

как защитить себя
и близких от **киберугроз?**

❤️ 627480

👤 25098

киберЗОЖ

Жизнь в цифровом мире дает нам новые широкие возможности, но и таит серьезные опасности

Несоблюдение элементарных правил может привести к краже ваших данных и финансов. Безопасность в сети зависит не только от компаний и государства, но и от вас.

👏 87483

🧐 24699

91%



россиян сталкивались
с попытками мошенничества

123456

самый популярный пароль
среди пользователей Рунета

<2 сек

требуется для взлома
любого пароля до 6 символов

59%

пользователей используют один
и тот же пароль для всех аккаунтов

от 80% угроз

защищает соблюдение простых
правил кибербезопасности

🔥 16881

🧐 25672

правил кибербезопасности

Правила кибергигиены

создавайте надежные пароли

Надежные пароли не обязательно сложные для запоминания

Легко запомнить фразу, связанную с жизненной ситуацией, и превратить ее в надежный пароль

Hotel_psa_s_10let!

Тайное желание и надежный пароль

Еще!

Bassein_ne!dly!svidani2008

Худшее свидание и надежный пароль

Еще!

Что делает пароль надежным?

Длина пароля 10 или более
символов



>10

Использование верхнего
и нижнего регистра, чисел
и символов



Aa3!

Использование случайных
комбинаций



rndm

Отсутствие простых комбинаций
букв и чисел



qwe123

Отсутствие публичной
информации



1985г.р.

Совет

Не используйте одинаковые пароли для важных ресурсов: соцсети,
почта, государственные сайты, интернет-банк.

придумайте пароль самостоятельно. не используйте общедоступную
информация о себе.

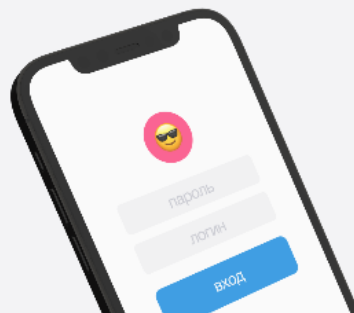


подключите двухфакторную аутентификацию

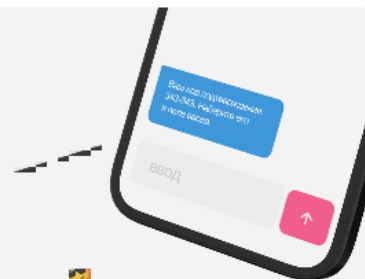
Двухфакторная аутентификация — это очень надёжный способ защиты «в два этапа».

1 этап

Стандартные логин и пароль



2 этап



Код, который приходит пользователю в смс, push-уведомлении или почте.



В настройках телефона можно установить дополнительную защиту в виде пароля или биометрических данных: отпечатка пальца или сканирования лица.

Как определить фишинговое письмо?

Оцените содержание

Проверьте автора письма

Наведите курсор на ссылку в сообщении

Оцените вложенный файл

Где использовать?

На всех ресурсах, где содержатся важные данные или совершаются финансовые операции: при входе в аккаунты социальных сетей, порталы государственных услуг, интернет-банкинг и прочие.

Совет

Если на ваш телефон пришло сообщение с одноразовым кодом, но при этом вы не выполняли попыток входа, значит, вас пытаются взломать и ваш пароль уже подобрали. В этом случае нужно немедленно сменить пароль к учетной записи.

Будьте внимательны к письмам со ссылками и файлами

Фишинг — вид кибермошенничества, цель которого — получить данные пользователя.

За год количество фишинговых атак в России выросло вдвое. 96% фишинговых атак осуществляется через электронную почту.



Будьте внимательны к именам сайтов или отправителям писем

Как определять
фишинговый сайт?

Количество выявленных фишинговых сайтов только
по банковской тематике в июне 2022 года увеличилось
в 2,5 раза в сравнении с 2021 годом.

gosuslugi.ru



Внимательно проверьте, что адрес сайта написан верно —
мошенники могут заменить всего одну букву.

bankzlo.org



Обратите внимание, что домен указан верно — иногда фишинговые
сайты размещают в домене .su, .org и прочих вместо .ru, тогда как сам
адрес до точки остается тем же.

bank@mail.ru

Иногда письма присылают с адреса типа bank@mail.ru. Помните, что
организации не присылают письма с адресов общедоступных
почтовых сервисов: @mail.ru, @gmail.com и прочие.

Совет

Лучше ввести адрес сайта вручную и найти
интересующий вас раздел с акцией или другой
информацией.



проверить сайт на безопасность

www.123.ru

Проверить

не скачивайте файлы из непроверенных источников

Под видом бесплатных программ (особенно, дорогих) мошенники могут замаскировать зловредное ПО. Задачами такого ПО могут быть: кража ваших данных (логинов, паролей, фото, контактов), перехват любой вводимой на устройстве информации, подписка на платные услуги, сбор информации в рекламных целях.

В 2021 году в Google Play Store заблокировали 1,2 млн вредоносных приложений. На сторонних ресурсах Apple и Google модерацию не проводят, поэтому опасность скачать вредоносное приложение вырастает в разы.

Совет

Скачивайте программы только из официальных источников: маркетов или официальных сайтов организаций.



минимизируйте использование открытого Wi-Fi

Если вы не знаете, кому принадлежит открытая сеть, не нужно вводить свои данные для регистрации. Особенно, если вам предлагают зарегистрироваться через аккаунт социальных сетей, Госуслуг и пр. - после регистрации вы можете потерять к ним доступ. И еще пара советов:



Кибермошенники могут создать поддельную сеть и через нее получить доступ к вашим данным. Чаще всего название сети будет максимально похоже на настоящее, например, Moscow-Free. В кафе или отеле в случае сомнений в названии сети Wi-Fi всегда уточняйте его у сотрудников заведения.



Используйте VPN-сервисы при подключении к публичным сетям: так весь трафик будет передаваться в зашифрованном виде и мошенники не смогут получить к ним доступ.

Больше информации об основных
правилах личной информационной
безопасности:



Кибрарий.
Сбер.



Кибербезопасность —
это просто на ГосУслугах