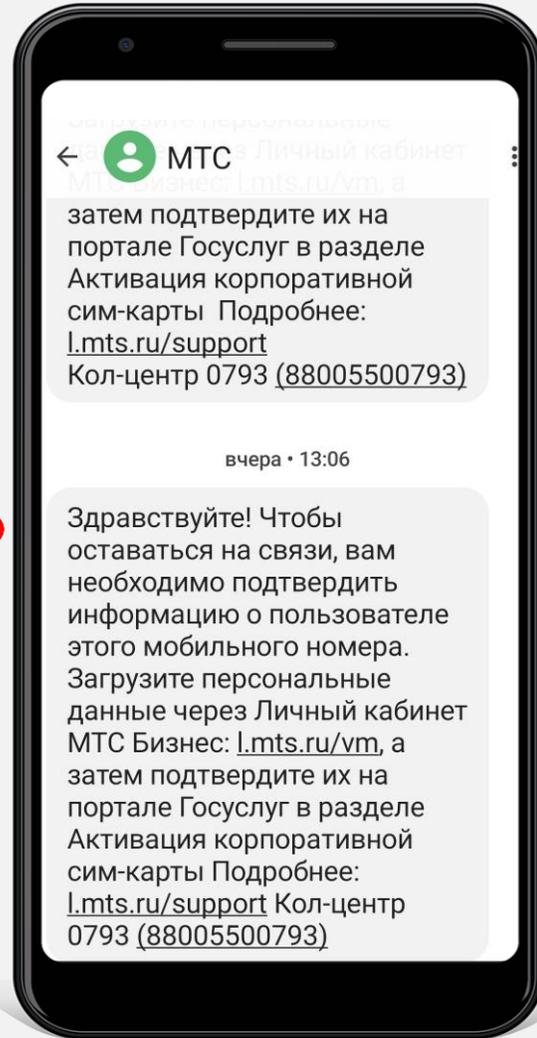
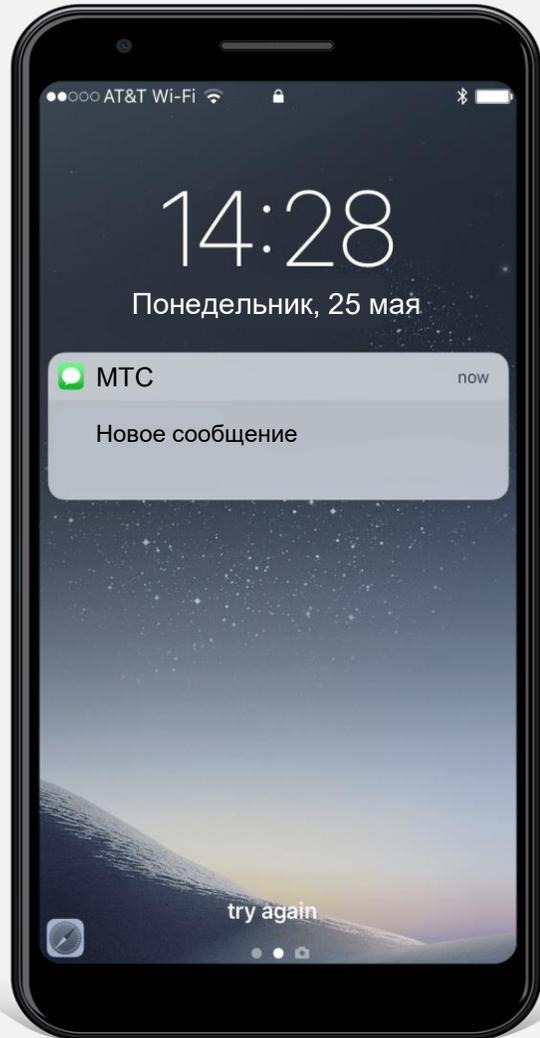


# Фишинг от имени оператора связи для взлома «Госуслуг»



Злоумышленники от имени оператора связи (под предлогом продления мобильного номера) совершают звонки, направляют электронные письма или push-уведомления.



Они просят подтвердить паспортные данные, для этого:

- Направляют фишинговую ссылку, с которой вы переходите на фиктивную страницу Госуслуг;
- Направляют код и просят его назвать или вписать.



