



Мы вам не писали. Фишинговые e-mail рассылки



Письма обладают очень высоким качеством подделки: логотип банка / сайта / провайдера, выглядящие в точности так же, как настоящие



Ссылки очень похожи на URL оригинальных сайтов

Пример фишинговой ссылки:

<https://www.google.ru>



Итак – основные признаки фишингового письма

Внезапность

Письмо и сообщаемые данные для вас неожиданны



Вредоносное ПО

Текст сопровождается ссылкой, которая ведет на фишинговый ресурс, либо к письму прикреплен файл с вредоносным содержанием



Ошибки

В тексте могут присутствовать орфографические, фактические ошибки



Как распознать фишинговое письмо?

Странный адрес

Адрес почтового ящика отправителя не принадлежит официальному домену организации, от имени которой направлено письмо



Тема

Письма могут вызвать тревогу и озабоченность

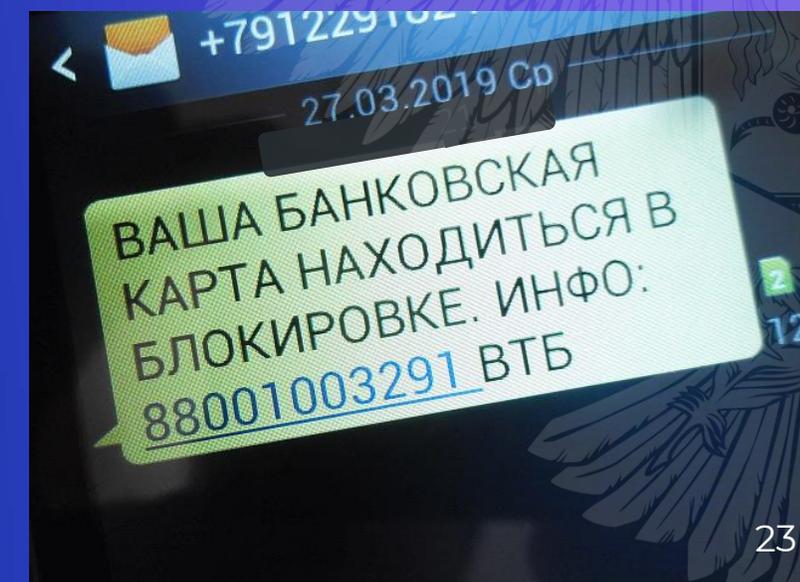
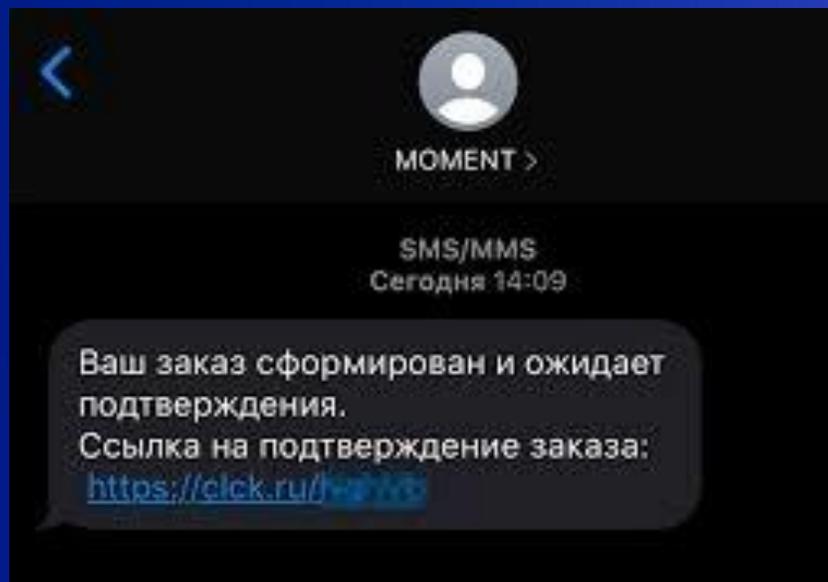
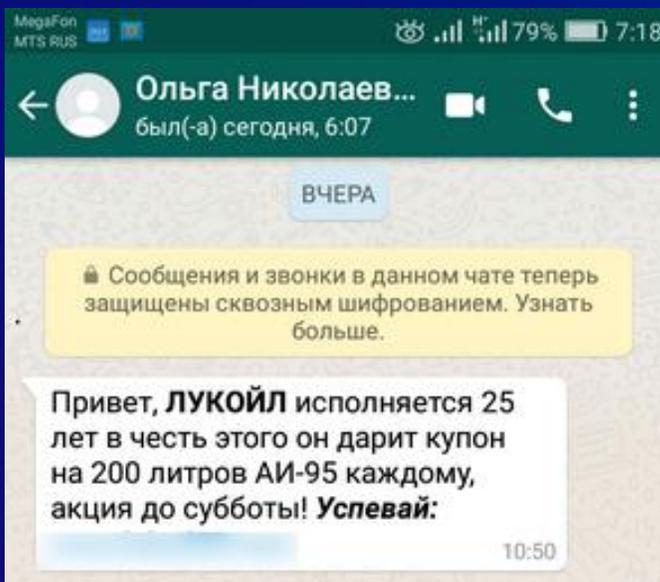
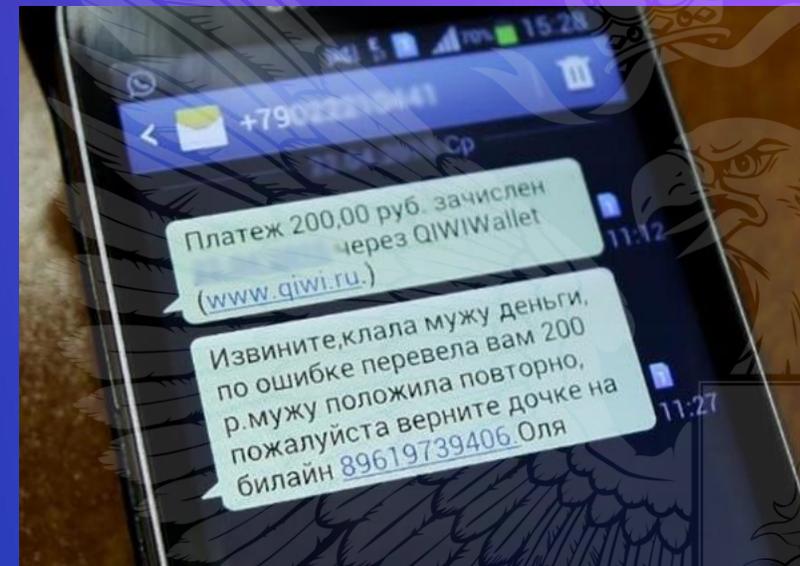
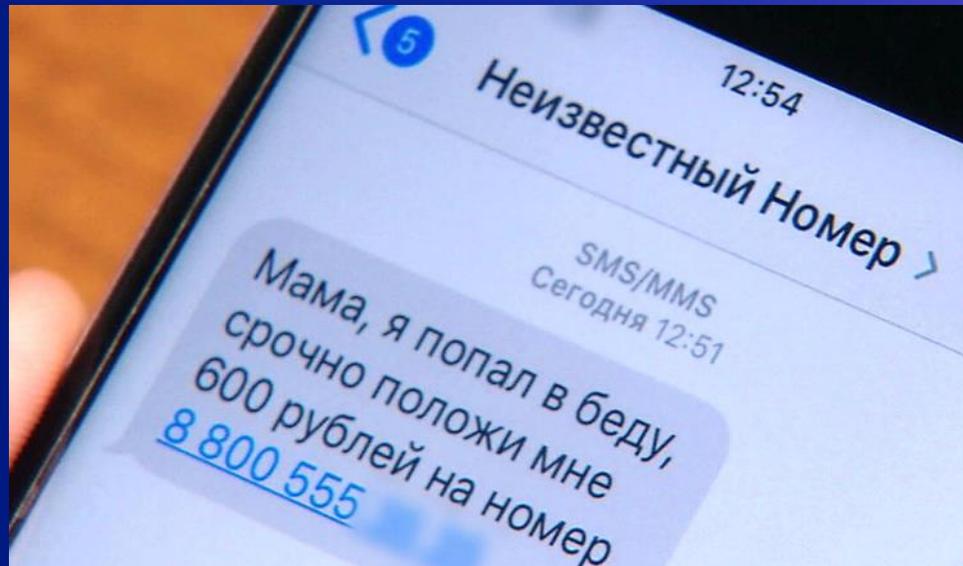
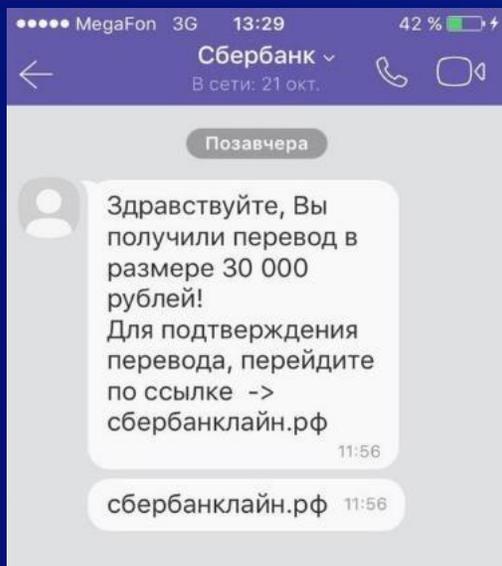


