

powered by

MSSP
GLOBAL



citizensec

citizen zen sec

Журнал о кибербезопасности

Знание — это защита.

Мы поможем вам понять риски и научимся вместе защищать себя и своих близких.

2025



Внимание! Журнал CitizenSec по кибербезопасности с практическими советами, которые предотвратят синие экраны и защитят вас от сбоев, вирусов и других киберугроз.

Четкие рекомендации от экспертов с 10-летним опытом.

Учитесь один раз, экономьте и защищайте себя всегда!

citizensec - кибергигиена и методология
powered by mssp.global



citizensec

"CitizenSec" — проект, разработанный экспертами mssp.global в сотрудничестве со специалистами Комитета по информационной безопасности МЦРИАП РК. Материал основан на более чем 10-летнем опыте работы в сфере кибербезопасности.

Наша миссия

— повышать киберкультуру, обучая необходимым знаниям и навыкам для цифрового мира.

Содержание

Социальная инженерия. Как действуют мошенники? **06**

Какие методы и психологические приёмы они используют, чтобы вводить людей в заблуждение. Способы их распознавать.

Фишинг и спам **09**

Основные методы фишингового мошенничества и способы защитить себя с помощью практических рекомендаций.

Надёжный пароль, какой он? **15**

Узнайте, как создавать надёжные пароли, а также какие пароли наиболее уязвимы для взлома.

Don't touch my phone! **18**

Ваш телефон хранит все — от личных данных до финансов. Узнайте, как защитить его от угроз.

Шын ба? Wi-Fi бар ма? **21/23**

Фактчекинг и дезинформация: как защититься, а также все способы использовать Wi-Fi безопасно.

Получите – распишитесь **25**

Узнайте как сохранить ваши персональные данные и ваши активы в безопасности. Все о защите ЭЦП.

Покажи мне деньги! **30**

Финансовая безопасность: как защитить свои деньги от мошенников.

Детки – конфетки **32**

Простые способы защитить своих детей от киберугроз и мошенников в интернете.

02

Социальная инженерия. Как действуют мошенники?

Какие методы и психологические приёмы они используют, чтобы вводить людей в заблуждение, и способы их распознавать.

Социальная инженерия

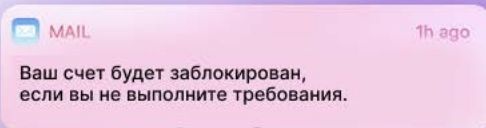
Социальная инженерия — это манипуляция для получения конфиденциальной информации, активации вредоносного ПО или выполнения нужных злоумышленнику действий.

- Мошенники манипулируют вашими эмоциями, используя страх, срочность и доверие.

**Методы
мошенников**



**Используют
страх
и срочность.**



Я звоню из вашего
банка, нам нужно
подтвердить вашу
информацию.

**Притворяются
представителями
авторитетных
организаций.**

**Давят на вас
через срочность.**

На вашем счете
зафиксирована
подозрительная операция.
Для отмены транзакции
подтвердите данные
карты в течение 10 минут.

Вы один из наших самых
ценных клиентов, и у нас
для вас есть особенное
предложение, которое
точно вас заинтересует.
Хотите узнать больше?

**Завоевывают
доверие с помощью
лестных отзывов.**

**Утверждают,
что все так делают.**

Тысячи людей уже
воспользовались
этим предложением.



Если сообщение **вызывает эмоции**, сделайте паузу. Не предоставляйте личные данные, не отправляйте деньги в спешке.

Проверяйте информацию через официальные каналы или позвоните в организацию напрямую.

03

Фишинг и спам.

Основные методы фишингового мошенничества и способы защитить себя.

Фишинг

— это как рыбалка, но это охота с целью украсть ваши данные.

Фишинговые атаки проявляются через поддельные уведомления по почте, СМС или в мессенджерах, чтобы заставить вас ввести чувствительные данные.

Фишинг

Классический метод с поддельными письмами и ссылками для получения доступа к конфиденциальным данным.

SEO-фишинг

Фейковые сайты, похожие на настоящие, которые появляются на первых строчках при поиске в браузере.

Вишинг

Мошенники звонят по телефону, придумывая разные сценарии для выманивания информации.

Смишинг

Мошенничество через СМС и текстовые сообщения.

Малвертайзинг

Встроенная вредоносная программа в онлайн рекламе.

Spear-фишинг

Целенаправленный фишинг на основе собранных данных о конкретной личности.

Спам-фишинг

Массовая рассылка фишинговых писем.

Как понять, что это фишинг?

