Личная безопасность в современной жизни

Комаров Валерий Валерьевич

Департамент
информационных
технологий
города Москвы

Уникальность пароля

Для каждого ресурса необходимо иметь уникальный пароль!

- ✓ Интернет-порталы (Госуслуги и т.д.)
- ✓ Соцсети (VK, Одноклассники и т.д.)
- ✓ Рабочий аккаунт
- ✓ Мессенджеры (Whatsapp, Telegram, Viber и т.д.)
- ✓ Электронная почта
- ✓ Интернет-магазины
- ✓ Онлайн-банка
- ✓ Файловые хранилища
- ✓ Облачные хранилища и т.д.

Важно!

При взломе пароля на одном ресурсе – остальные пользовательские ресурсы будут защищены

Сложность пароля

Правила для создании **СЛОЖНОГО пароля**:

- ✓ Пароль должен состоять **не менее чем из 8 символов**, а лучше – 10 и более
- ✓ Наличие цифр и **букв верхнего и нижнего регистров**, идущих не подряд – AAaaBBbb
- ✓ Наличие **специальных знаков** – «!», «@», «#» и т.д. (если допустимо их присутствие)

Примеры надежных паролей:

- ✓ !tKbiPfDtNf19@(53)
- ✓ G1o!Og(9L)@e$
- ✓ 2!D4ci$6W8z(0o)

Надежный пароль **не должен содержать**:

- ✓ Имена
- ✓ Клички животных
- ✓ Названия городов
- ✓ Даты рождения
- ✓ Номера телефонов

Примеры НЕ надежных паролей:

- ✓ Qwerty12345
- ✓ p@ssword54321
- ✓ Zxcvbnm2023

Генерация пароля

- **Генерация пароля с помощью специализированных программ:**

✓ Желательно использовать установленные на **компьютер программы (оффлайн)**, т.к. онлайн сервисы не надежны

- **Создание пароля для каждого ресурса с помощью своего собственного алгоритма:**

Плюсы:

✓ Алгоритм создания знаете только Вы
✓ Алгоритм разрабатывается один раз (до следующего изменения алгоритма и соответственно пароля)
✓ Пароль не надо запоминать
✓ Нет необходимости где-то хранить пароль
✓ Легко заменить много паролей, меняя только алгоритм создания

Минусы:

✓ Если пароль был скомпрометирован, злоумышленник может попробовать расшифровать алгоритм создания пароля и подобрать пароль и к другим ресурсам

Пример. Придумываем алгоритм и пароль

- **1 этап** – **Буквы** (для почтового ящика на https://mail.ru/ берем слово «**MAIL**» набираем его в обратной последовательности, изменяя регистр, начиная с большой буквы).

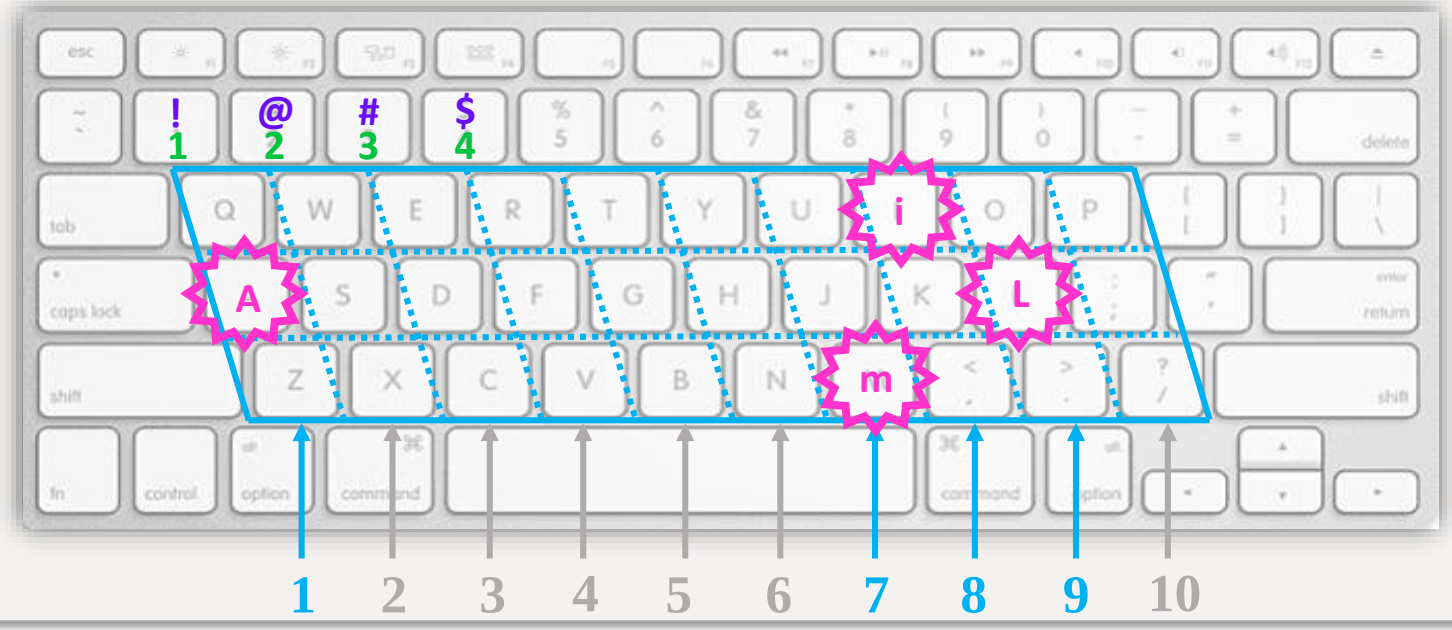
  Получим: L***i***A***m***

- **2 этап** – **Специальные знаки** «!», «@», «#» и «$» расположим их после букв по порядку, начиная с «!».

  Получим: **L!**i@**A#**m$****

- **3 этап** – **Цифры** – первую цифру после специального знака поставим по порядку, начиная с единицы: Получим: **L!1*i@2*A#3*m$4*.** Вторую цифру выберем по номеру буквы по вертикали («9», «8», «1», «7»).

  Получим итоговый надежный пароль по придуманному алгоритму: **L!19i@28A#31m$47**



Хранение пароля

Важно!

Сохранение пароля в браузере не безопасно, т.к. пароли хранятся на третьей стороне

- Если для создания паролей пользоваться своим **личным алгоритмом**, то запоминать необходимо сам алгоритм, необходимости хранения паролей нет

  ✓ Сам алгоритм рекомендуется записать где-то в блокноте дома во избежание его похищения

- Менеджер паролей — это специальная программа, установленная на вашем устройстве (оффлайн), которая шифрует ваши пароли в специальном файле-хранилище

  ✓ Храните мастер-пароль от хранилища паролей на бумаге

  ✓ Никому не сообщайте мастер-пароль

  ✓ Мастер-пароль от хранилища паролей должен иметь высокую степень надежности

Время жизни пароля

- Рекомендуемая **частота смены паролей** или алгоритма их создания не реже, чем **раз в квартал**

- Если ресурс особенно интересен для злоумышленников – его «**угоняемость**» возрастает

Например:

- ✓ портал Госуслуг
- ✓ онлайн-банки
- ✓ почта рабочая и личная
- ✓ социальные сети
- ✓ мессенджеры

Для подобных ресурсов пароль необходимо обновлять чаще

Основные инструменты и сервисы, используемые в работе и личной жизни

- **По работе:**

✓ Электронная служебная почта **(ЕПС ПМ)**
✓ Городской рабочий телефон
✓ Система электронного документооборота
✓ Видеконференцсвязь служебная **(Peregovorka.mos.ru)**
✓ Служебные облачные хранилища документов **(Cloud.dit.mos.ru)**
✓ Курьерская доставка документов
✓ Мессенджеры **(TDM)**

- **В личной жизни:**

✓ Электронная личная почта
✓ Мобильная связь
✓ Городской домашний телефон
✓ Видеконференцсвязь публичная (Яндекс, Мэйл и т.д.)
✓ Коммерческая почта (Почта России, СДЭК и т.д.)
✓ Публичные облачные хранилища документов (Яндекс диск)
✓ Мессенджеры
✓ Заказ такси
✓ Службы доставки
✓ Онлайн-магазины
✓ Онлайн-банкинг

При этом используются личные и служебные аккаунты с одних и тех устройств: смартфон, планшет или ноутбук

Корпоративная этика

ВАЖНО!