Незнакомый отправитель

Если вы неожиданно получаете письмо от незнакомого отправителя – не спешите на него отвечать



Фишинг через SMS и мессенджеры



Фишинговые телефонные звонки

Более **98%** российских пользователей мобильных устройств сталкивались со звонками мошенников

12% респондентов потеряли деньги из-за стандартных телефонных «разводов»

НО

29% абонентов из России используют софт для определения телефонных номеров мошенников

19% устанавливают различные баннеркаты и адблокеры (BannerCut, AdBlocker)

Февраль 2022, отчёт TelecomDaily

92%

целевых атак были направлены против объектов критической информационной инфраструктуры. Всего в 2021 году в России было выявлено 300 таргетированных атак



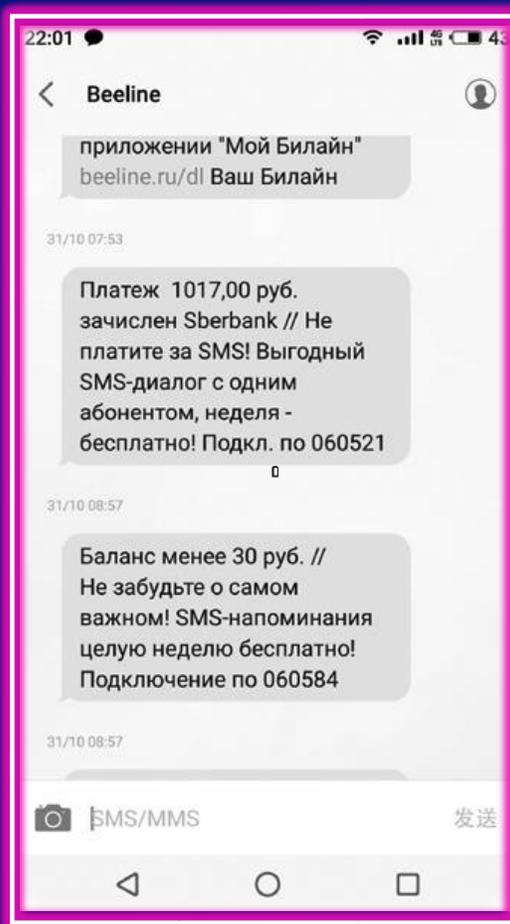
18%

зафиксированных атак — дело рук высоко-профессиональных киберпреступных группировок



