

Как защититься от мошенников: простые правила

Распространенный способ действий мошенников: они обманным путем получают данные для доступа к личным кабинетам и приложениям. Используя нейротехнологии, способны подделывать аккаунты и голоса, создавая видеосообщения, сгенерированные искусственным интеллектом, от имени ваших знакомых и руководителей. Зачастую мошенники представляются сотрудниками различных служб или предлагают финансовые выигрыши. Данный подход известен как социальная инженерия. Вот несколько советов, которые помогут вам защититься от мошенников:

- Будьте бдительны: Если разговор кажется подозрительным, завершите его и перезвоните в организацию по официальным номерам.
- Проверяйте способ связи: Мошенники часто используют мессенджеры, тогда как настоящие представители не звонят через WhatsApp или Telegram.
- Не сообщайте логины и пароли: Читайте назначение смс-кодов и не делитесь ответами на контрольные вопросы.
- Следите за актуальностью номера: Убедитесь, что номер, к которому привязан аккаунт, актуален.
- Используйте сложные пароли: Меняйте их регулярно и подключайте двухфакторную аутентификацию.
- Проверяйте адрес страницы: Убедитесь, что сайт — это официальный ресурс (например, gosuslugi.ru).

Госуслуги обеспечивают защиту, но злоумышленник может получить доступ только при передаче вами необходимых данных. Будьте внимательны и защищайте свои данные.

С дополнительной информацией по теме личной информационной безопасности, в том числе по эффективному распознаванию звонков мошенников, можно ознакомиться на следующих информационных ресурсах:

Раздел «Кибербезопасность – это просто!» на Едином портале государственных услуг – <https://www.gosuslugi.ru/cybersecurity>;
Лендинговая страница в сети «Интернет» – <https://киберзож.рф/>;

Хотим напомнить вам о правилах кибербезопасности, которые помогут защитить наши данные от угроз. Пожалуйста, будьте бдительны при работе с электронной почтой. Вот простые рекомендации по предотвращению угроз безопасности информации:

1. Проверяйте адреса электронной почты отправителя, даже если имя совпадает с известным контактом.
2. Не открывайте письма и чаты от неизвестных отправителей.
3. Осторожно относитесь к письмам с призывами к действиям или темами о финансах и угрозах.
4. Не переходите по ссылкам в письмах, особенно если они короткие или используют сокращения.
5. Не открывайте вложения с подозрительными расширениями (.zip, .js, .exe и т. д.) и документами с макросами.
6. Не подключайте неизвестные внешние носители информации к компьютерам.
7. Используйте надежные пароли, создавая их с нестандартными комбинациями символов.

При получении подозрительных писем обратите внимание:

- Знаком ли вам отправитель?
- Присутствуют ли URL-ссылки?
- Есть ли вложение с расширениями .zip, .js, .exe?
- Просит ли файл включить поддержку макросов?

Если есть сомнения и хоть что-то в письме вызывает у вас подозрение, то велика вероятность, что это фишинг.

С дополнительной информацией по теме личной информационной безопасности, в том числе по эффективному распознаванию фишинговых писем, можно ознакомиться на следующих информационных ресурсах:

Раздел «Кибербезопасность – это просто!» на Едином портале государственных услуг – <https://www.gosuslugi.ru/cybersecurity>;
Лендинговая страница в сети «Интернет» – <https://киберзож.рф/>;

Рекомендации по защите учетных записей

Для того, чтобы защитить свой аккаунт соблюдайте следующие рекомендации:

1 Создавайте сложные пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных символов. Избегайте простых и легко угадываемых паролей.

2 Не используйте один и тот же пароль для разных учетных записей. Создавайте уникальные пароли для каждой важной учетной записи.

3 Регулярно меняйте пароли каждые 3-6 месяцев и обновляйте их при подозрении на утечку.

4 Используйте надежные менеджеры паролей для их хранения и управления.

5 Активируйте двухфакторную аутентификацию (2FA) на всех доступных платформах.

6 Обновляйте пароли при смене сотрудников или их ролей и следите за управлением доступом.

7 При хранении пароля на физическом носителе, убедитесь, что место его хранения абсолютно безопасно.