- **ЗАПРЕЩЕНО пользоваться личной почтой для ведения рабочей переписки!**
  - ✓ Единая почтовая система Правительства Москвы (ЕПС ПМ) – единственный сервис электронной почты, разрешенный для использования в рабочих целях
- **ЗАПРЕЩЕНО пользоваться рабочей почтой в личных целях!**
  - ✓ Не стоит регистрироваться на сторонних сайтах, интернет-магазинах с помощью рабочей почты

Основные способы распространения фишинга

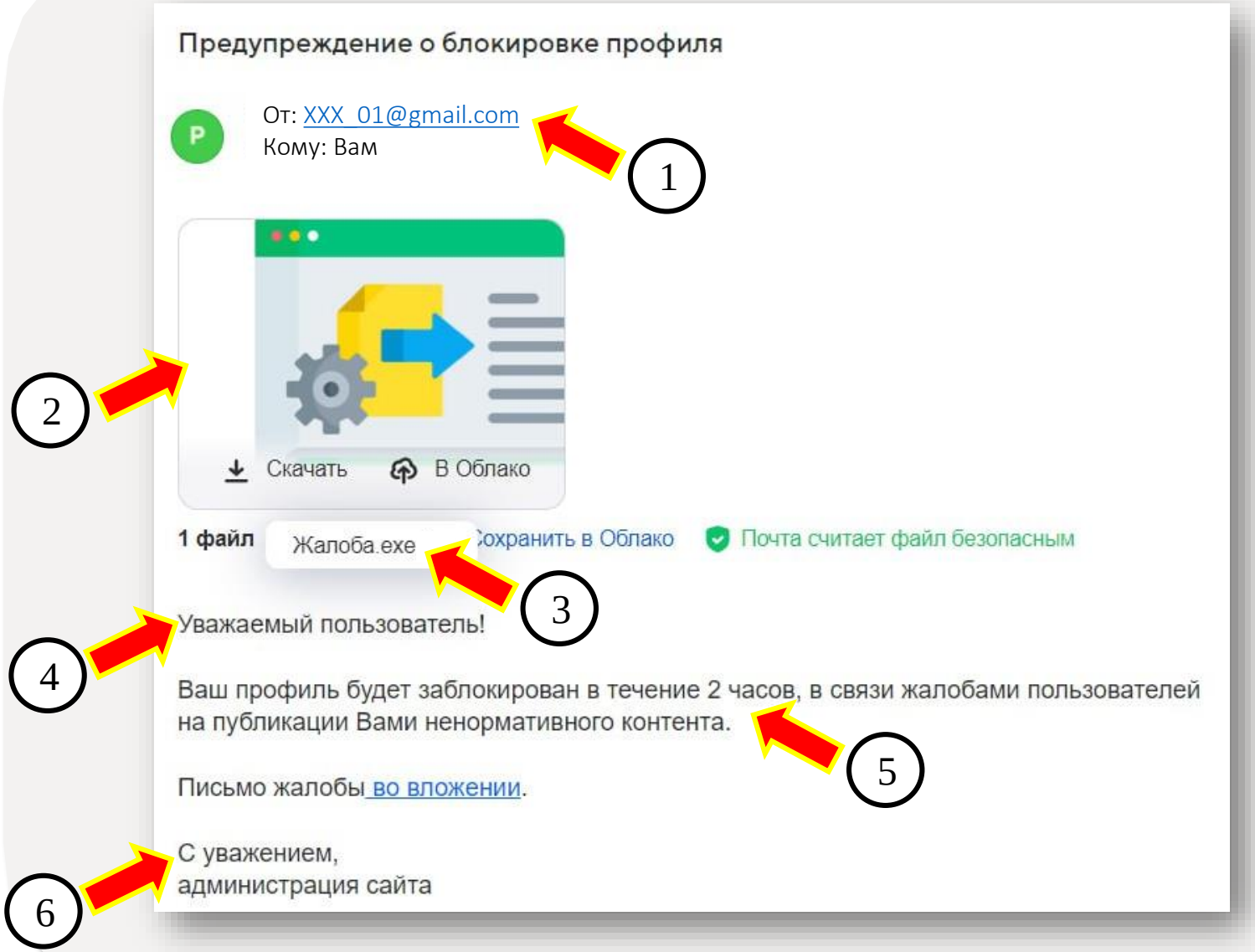
- **Электронная почта**
  - ✓ Электронная служебная почта (ЕПС ПМ)

- **Мессенджеры (Telegram, Whatsapp) и социальные сети**
  - ✓ Личный аккаунт

- **СМС**
  - ✓ Личный номер телефона

- **Почта**
  - ✓ Почтовый адрес

Признаки фишинговых писем



Что должно насторожить в данном примере письма:

1 - странный отправитель,

2 - наличие вложения,

3 - файл в формате .exe, а в письме говорится о текстовом файле,

4 - обезличенное обращение

5 - манипуляции (в примере страх и срочность)

6 - администрация сайта использует официальные бланки организации

Какие приемы используют злоумышленники

- **Обращайте внимание на вид ссылки**

Подмена ссылки	На вид одна, а при наведении курсором на нее – другая: https://www.mos.ru/ Текст ссылки не равен ее URL.
Ссылки-обманки	Используются похожие символы: yanbex.ru, m0s.ru
Странные символы в ссылках	https://bank.ru@yandex.ru
Отсутствие в ссылке «://»	wwwyandex.ru, www-yandex.ru, httpsyandex.ru
Ссылка обычным текстом	Ссылки могут быть замаскированы под изображения, документы и другие активные объекты (кнопки, QR-коды и т.п.), переводящие на фишинговые сайты

Важно!

Не кликайте, если не знаете доменное имя или если адрес ссылки не соответствует тексту ссылки. Даже если текст выглядит как ссылка, он может вести на другой адрес

Как вычислить фишинговое письмо?

❖ **Ответьте для себя на несколько вопросов при получении письма:**

Я ждал это письмо?	Да	Нет
Я знаю отправителя письма?	Да	Нет
Я ждал, что будет ссылка в письме?	Да	Нет
В письме есть манипуляции моими чувствами?	Да	Нет
Я знаю URL-ссылку (адрес куда ведет ссылка)?	Да	Нет
Под текстом ссылки скрывается та же ссылка?	Да	Нет
Письмо с вложенным файлом в формате ZIP/ JS/ EXE /SRC?	Да	Нет
Вложение формата DOC/ DOCX/ XLC просит включить макрокоманды при открытии файла?	Да	Нет

Важно!