Как это происходит

Отправка сообщения



Шаг 1

Пользователь отправляет СМС



Шаг 2

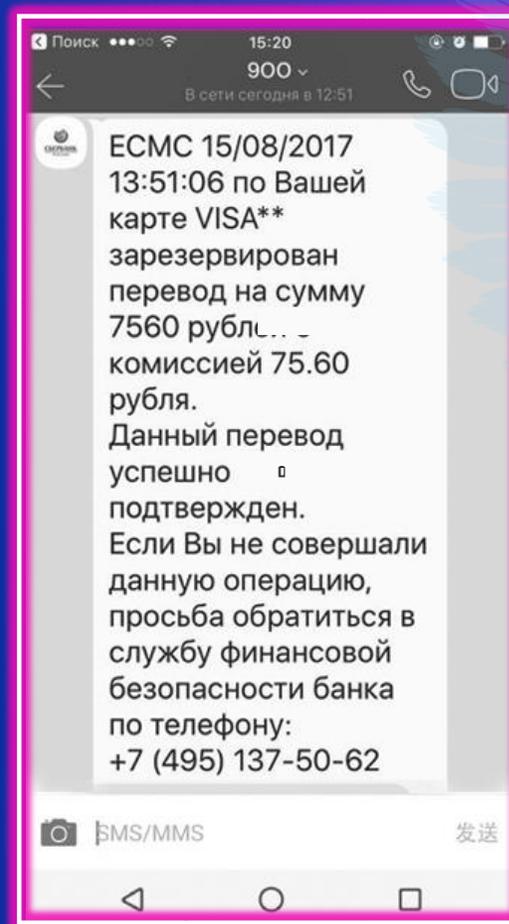
Получает код подтверждения и вводит его ответным сообщением



Результат

Преступник, получив код подтверждения, использует его для авторизации списания со счёта мобильного телефона пользователя денежных средств

Звонок на номер



Шаг 1

Преступник звонит и убеждает пользователя, что он — сотрудник СБ банка



Шаг 2

Пользователь выполняет указания «сотрудника»



Результат

Денежные средства Пользователя украдены, банковские реквизиты скомпрометированы и могут быть использованы третьими лицами для «отмывания»

Взлом сайта, на котором вы были зарегистрированы

Как это происходит

Шаг 1

Регистрация на разных сайтах

Шаг 2

Аккумуляирование личной информации

Шаг 3

Взлом сайтов с вашими данными

Результат:

ваши данные в свободной продаже

Будут скомпрометированы и окажутся в публичном доступе: ваш e-mail, номер телефона, логин/пароль, вся переписка данные

Высокий риск оказаться в ситуации шантажа!

Проверьте: <https://haveibeenpwned.com/>

Персональные данные могут быть скомпрометированы независимо от пользователя

Причины

- 1 Утечка из государственных СУБД или информационных систем
- 2 Взлом сервиса с большим пользовательским пулом
- 3 Квалифицированная хакерская атака
- 4 Прочие ЧП, связанные с компрометацией данных по вине третьих лиц

Утечки 2021

Январь:

В результате взлома сайта Hyundai.ru в сети появились данные 1,3 млн российских владельцев машин этого бренда

Февраль:

В результате «внутренней утечки» скомпрометированы почти 5000 почтовых адресов Яндекс

Апрель:

Выставлена на продажу база банка «Дом.рф» с более, чем 100 тыс. «профайлов» тех, кто обращался в банк за кредитом. В профайле желаемая сумма, телефон, e-mail, ФИО, дата рождения, сумма и вид кредита, паспортные данные, ИНН и СНИЛС, адрес, место работы и размер дохода

Октябрь:

Выставлена на продажу база автовладельцев Москвы. В каждой строке ФИО, дата рождения, телефон, код VIN, номер машины, марка и модель. Всего в базе более 50 млн. строк

Как защититься?



Уникальный пароль

Он должен быть для **каждого** сервиса, на котором хранится ценная информация



Резервное копирование

Одна копия – на физическом носителе, вторая – в облачном хостинге



Двухфакторная аутентификация

Туда, где это невозможно, не следует загружать или отправлять ничего ценного и конфиденциального

Рекомендации по защите от технологических угроз

Три важных «НЕ»

1

Не открывайте

email, смс от незнакомых отправителей,

не переходите по ссылкам и не открывайте вложенные файлы

2

Не размещайте

персональные данные
в ненадежных
онлайн-сервисах

3

Не передавайте

конфиденциальные
данные (реквизиты
доступа, финансовую
информацию, и пр.)
**по общедоступным
Wi-Fi сетям**