С дополнительной информацией по теме личной информационной безопасности, в том числе по созданию надежных паролей и эффективному распознаванию фишинга в интернете, можно ознакомиться на следующих информационных ресурсах:

Раздел «Кибербезопасность – это просто!» на Едином портале государственных услуг – <https://www.gosuslugi.ru/cybersecurity>;

Лендинговая страница в сети «Интернет» – <https://киберзож.рф/>;



ГОСУДАРСТВЕННЫЙ КОМИТЕТ РЕСПУБЛИКИ БАШКОРТОСТАН ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ

ОБ ОБЕСПЕЧЕНИИ ОТДЕЛЬНЫХ КАТЕГОРИЙ ГРАЖДАН АВТОНОМНЫМИ ПОЖАРНЫМИ ИЗВЕЩАТЕЛЯМИ

СЕМЬИ,
НАХОДЯЩИЕСЯ
В СОЦИАЛЬНО-
ОПАСНОМ
ПОЛОЖЕНИИ

СЕМЬИ, ПРИ
РОЖДЕНИИ
РЕБЕНКА
С 1 ЯНВАРЯ
2018 ГОДА

ВETERАНЫ
ВЕЛИКОЙ
ОТЕЧЕСТВЕННОЙ
ВОЙНЫ

ЧЛЕНЫ СЕМЬИ
ПОГИБШЕГО
ИНВАЛИДА ВОЙНЫ
УЧАСТНИКА
ВОВ

ВETERАНЫ
БОЕВЫХ
ДЕЙСТВИЙ

ДЕТИ ВОЙНЫ

ГРАЖДАНЕ
ПЕНСИОННОГО
ВОЗРАСТА,
ПОСТОЯННО
ПРОЖИВАЮЩИЕ В
ИНДИВИДУАЛЬНЫХ
ЖИЛЫХ ДОМАХ

МАЛОИМУЩИЕ
МНОГОДЕТНЫЕ
СЕМЬИ

СЕМЬИ С ДЕТЬМИ
В ВОЗРАСТЕ
ДО 7 ЛЕТ,
РОДИВШИМИСЯ
ДО 1 ЯНВАРЯ
2018 ГОДА

ИНВАЛИДЫ
ВЕЛИКОЙ
ОТЕЧЕСТВЕННОЙ
ВОЙНЫ

БЫВШИЕ
НЕСОВЕРШЕННОЛЕТНИЕ
УЗНИКИ КОНЦЛАГЕРЕЙ,
ГЕТТО, ДРУГИХ МЕСТ
ПРИНУДИТЕЛЬНОГО
СОДЕРЖАНИЯ,
СОЗДАННЫХ ФАШИСТАМИ
ИХ СОЮЗНИКАМИ
В ПЕРИОД ВТОРОЙ
МИРОВОЙ ВОЙНЫ

ИНВАЛИДЫ
БОЕВЫХ
ДЕЙСТВИЙ

ОДИНОКО
ПРОЖИВАЮЩИЕ
ГРАЖДАНЕ
В ВОЗРАСТЕ
ОТ 55 ЛЕТ
И СТАРШЕ

ГРАЖДАНЕ,
ПОСТОЯННО
ПРОЖИВАЮЩИЕ
В САДОВОДЧЕСКИХ
НЕКОММЕРЧЕСКИХ
ТОВАРИЩЕСТВАХ

ДЛЯ ПОЛУЧЕНИЯ АВТОНОМНОГО ПОЖАРНОГО ИЗВЕЩАТЕЛЯ НЕОБХОДИМО ВЫБРАТЬ УДОБНЫЙ СПОСОБ:

- ОСТАВИТЬ ЗАЯВКУ ПО НОМЕРУ 8(347) 272-00-24 В БУДНИЕ ДНИ С 9:00 ДО 18:00 ЧАСОВ
- ОСТАВИТЬ ЗАЯВКУ НА ЭЛЕКТРОННУЮ ПОЧТУ: CENTRPPU@PPSRB.RU
- ПОДАТЬ ЗАЯВЛЕНИЕ ЧЕРЕЗ САЙТ РЕГИОНАЛЬНЫХ ГОСУСЛУГ ИЛИ В ОФИСЕ МФЦ
- ОСТАВИТЬ ЗАЯВКУ НА САЙТЕ [HTTPS://GKCHS.BASHKORTOSTAN.RU](https://gkchs.bashkortostan.ru) В РАЗДЕЛЕ «ОБРАЩЕНИЕ ГРАЖДАН»





ГОСУДАРСТВЕННЫЙ КОМИТЕТ РЕСПУБЛИКИ БАШКОРТОСТАН ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ

**ЗАЩИТИТЕ СВОЮ ЖИЗНЬ И ЖИЗНЬ СВОИХ БЛИЗКИХ -
УСТАНОВИТЕ АУТОНОМНЫЙ ДЫМОВОЙ ПОЖАРНЫЙ ИЗВЕЩАТЕЛЬ!**

- ✓ ОБНАРУЖИТ ПОЖАР
- ✓ ПОДАСТ МОЩНЫЙ ЗВУКОВОЙ СИГНАЛ
- ✓ РАЗБУДИТ СПЯЩЕГО ЧЕЛОВЕКА
- ✓ НЕ ТРЕБУЕТ ОБСЛУЖИВАНИЯ СПЕЦИАЛИЗИРОВАННОЙ ОРГАНИЗАЦИИ
- ✓ РАБОТАЕТ ОТ БАТАРЕЕК «КРОНА»