Если есть хотя бы один красный флаг не переходите по ссылке и не открывайте вложение в письме. Скорее всего письмо фишинговое

Варианты фишинговых атак

- **Письмо или сообщение от лица руководителя Департамента или руководителя подведомственной организации (поддельный аккаунт) с поручением провести диалог с сотрудником федерального органа власти, курирующим вашу организацию**
  - ✓ Преступник использует реальные фамилию, имя, отчество руководителя и его официальное фото на аватарке
  - ✓ Используется давление на человека через свой авторитет

- **Письмо или сообщение от органа государственной власти с требованием быть на связи и максимально сотрудничать с их специалистом**

- **Письмо или сообщение от коллеги, друга или близкого человека аккаунт которого взломали**
  - ✓ Злоумышленник делает рассылку фишингового сообщения с вредоносной ссылкой или вложением всем контактам из телефонной книги взломанного аккаунта
  - ✓ В сообщении описывается проблема или просьба о помощи, любопытный факт или новость с предложением перейти по ссылке или скачать файл

Пример фишингового электронного письма в ЕПС ПМ

От: Федеральная Налоговая служба <nalog.gov.ru.msc@yandex.ru>
Отправлено: 18 октября 2023 г. 12:47
Кому: DKN_INFO
Тема:

ВНЕШНЯЯ ПОЧТА: Если отправитель почты неизвестен, не переходите по ссылкам, не сообщайте пароль, не запускайте вложения и сообщите коллегам из службы безопасности по адресу DITantifishing@mos.ru

Уважаемый Емельянов Алексей Александрович,

Беспокоит Вас Федеральная налоговая служба с очень важной информацией относительно ситуации, произошедшей в Вашем департаменте культурного наследия города Москвы.

По нашим данным, некоторые сотрудники вашего департамента подали заявки на кредитование в одном и том же банке с разницей во времени в 4 минуты. После проведения проверок, мы обнаружили, что главный бухгалтер Вашего департамента может иметь к этому отношение.

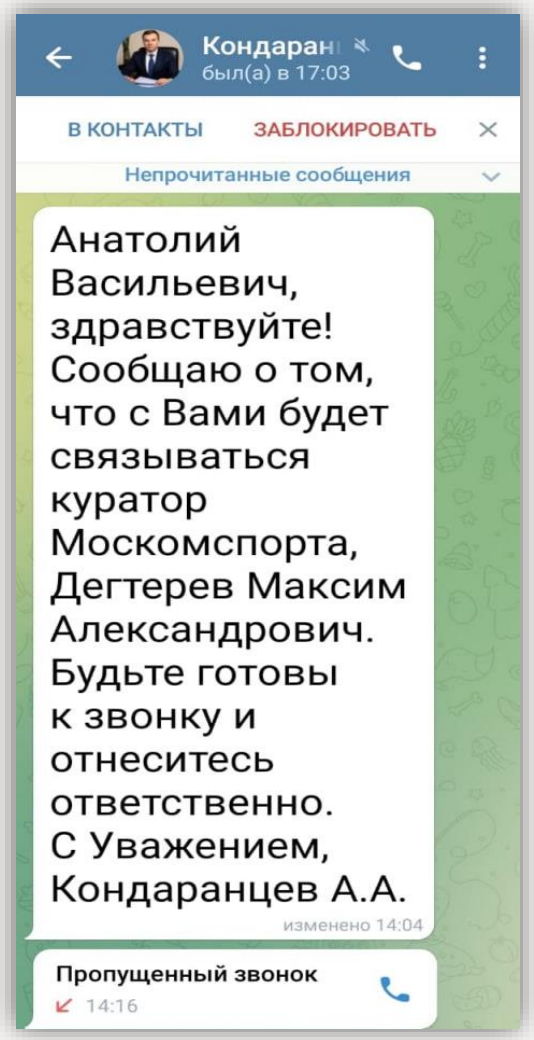
Убедительное требование быть на связи в течение дня, так как с Вами свяжется специалист налоговой службы для выяснения обстоятельств данного инцидента. Важно, чтобы вы предоставили всю необходимую информацию и сотрудничали в ходе разбирательства. Важно отметить, что мы настоятельно рекомендуем Вам не предпринимать самостоятельно никаких мер по решению данного вопроса, так как это может нарушить ход разбирательства.

Мы просим Вас принять эту ситуацию всерьез и сотрудничать с нами в целях разрешения данного инцидента. Мы рассчитываем на ваше понимание и сотрудничество.

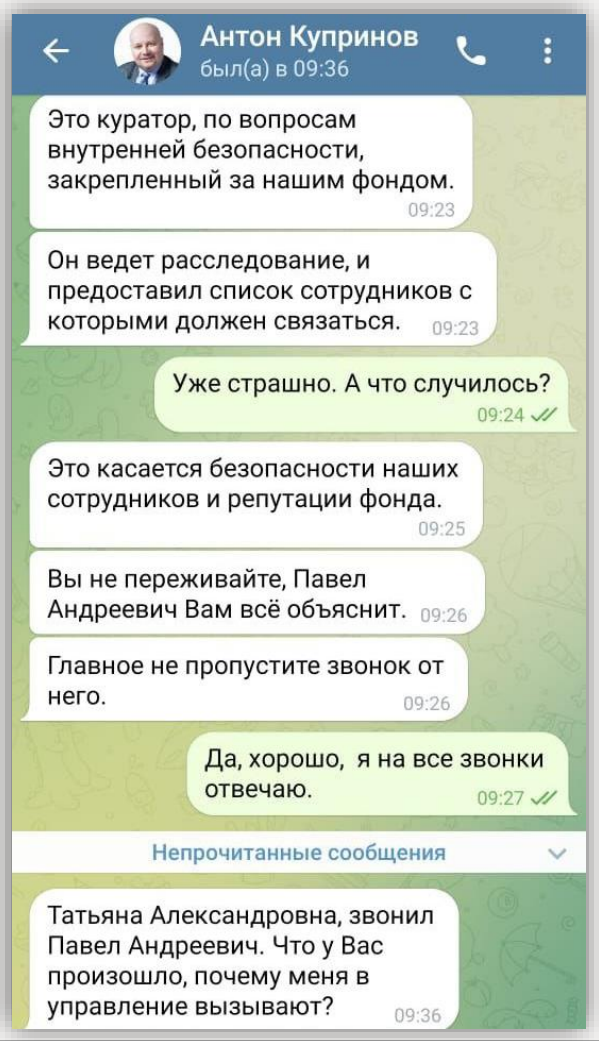
С уважением,
Федеральная налоговая служба.