Рекомендации по защите от технологических угроз

Используйте двухфакторную аутентификацию (2FA) и надёжные пароли

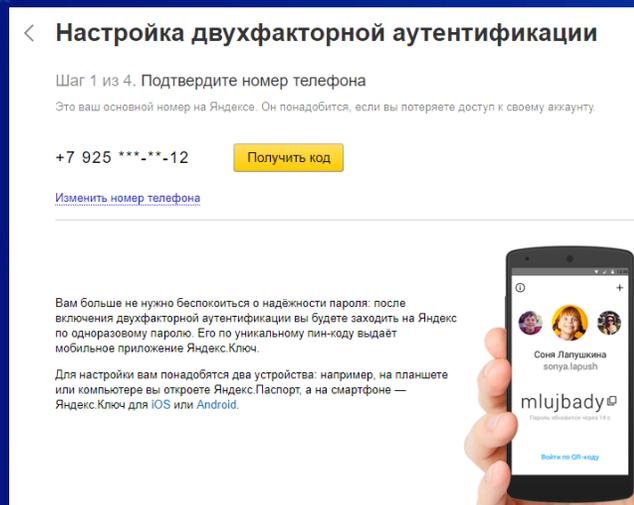
На примере аккаунта в почтовой системе:

1 **Откройте**
страницу настройки почты

2 **Выберите «безопасность»**
на панели навигации

3 **Нажмите**
«Двухэтапная
аутентификация»
в разделе «Вход
в аккаунт»

4 **Следуйте**
инструкциям
на экране



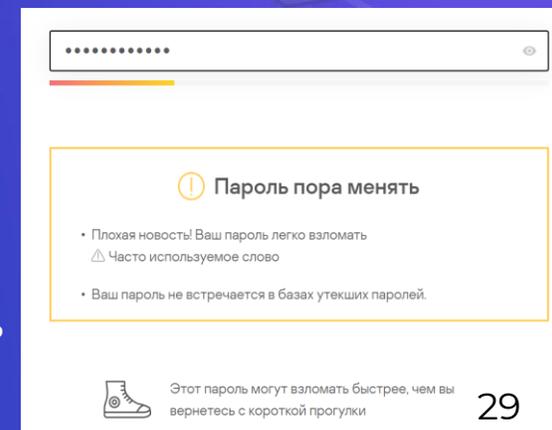
Критерии создания надёжного пароля:

1 **12 символов**
пароль должен составлять не менее 12 символов

2 **Разные регистры**
пароль должен содержать буквы разных регистров (строчные и прописные), цифры и символы — \$, #, &, @

3 **Уникальность**
нельзя использовать
один пароль на двух
и более сервисах

4 **Обновление**
каждый пароль
необходимо обновлять
несколько раз в год



Рекомендации по защите от технологических угроз

Установите ограничения конфиденциальности в социальных сетях

1

Откройте
страницу социальной сети

2

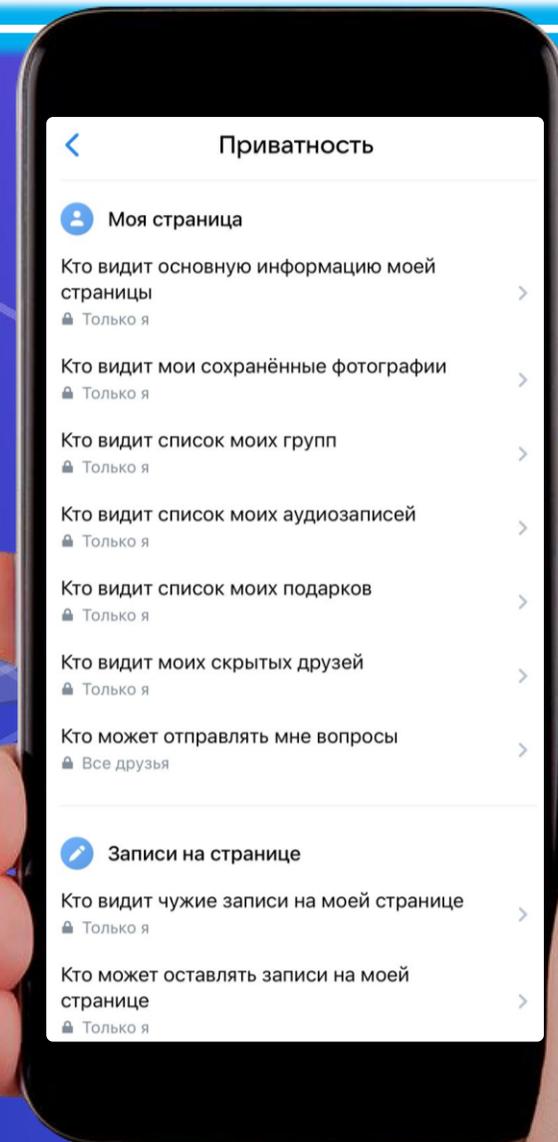
Выберите
«Настройки» на панели навигации