Перейдя по ссылке или сообщив код, вы теряете доступ к личному кабинету Госуслуг

# Мошенники взломали личный кабинет на сайте «Госуслуг».

## Что делать?



Стандартная/ упрощенная учетная запись  
– онлайн

**Онлайн на Госуслугах —  
если есть доступ к телефону и почте  
из личного кабинета**  
(мошенники НЕ поменяли почту и пароль  
в вашем личном кабинете)

1. На [странице ввода логина и пароля](#) нажмите «Восстановить»
2. Укажите номер телефона или электронную почту, а также данные одного из документов:
  - паспорт
  - ИНН
  - СНИЛС
3. Ответьте на контрольный вопрос, если он был установлен
4. Перейдите по ссылке из письма в электронной почте или введите код из смс.
5. Придумайте новый пароль и нажмите «Сохранить».

Стандартная/ упрощенная учетная запись  
– онлайн

**Онлайн через банк —  
если нет доступа к телефону и почте из  
личного кабинета**  
(мошенники поменяли почту и пароль в  
вашем личном кабинете)

1. Посмотрите [список банков](#), в которых можно онлайн восстановить доступ к portalу.
2. Если вы являетесь клиентом одного из них, зайдите в свой личный кабинет на сайте или в приложении, найдите сервис «Регистрация на «Госуслугах» и следуйте инструкциям.
3. Новый пароль от аккаунта придет на номер телефона, который вы указали в банке как основной.
4. Даже если мошенники успели заменить его в «Госуслугах» на свой, код для входа получите именно вы.

Подтвержденная учетная запись  
– офлайн

**Лично в центре обслуживания —  
если нет доступа к телефону и почте  
из личного кабинета**  
(мошенники поменяли или установили  
контрольный вопрос и иные данные)

1. Выберите удобный [центр обслуживания](#). Нажмите на фильтр (значок, похожий на воронку), выберите «Восстановление доступа».
2. Возьмите с собой паспорт и СНИЛС
3. Предъявите документы и попросите оператора восстановить пароль от Госуслуг
4. Проверьте, какой номер телефона привязан к профилю. Если указан не ваш, сразу замените его.
5. При первом входе на Госуслуги с новым паролем укажите в качестве логина СНИЛС
6. Смените полученный пароль.

# Как обеспечить безопасность личного кабинета после его восстановления?



1

## В разделе «Настройка учетной записи»

- Проверьте телефон и почту, если там указаны неизвестные номер или адрес, сделайте скриншот — эти данные помогут в поиске преступников
- Поменяйте телефон и электронную почту

2

## В разделе «Безопасность» настройте

- Вход с подтверждением по смс в дополнение к паролю
- Оповещение на электронную почту после входа
- Восстановление доступа контрольным вопросом

3

## В разделе «Безопасность» в подразделе «Действия в системе»

- Проверьте, не было ли подозрительных действий в учётной записи
- При необходимости обратитесь [в службу поддержки](#)
- При необходимости сделайте фото или скриншот — возможно, эта информация вам пригодится

4

## В разделе «Согласия и доверенности» в подразделе «Разрешения»

- Отзовите разрешения, которые вы не выдавали
- Узнаете, какие ведомства запрашивали вашу личную информацию
- При необходимости сделайте фото или скриншот — возможно, эта информация вам пригодится

5

## Проверьте информацию о ранее поданных заявлениях

- Перейдите в личный кабинет в Уведомления → Заявления
- Это поможет выявить, какие действия хотели совершить или совершили мошенники от вашего имени

6

## Подайте заявление в МВД России

- Обратитесь в подразделение [МВД России](#)
- Расскажите о взломе и приведите всю информацию, которую знаете

# Дополнительные меры безопасности



Используйте уникальный логин и пароль, которые не встречаются на других сайтах

Никому не сообщайте ответ на контрольный вопрос и коды из смс, в том числе приходящие от отправителя gosuslugi и с номера 0919

Внимательно проверяйте адрес сайта <https://www.gosuslugi.ru>. Проверяйте, чтобы в адресной строке не было похожих написаний вроде gossuslugi, gos.uslugi, gosucslugi и т.д.

Не переходите по подозрительным ссылкам. Ссылки от Госуслуг обычно ведут в личный кабинет, на конкретную услугу и сайты ведомств

Не открывайте присланные файлы, если не уверены в отправителе. Письма от Госуслуг приходят с адресов [no-reply@gosuslugi.ru](mailto:no-reply@gosuslugi.ru) или [no-reply@pos.gosuslugi.ru](mailto:no-reply@pos.gosuslugi.ru)

Устанавливайте официальные приложения. Приложение «Госуслуги» можно скачать [в RuStore](#), [Google Play](#), [App Store](#) и [AppGallery](#)