Пример фишинговых сообщений в мессенджере

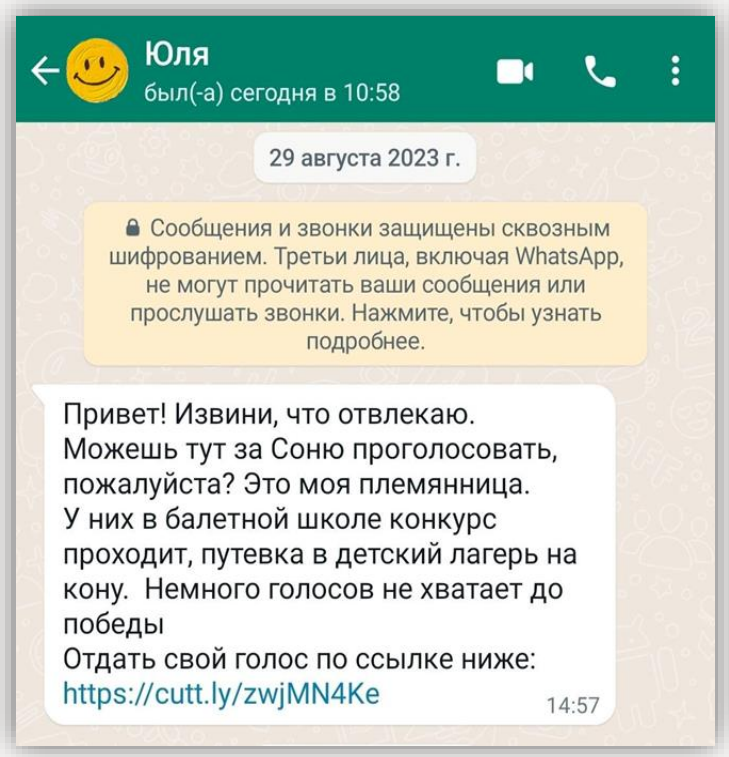
- От лица якобы руководителя Департамента спорта города Москвы Кондаранцева А.А.

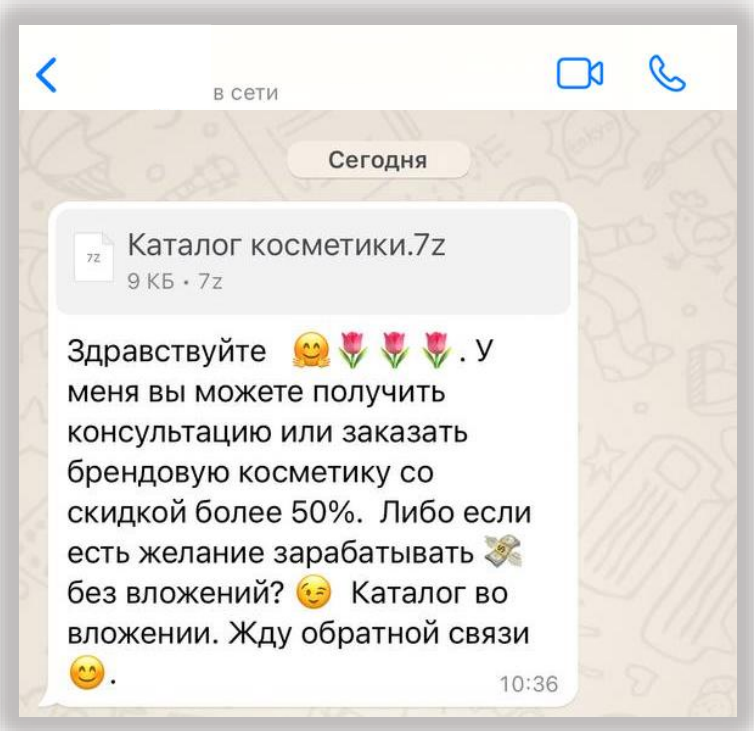


- От лица якобы исполнительного директора Фонда содействия кредитованию малого бизнеса Москвы



Пример фишингового сообщения от взломанного аккаунта коллеги или близкого человека





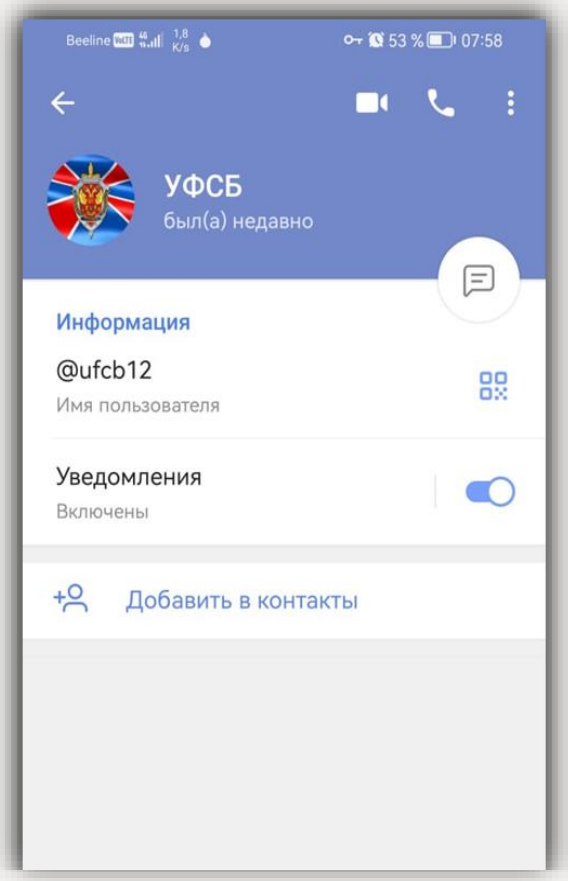
- Переход по ссылке или открытие вредоносного файла ведет к заражению вашего смартфона или любого другого устройства, с которого вы проходите по ссылке или открываете файл
- Мошенник получает контроля над вашим устройством
- Затем схема мошенничества повторяется, теперь уже вашим контактам рассылается фишинговое письмо

Уловки мошенников

- **Злоумышленники пытаются максимально расположить к себе собеседника, склонить его к дальнейшему общению, конечная цель которого является финансовая нажива для этого:**
  - ✓ подменяют номер телефона на официальный (например, при входящем звонке отображается телефон ФСБ России и т.д.)
  - ✓ направляют фото якобы своего служебного удостоверения
  - ✓ используют официальную символику органов государственных власти (например, при входящем звонке отображается геральдический знак – эмблема ФСБ России и т.д.)

- **Направляют от имени органа государственной власти якобы официальные обращения заверенные подписью и печатью руководителя, в которых как пример сообщают:**
  - ✓ о голосовом согласии в сотрудничестве с органами государственной власти
  - ✓ об установлении факта мошеннических действий в отношении данного лица
  - ✓ о необходимости выполнения процедуры обновления единого лицевого счета и т.д.

Уловки мошенников. Примеры



Уловки мошенников. Пример

ФСБ РОССИИ
Управление
Федеральной службы безопасности
Российской Федерации
по Московской области
(УФСБ России по Московской области)
ул.Большая Лубянка,д.2,г.Москва,107031

[redacted]

Согласие на сотрудничество

[redacted] дав голосовое согласие на сотрудничество с Федеральной Службой Безопасности Российской Федерации обязуется не разглашать сведений, составляющих государственную и служебные тайны, точно выполнять относящиеся к ней (нем) требования приказов, положений, инструкций по обеспечению режима секретности проводимых работ.

Об ответственности по закону разглашений сведений, составляющих государственную тайну, утрату документов, содержащие такие сведения, а также об ответсвенности за нарушения установленного режима секретности проводимых работ предупрежден (а).

Инструктаж провел [redacted]

ст. следователь следственного отдела УФСБ

«26» сентября 2023 г. [redacted]

Уловки мошенников. Примеры

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
УПРАВЛЕНИЕ ПО МОСКВЕ И МОСКОВСКОЙ ОБЛАСТИ
Ул.Большая Лубянка, 20 стр.2, г.Москва, 101000

У/Д 429713 /23

ПОСТАНОВЛЕНИЕ

о приобщении отдельного эпизода преступления
к материалам уголовного дела № 429713 /23

г.Москва

Старший следователь по особо-важным делам Управления ФСБ Российской Федерации по г.Москва, майор Калашников В.Н., рассмотрев сообщение о совершении преступления, поступившее от заместителя начальника ОПИО РОО "Москва" Центрального Банка Российской Федерации.