3

Выберите
«Приватность»

4

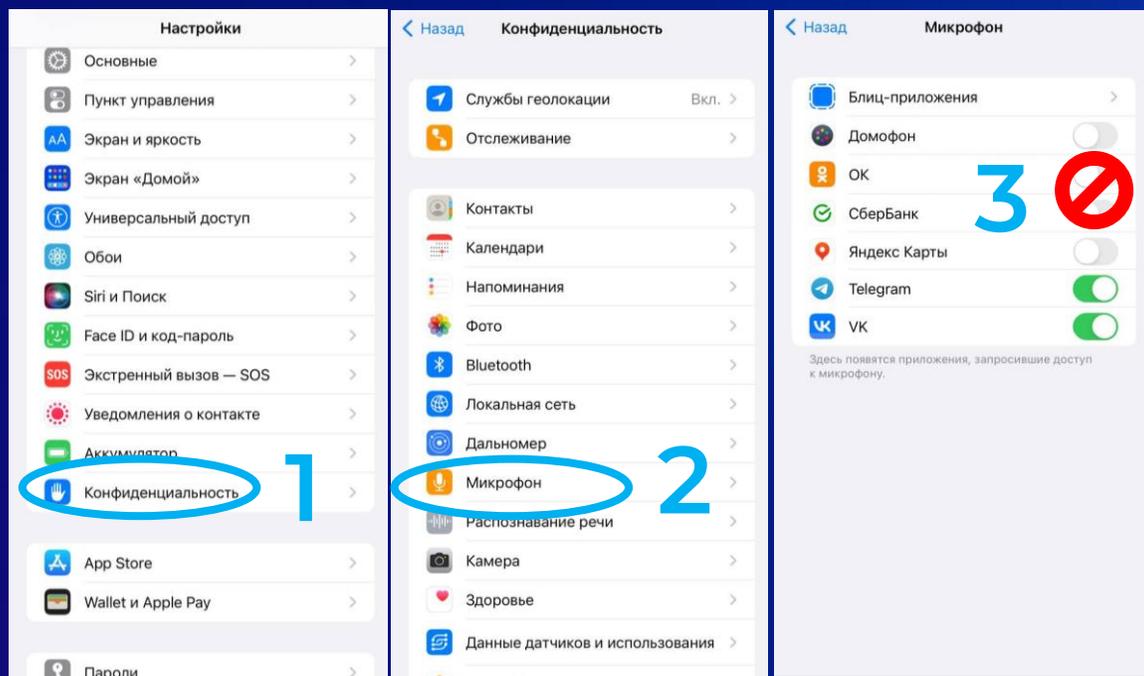
Максимально ограничьте
круг лиц, которые имеют доступ
к вашим данным



