Основы информационной безопасности в современном мире.

Противодействие кибермошенничеству

Минцифры Чувашии
Февраль 2026 г.

Почему это касается каждого?

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.

91%

россиян сталкивались с попытками мошенничества

59%

пользователей используют один и тот же пароль для всех аккаунтов

123456

самый популярный пароль среди пользователей Рунета

Хорошая новость: кибергигиена — это просто!

Что такое персональные данные и почему их нужно беречь?

Персональные данные — это любая информация, которая относится к конкретному человеку (к прямо или косвенно определенному или определяемому физическому лицу).

специальные категории

сведения о расовой, национальной принадлежности, политических взглядах, состоянии здоровья и прочие

биометрические персональные данные

сведения, характеризующие физиологические или биологические особенности человека, на основании которых можно установить его личность (идентифицировать и аутентифицировать) и которые используются оператором для такого установления личности (например, цифровое фотографическое изображение);

иные персональные данные

те, которые не относятся к специальным или биометрическим, например, ФИО, адрес регистрации, место работы).

Главная опасность — социальная инженерия (обман)

Это психологическое манипулирование людьми с целью заставить их совершить ошибку — перевести деньги, раскрыть пароли или скачать вредоносный файл.

Схема 2024 года

Вам в мессенджер пишет «руководитель» (с его фото и именем) и сообщает, что в компанию придут с проверкой. Через минуту звонит «куратор из ФСБ/безопасности банка» и запугивает уголовной ответственностью, требуя срочно перевести деньги на «безопасный счет».

Мошенники играют на эмоциях, используя классические психологические ловушки

Эмоциональный триггер	Как это работает	Примеры фраз мошенников
Страх и Срочность	Давление и угроза потери, чтобы отключить логику.	*«Ваш счет заблокируют через час!», «На вас оформили кредит, срочно нужен ваш звонок».*
Жадность и Радость	Ослепление халявой, притупление бдительности.	*«Вы выиграли в лотерею!», «Суперскидка только сегодня!», «Пособие от государства — перейдите по ссылке».*
Доверие и Авторитет	Подмена личности, использование уважения к знакомым.	*«Звонок от родственника» (с просьбой перевести деньги), «Директор просит срочно ответить в мессенджере».*
Любопытство	Желание узнать тайну перевешивает осторожность.	*«Посмотри фото с твоего дня рождения», «А это ты на видео?», «Пришла посылка, перейди для отслеживания».*

Главная опасность — социальная инженерия (обман)

Это психологическое манипулирование людьми с целью заставить их совершить ошибку — перевести деньги, раскрыть пароли или скачать вредоносный файл.

Актуальные схемы (2025 – начало 2026):

Новая схема	В чем суть	Почему это опасно
Дипфейки (Deepfakes)	Мошенники клонируют голос (30 сек. записи достаточно) или видео начальника/родственника через нейросети и звонят вам	Раньше писали в чат, теперь звонят "лично". Доверие резко растет. *(В 2025 году в России зафиксирован рост таких атак на 300%).*
Мошенничество с Госуслугами 2.0	Звонок от "оператора сотовой связи" о продлении договора. Для этого просят назвать код из СМС.	Код дает мошенникам вход в Госуслуги. Оттуда они берут ваши паспортные данные и оформляют микрозаймы.
Фейковые инвестиции + "Брокер"	Вам пишут "красивые люди" в Telegram/WhatsApp, зовут на обучение трейдингу, а затем просят перевести крупную сумму "под руководством личного брокера".	Люди теряют не только свои деньги, но и кредитные. Схема растянута на недели, втираются в доверие.
Гибридные атаки	Комбинация: сначала взламывают аккаунт знакомого в Telegram, а потом звонят вам по видео (запись дипфейк) и просят денег.	Сочетает сразу несколько триггеров: доверие (друг) + авторитет (видео) + срочность.

96% киберпреступлений сегодня связаны с обманом людей, а не со взломом программ

Прогноз Positive Technologies на 2026 год

Основной вектор атак останется социальная инженерия, но с массовым внедрением ИИ-технологий (дипфейки) для подделки лиц и голосов

Основные правила цифровой безопасности

Доверяй, но проверяй!

1 Критическое мышление

СТОП → ПРОВЕРЬ
Не верь номеру звонящего (даже 900)

Никому:
коды из СМС, CVV, пароли

2 Защита входов

Пароли:
длинные и разные.
Храни в менеджере

2FA включи везде (код из приложения).

3 Приватность

Настройки:
закрой профиль от чужих.

Друг просит денег?
Перезвони ему!

Основные правила цифровой безопасности

4 Мобильные угрозы

Wi-Fi:
Не входи в банк через публичные сети

Приложения:
Качай из официальных магазинов

5 Резерв

Бэкап:
Фото и доки на внешний диск

Обновления:
Для телефона и приложений – закрывает «дыры»

6 Кому верить?

Можно:
Госуслуги и банки (защищены законом).

Нельзя:
Мелкие сайты и сайты «однодневки»

Читай:
Согласие на обработку персональных данных , перед тем как ставить галочку

Правила кибергигиены: пароли

от 80% угроз

защищает соблюдение простых правил кибербезопасности

создавайте надежные пароли

Надежные пароли не обязательно сложные для запоминания

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

Mashin_borch_na_5_ballov!

Длина пароля 10 или более символов **>10**

Использование случайных комбинаций **mdm**

Использование верхнего и нижнего регистра, чисел и символов **Ab9?**

Отсутствие простых комбинаций букв и чисел **qwe123**

Отсутствие публичной информации **1989г.р.**

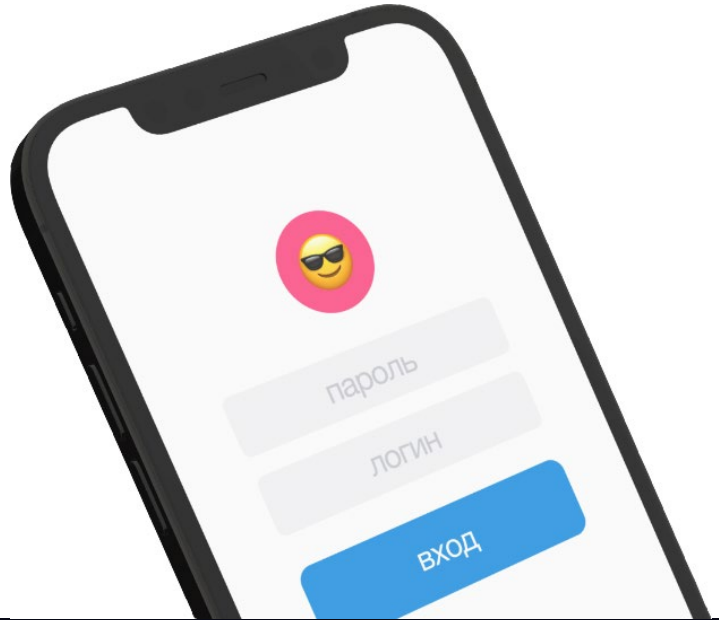
Не используйте одинаковые пароли для важных ресурсов: соцсети, почта, государственные сайты, интернет-банк

Двухфакторная аутентификация

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

1 этап

Стандартный 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.

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.

Внимание к именам сайтов и отправителям писем

Как определять фишинговый сайт?

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.

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