УСТАНОВИЛ:

_____ в отношении гр. _____ обнаружен факт мошенничества, который заключается в попытках хищения денежных средств путем различных манипуляций с основным счетом со стороны злоумышленников.

В процессе телефонного разговора с _____, который отрицает свою причастность к подобного рода операциям, т.е. никаких изъятий, переводов денежных средств, в т.ч. переводов в адрес третьих лиц не проводил, в связи с чем _____, в установленном законом порядке, был проинформирован об ответственности за нарушения ст. 310 УК РФ и предоставил под запись диалога голосовое соглашение[1] на сотрудничество с органами ФСБ России и Центральным банков Российской Федерации, таким образом обязуясь сотрудничать с вышеупомянутыми структурами в рамках предотвращения действий по основному счету.

В связи с вышеупомянутым деяния совершенные по отношению к гр. _____, являются неправомерными и попадают под ч.3 ст. 159 УК РФ. Учитывая характерные признаки совершенного преступления в отношении _____ следует сделать вывод, что эти деяния попадают под уголовное дело № 429713 /23 от 26.09.2023 г., которое находится в сопровождении УФСБ РФ по г.Москве.

Принимая во внимание, что имеются достаточные данные, указывающие на признаки преступления, предусмотренного ч.3 ст.159 УК РФ, руководствуясь ст. 140, 145, ч.2 ст.156 УПК РФ.

ПОСТАНОВИЛ:

1. Приобщить эпизод преступления в отношении гр. _____ к уголовному делу № 429713 /23, и приступить к его расследованию.
2. Копию настоящего постановления направить первому заместителю Генерального прокурора Российской Федерации.

Старший следователь по ОВД
УФСБ по г. Москве Калашников В.Н.

Копия настоящего постановления направлена первому заместителю Генерального прокурора Российской Федерации.
Старший следователь по ОВД
УФСБ по г. Москве Калашников В.Н.

_____

[1] К документу прилагается запись голосового согласия, далее именуется "запись № 3 от 26.09.2023 г."

Банк России ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: d107312a3a9a80b8543c329adbbf9abb
Владелец: А. С. Набережный
Действителен с 07.10.2022 по 06.03.2024

Банк России
Центральный банк Российской Федерации

Исх. № 53517742 г. Москва

Документ № 53517742

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы, _____, стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого лицевого счета.
Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Переоформление кредитной заявки.
Если в системе банков отображается активная заявка на кредит - её необходимо отклонить, путем подачи новой заявки. Финансы для проведения операции по отклонению кредитной заявки предоставляются из резервного фонда ЦБ РФ (согласно ФЗ "О противодействии отмывания доходов, полученных преступным путем, и финансированию терроризма", в целях совершенствования контроля). Данная заявка не будет отображаться в кредитной истории и не влияет на кредитный рейтинг в дальнейшем.

II этап:
- Погашение кредиторй задолженности.
Выполняется методом внесения финансовых активов, предоставленных вам из резервных фондов ЦБ РФ. Внесение выполняется зашифрованным методом (с помощью АТМ устройства, рассчетно-кассового центра страхового банка партнера), предоставленным отделом финансового мониторинга.

III этап:
После выполнения всех регламентных работ, представителем ЦБ РФ будет назначено время и адрес отделения банка в которое клиенту необходимо явиться для: актуализации паспортных данных, перевыпуска пластиковых носителей, подписания и получения документации.

Уведомляем Вас
- о наступлении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (Согласно ст. 183 УК РФ (соблюдение политики конфиденциальности, коммерческой, налоговой и банковской тайны)).
- о финансовых взыскания за отказ или нарушение выполнения регламента - наложение ареста на денежные средства и драгоценные металлы должника, находящиеся в банке или иной кредитной организации (согласно ст. 81 УК РФ) и взыскании денежных средств, выделенных Банком для выполнения регламентных действий (выпуск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

Срок обновления реквизитов с момента выполненных работ, составляет 2 часа.
Специалист Банка России: Беляев Роман Алексеевич.
Финансово-ответственное лицо: Ожидает закрытие кредитного договора.

Зам. Начальника ОПИО РОО "Москва" филиала №3 ЦБ РФ
М.П.

А. С. Набережный

Что делать, если вы получили письмо от лица руководителя Департамента или вашей организации?

ВАЖНО:

- ✓ **Прекратите какое-либо общение с мошенником. Вас могут начать пугать фотографиями служебных удостоверений, официальных документов и тому подобным. Не поддавайтесь давлению!**
- ✓ **Расскажите своему непосредственному руководителю о факте обращения от лица руководителя Департамента или вашей организации**
- ✓ **Дождитесь от непосредственного руководителя подтверждения достоверности обращения от руководителя Департамента или организации**
- ✓ **В случае, если это всё-таки были мошенники, напишите об инциденте на почту: DITsecurity@mos.ru**

Безопасность аккаунта на Госуслугах

- С 01 октября 2023 года двухфакторная аутентификация на Госуслугах стала обязательной для новых пользователей портала и для тех, кто восстанавливает учётную запись, в скором времени эта мера защиты аккаунта станет обязательной для всех.

Сценарий обмана на Госуслугах

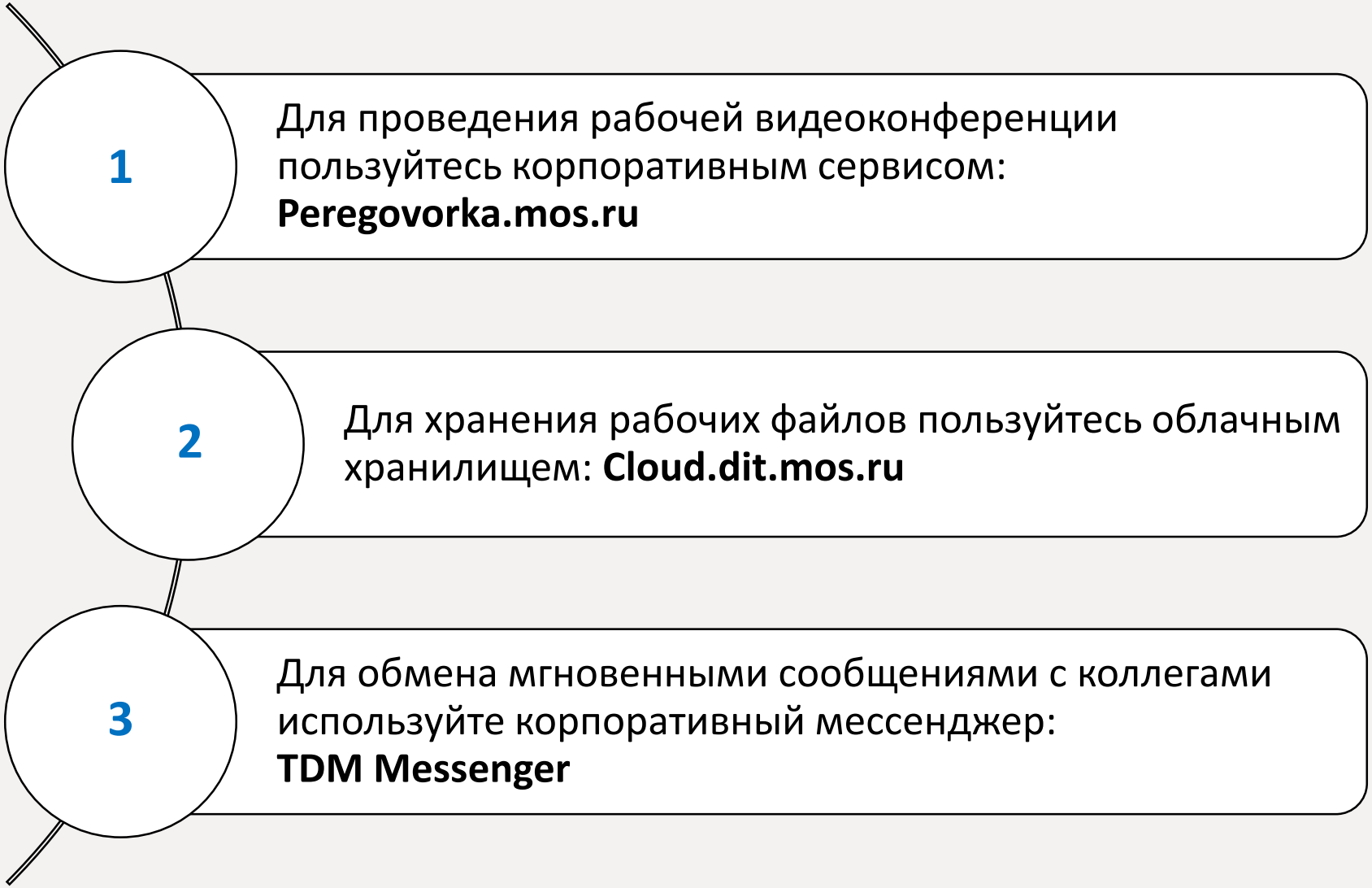
1. Звонок от имени оператора сотовой связи. Предлог: улучшение качества сотовой связи, продление действия абонентского контракта
2. На ваш телефон приходит код для изменения пароля от личного кабинета Госуслуг
3. Мошенник осуществляет смену пароля от вашего аккаунта на Госуслугах и привязывает к нему новый номер телефона