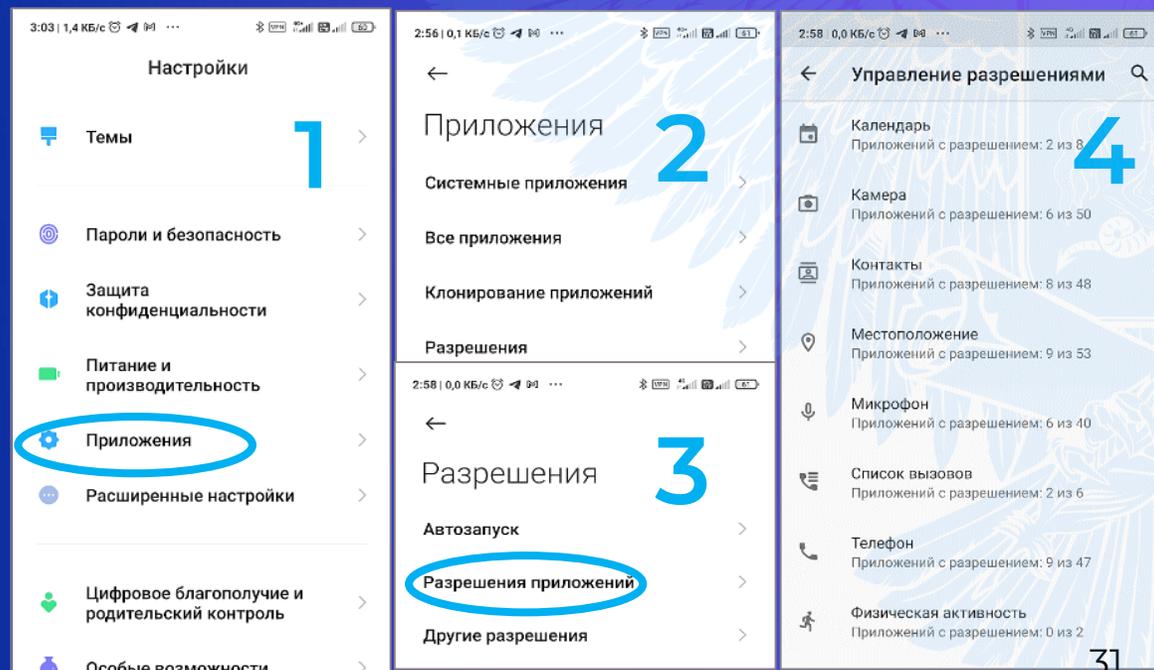
Рекомендации по защите от технологических угроз

Проверяйте разрешения и установите ограничения прав мобильных приложений и дополнений от браузеров. Оставьте приложениям минимальные права доступа к микрофону, камере, местоположению, контактам, хранилищу и пр.

iOS (iPhone)



Android



Рекомендации по защите от технологических угроз

Регулярно устанавливайте обновления безопасности

iOS



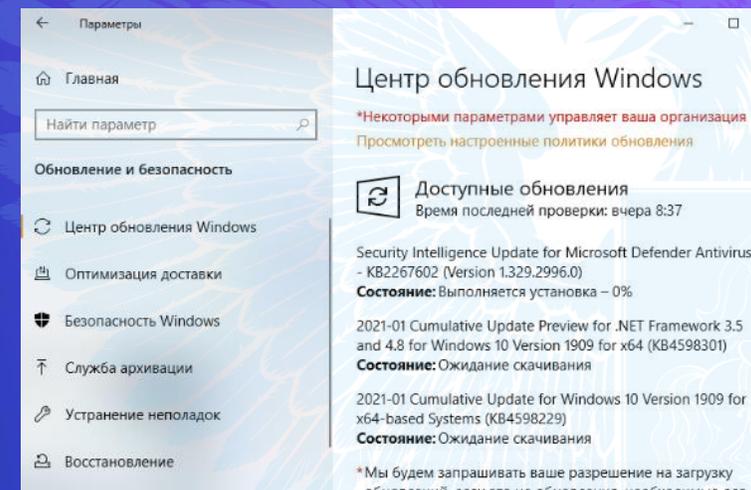
1 **Выбрать**

«Системные настройки» в меню Apple, затем нажать «Обновление ПО»

2 **Выбрать**

«Автоматически устанавливать обновления ПО Mac» для независимой установки будущих обновлений, в том числе для приложений, загруженных из App Store

Windows



1 **Выбрать**
в меню «Пуск»

2 **Перейти**
в раздел «Параметры» —
«Обновление и безопасность»

3 **Выбрать**
в разделе «Дополнительные
параметры» — способ установки
обновлений — «Автоматический»