ГОСУДАРСТВЕННЫЙ КОМИТЕТ РЕСПУБЛИКИ БАШКОРТОСТАН
ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ

ДЕЙСТВИЯ ПРИ ПОЖАРЕ

сохраняйте спокойствие!



**СРОЧНО ПОКИНЬТЕ ПОМЕЩЕНИЕ, ПЕРЕДВИГАЯСЬ
В ПРОТИВОПОЛОЖНУЮ СТОРОНУ ОТ ПОЖАРА**



**ИСПОЛЬЗУЙТЕ СРЕДСТВА ЗАЩИТЫ ОРГАНОВ ДЫХАНИЯ
ИЛИ ДЫШИТЕ ЧЕРЕЗ МОКРУЮ ТКАНЬ**



**СООБЩИТЕ О ПОЖАРЕ ПО ТЕЛЕФОНУ
ЭКСТРЕННЫХ СЛУЖБ «112»**



**ПРИ ОТСУТСТВИИ УГРОЗЫ ЖИЗНИ И ЗДОРОВЬЮ
ПРИСТУПИТЕ К ТУШЕНИЮ ПОЖАРА**



**ОКАЖИТЕ ПОМОЩЬ ПРИ ЭВАКУАЦИИ ДЕТАМ,
ПОЖИЛЫМ, РАНЕНЫМ И БОЛЬНЫМ**



**В СЛУЧАЕ ПОЖАРА В ЧАСТНОМ ДОМЕ, ПРИ НЕВОЗМОЖНОСТИ
ПОКИНУТЬ ПОМЕЩЕНИЕ ЧЕРЕЗ ДВЕРЬ, ЭВАКУИРУЙТЕСЬ ЧЕРЕЗ
ОКНО, ПРЕДВАРИТЕЛЬНО ПЛОТНО ЗАКРЫВ ДВЕРЬ В ПОМЕЩЕНИЕ
(БЕРАНДУ), ГДЕ ВОЗНИК ПОЖАР.**

УВАЖАЕМЫЕ ЖИТЕЛИ ГОРОДА!

СОБЛЮДАЕТЕ ЭЛЕМЕНТАРНЫЕ ПРАВИЛА ПОЖАРНОЙ БЕЗОПАСНОСТИ:



- уходя из дома, убедитесь, что все электронагревательные приборы выключены;
- не применяйте самодельные электронагревательные приборы;



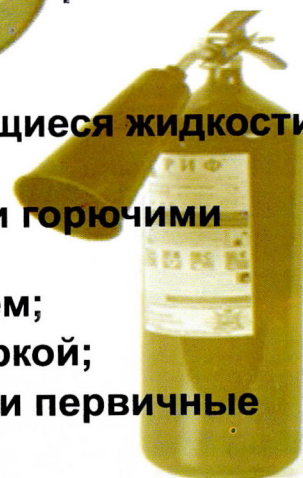
- не пользуйтесь поврежденными розетками;
- не курите в постели;
- храните спички и зажигательные приборы в местах, недоступных для детей;
- не оставляйте детей без присмотра;



- не храните дома легковоспламеняющиеся жидкости и взрывоопасные предметы;
- не загромождайте балконы и лоджии горючими материалами;



- не пользуйтесь дома открытым огнем;
- не сушите белье над газовой конфоркой;
- имейте дома пожарные извещатели и первичные средства пожаротушения.



СДЕЛАЙТЕ СВОЮ ЖИЗНЬ БЕЗОПАСНЕЕ – УСТАНОВИТЕ АВТОНОМНЫЙ ДЫМОВОЙ ПОЖАРНЫЙ ИЗВЕЩАТЕЛЬ!

- обнаружит пожар
- подаст мощный звуковой сигнал
- разбудит спящего человека
- легко устанавливается
- работает от батареек



**О ПОЖАРЕ
ЗВОНИТЬ**

101

Другие экстренные службы:

ПОЛИЦИЯ

102

**АВАРИЙНАЯ
ГАЗОВАЯ СЛУЖБА**

104

**СКОРАЯ
ПОМОЩЬ**

103

**ЕДИНАЯ СЛУЖБА
СПАСЕНИЯ**

112