Важно!

Не передавайте и не сообщайте одноразовые пароли (коды) из СМС — их запрашивают только мошенники.

Если ваш аккаунт на Госуслугах взломали, то действуйте по следующему алгоритму – https://www.gosuslugi.ru/help/faq/login/101487

Корпоративные инструменты взаимодействия



QR-код

QR-коды позволяют:

- оплачивать покупки в магазинах,
- курьерскую доставку,
- услуги ЖКХ,
- оставлять чаевые,
- обмениваться контактами в мессенджерах и соцсетях,
- быстро переходить на интересующий ресурс,
- участвовать в онлайн-опросах;
- передавать ссылки, файлы, картинки, текст и т.д.

Важно!

Злоумышленники часто заменяют реальные QR-коды фишинговыми (поддельными) и опасность заключаются в том, что QR-коды могут содержать абсолютно любую ссылку

Безопасность при работе с QR-кодом

Что делать, чтобы избежать проблем?

- Подумайте, прежде чем сканировать QR-код.
- Оцените его расположение.
- Перед сканированием убедитесь, что QR-код не наклеен поверх другого.
- Уточните достоверность QR-кода (например у владельца или сотрудника заведения).
- Воспользуйтесь приложением (антивирусный сканер) для смартфона, которое позволяет проверять сайты на вредоносное содержимое.
- Изучите URL-адрес QR-кода:
  - ✓ URL-адрес должен иметь «HTTPS» расширение в начале адреса
  - ✓ Доменное имя должно соответствовать бренду или названию компании

Примеры QR-кодов

Реальный QR-код

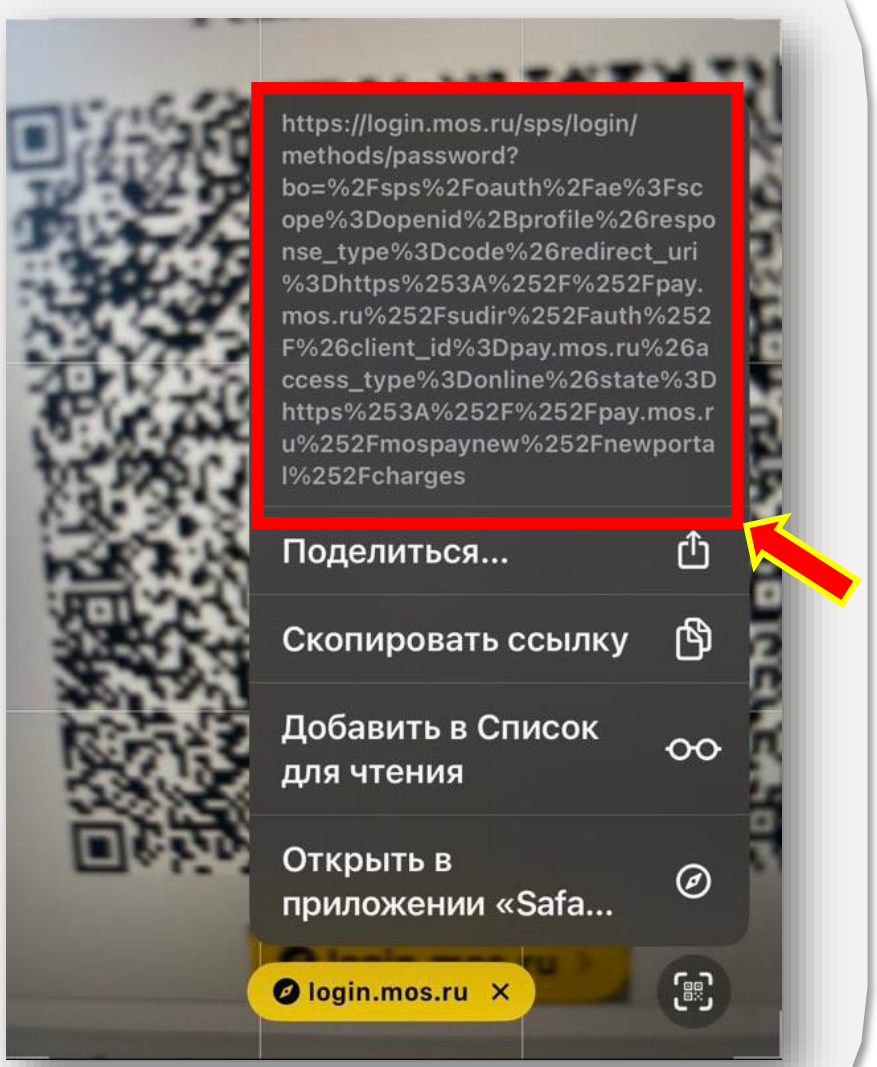
login.mos.ru

QR-код ведет на сайт-двойник

login.m0s.ru

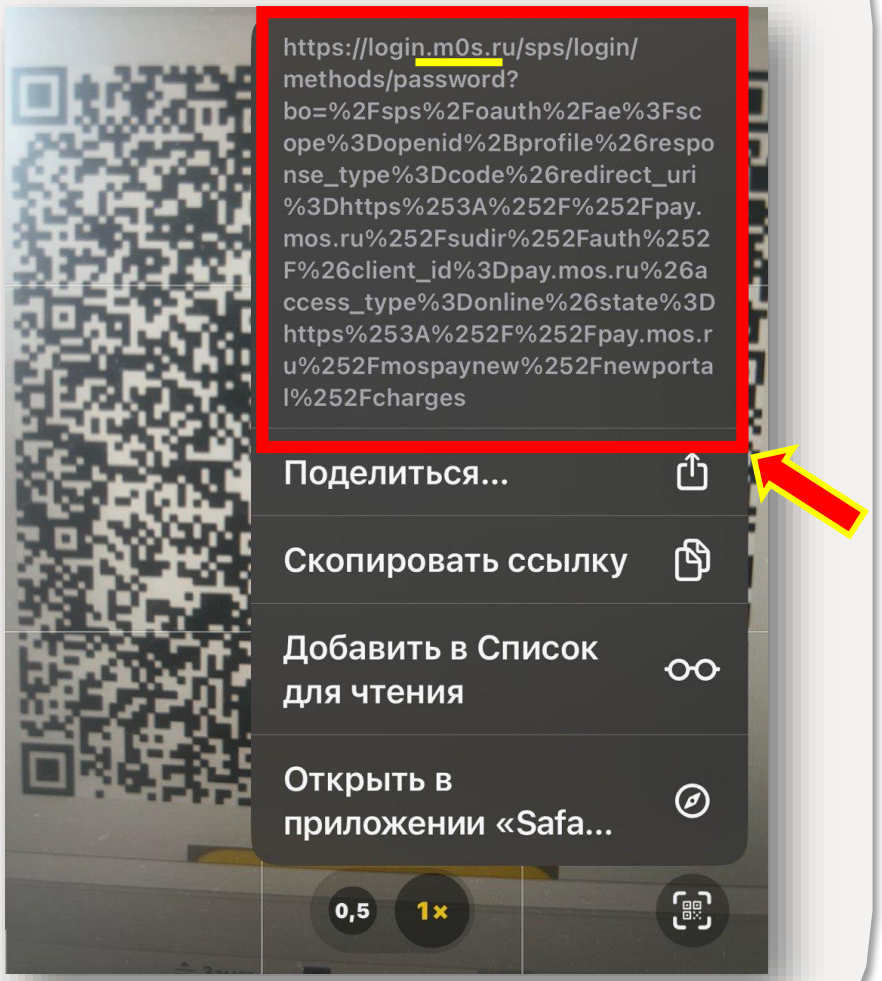
Пример сканирования реального QR-кода

- При сканировании QR-кода на смартфоне (на рисунке iOS) в правом нижнем углу появляется значок  , если на него нажать, то появится окно, на котором будет указан URL-адрес: https://login.mos.ru/sps/login/methods/password..., необходимо **внимательно изучить ссылку**, прежде чем переходить на этот сайт



Пример сканирования QR-кода, который ведет на сайт-двойник

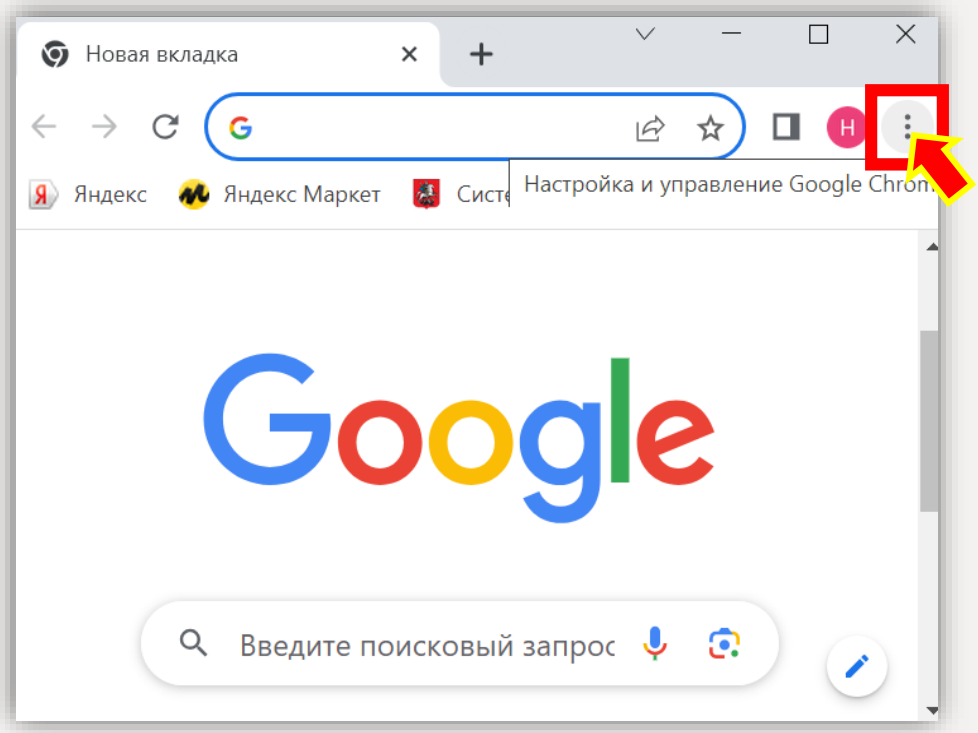
- При сканировании QR-кода на смартфоне (на рисунке iOS) в правом нижнем углу появляется значок  , если на него нажать, то появится окно, на котором будет указан URL-адрес: https://login.m0s.ru/sps/login/methods/password..., необходимо **внимательно изучить ссылку**, прежде чем переходить на этот сайт



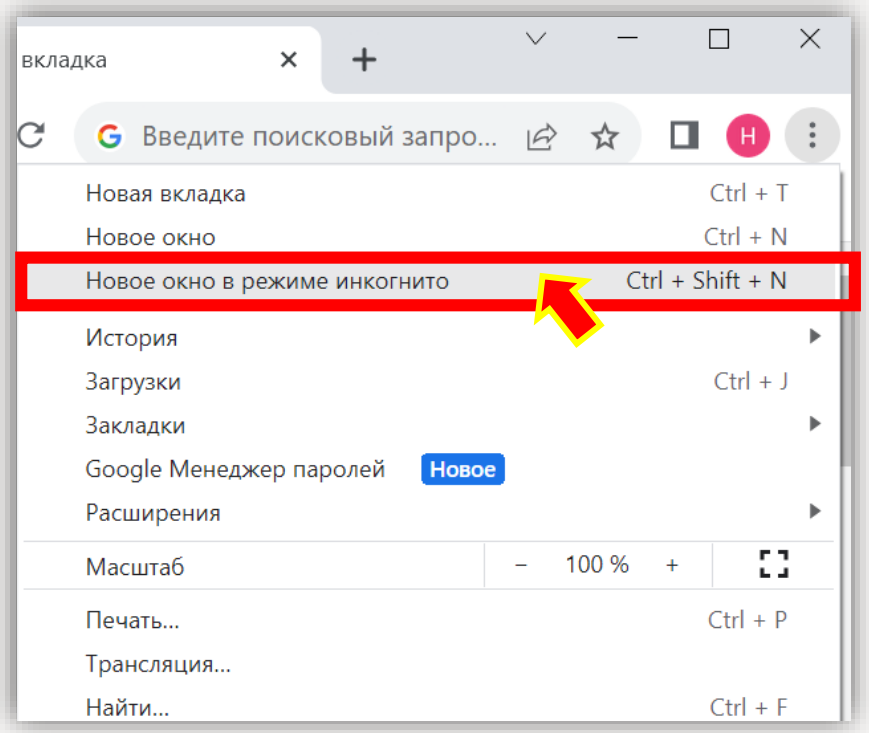
Работайте в браузере «под прикрытием»

- **Включите режим «Инкогнито»**
  - ✓ Файлы cookie и данные сайтов не сохраняются

1 шаг – в браузере Google Chrome нажмите на кнопку с тремя точками



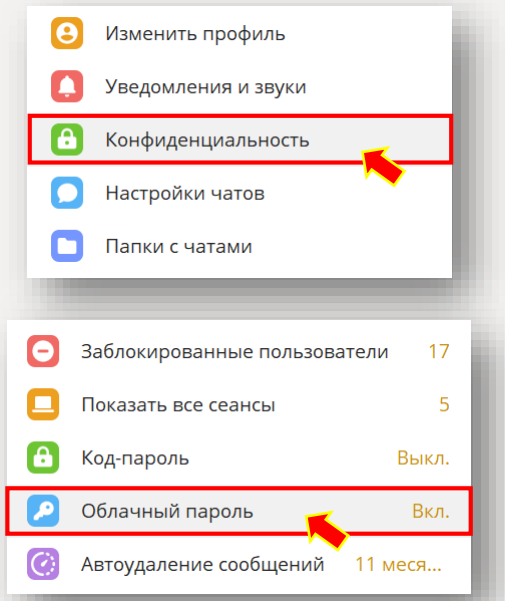
2 шаг – нажмите окно в режиме инкогнито



Настройка двухфакторной аутентификации в Telegram

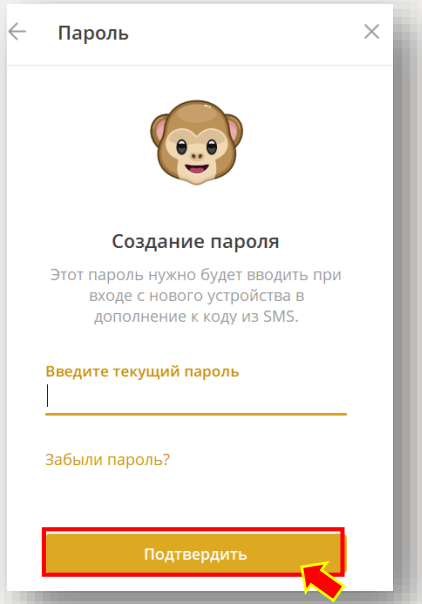
Перейти в «Настройки», выберите раздел «Конфиденциальность» и там кликните на пункт «Облачный пароль»

1



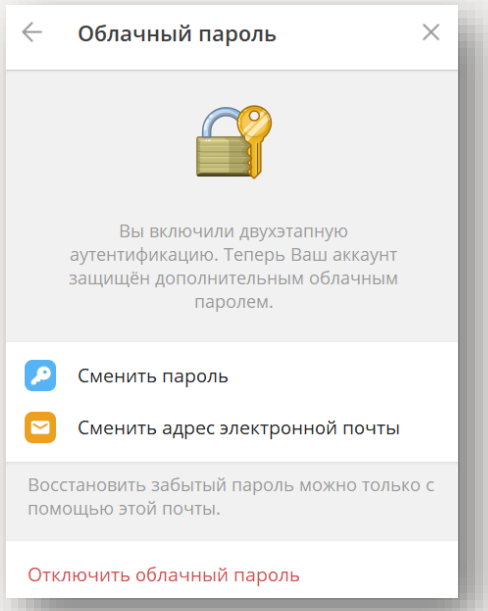
Придумайте пароль и нажмите «Подтвердить»

2



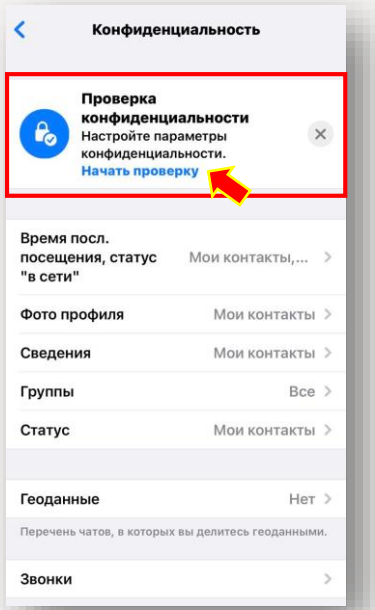
Двухэтапная аутентификация включена

3

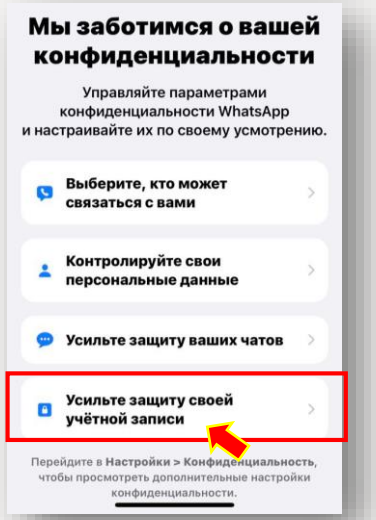


Настройка двухфакторной аутентификации в WhatsApp

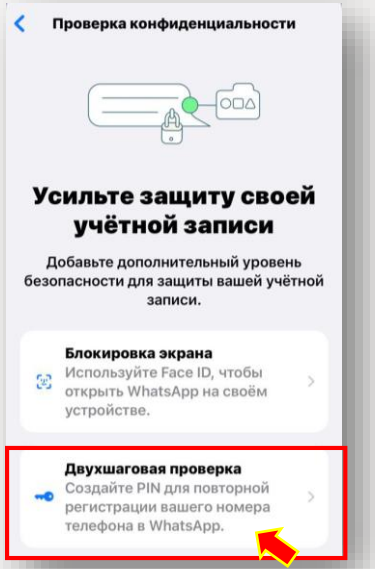
1. Перейти в «Настройки», выберите раздел «Конфиденциальность» и там кликните на пункт «Начать проверку»



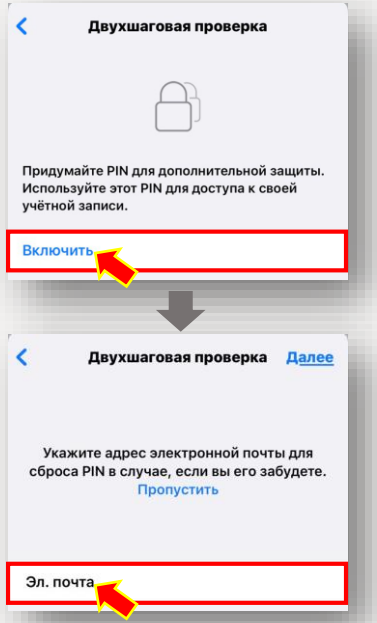
2. Перейти в раздел «Усильте защиту своей учётной записи»



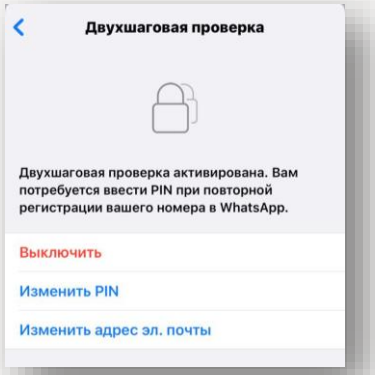
3. Выберите раздел «Двухшаговая проверка»



4. Введите PIN-код и укажите адрес электронной почты



5. Двушаговая проверка активирована



Подведем итоги

- ✓ Используйте надежные, уникальные для каждого ресурса пароли и обновляйте их не реже, чем раз в квартал
- ✓ Не смешивайте личное и рабочее – для работы используются только корпоративные сервисы
- ✓ Не поддавайтесь на манипуляции в переписке или общении. Главная задача мошенников вывести вас на эмоции
- ✓ Не спешите переходить по ссылкам и скачивать вложения из писем и сообщений
- ✓ Настройте двухфакторную аутентификацию для различных ресурсов