**1 Остановитесь,
посмотрите,
подумайте.**

2 Предупреждающие знаки:

- Ошибки в письме или адресе.
- Проверяйте адрес отправителя и ссылки.
- Осторожно с письмами, вызывающие сильные эмоции.
- Проверяйте адресную строку сайта.

3 Не открывайте подозрительные вложения.

4 Не делайте предположений, всегда проверяйте.

**5 Не ведитесь
на уловки
и выгодные
предложения,
сохраняйте
холодный рассудок.**

Анатомия фишинга

Создание убедительного контента для фишинговой атаки

1. Часто используются актуальные темы
2. Создание фальшивых электронных писем с ссылками на поддельные сайты или с зараженными вложениями.

001

002

003

Привлечение внимания и обмана жертв

Использование срочных или эмоционально заряженных сообщений (например, "Акция истечет через несколько часов").

Массовая отправка фишинговых писем

Использование серверов для массовой рассылки или взломанных учетных записей для отправки писем, чтобы они выглядели как легитимные.

Захват данных, получение конфиденциальной информации

Ссылка в письме ведет
на фальшивый сайт, который
выглядит как легитимный
(законный).

Скрытие следов

Для того, чтобы их
не поймали и не задержали.

004

005

006

007

Воспользоваться украденной информацией

Использование
полученных учетных
данных для входа
в настоящие аккаунты
жертв.

А это уже агент...

**Как они
подбирают
пароли,
и почему
у них это
получается?**

04

Надёжный пароль, какой он?

Как создавать надёжные пароли и какие
из них наиболее уязвимы для взлома.

ПАРОЛЬ

Статистика:

80%

взломанных аккаунтов
использовали
популярные пароли?

Даже Марк Цукерберг был взломан из-за использования одного пароля на всех аккаунтах.

Знакомо?

Мы знаем, что ты тоже иногда так делаешь. Да и сложно запоминать все пароли....

Брутфорс — это метод подбора паролей путем перебора всех возможных комбинаций. Слабые пароли могут быть взломаны за считанные секунды. Защита проста: создавайте сложные и уникальные пароли для каждого аккаунта.



ОРЁЛ

Решение: Используйте менеджер паролей.

Типы паролей по важности:

Обычная важность

Эти пароли используются для повседневных задач и менее критичных сервисов.

- Социальные сети.
- Почтовые сервисы.
- Мессенджеры.
- Различные сайты и онлайн-магазины.

Высокая важность

Эти пароли защищают доступ к самым важным и чувствительным данным.

- Банковские аккаунты и финансовые приложения.
- Шифрование жесткого диска.
- Доступ к менеджеру паролей.
- Учетные записи с административным доступом.

Совет:

Менеджер паролей поможет безопасно хранить все пароли и использовать уникальные, сложные комбинации для каждого аккаунта. Это снизит риск взлома и защитит ваши данные.

Не храните все пароли в одном месте.

Разделяйте пароли по важности.

Используйте **менеджеры паролей**. Они обеспечивают безопасное хранение и управление паролями.

Создавайте **сложные и уникальные пароли**. Для этого используйте встроенные генераторы в менеджерах паролей.

Не передавайте пароли **целиком**. Если нужно поделиться паролем, разделите его на части и передайте через разные каналы связи.

Рекомендуемые менеджеры: Dashlane, 1Password, KeyPassXC, Bitwarden, Enpass.

05

Do not touch my phone!

Ваш телефон хранит все — от личных
данных до финансов.
Узнайте, как защитить его от угроз.

Защита гаджетов

Гаджеты всегда с нами — это карманные компьютеры, где хранится вся наша жизнь: от часов и фотографий до работы и финансов.

Проблема:

Вредоносные приложения угрожают вашей личной и финансовой безопасности, похищая банковские данные и пароли.

Современные схемы мошенников включают видеозвонки для сбора биометрии, что позволяет оформлять кредиты и проводить операции **от вашего имени.**

Решение:

Ключевые меры защиты наших устройств:

- 1** Установите сложный пароль, ПИН-код и используйте биометрию для защиты устройства.
- 2** Загружайте приложения только из официальных источников: Приложения из Google Play или App Store безопаснее.
- 3** Надежный антивирус помогает обнаруживать и блокировать вредоносные программы.
- 4** Ограничьте доступ приложений к вашим данным, чтобы защитить свою информацию.
- 5** Настройте функции, позволяющие отслеживать местоположение устройства и удаленно стирать данные в случае кражи.
- 6** Регулярно сохраняйте важные данные, чтобы не потерять их в случае кражи или поломки устройства.

06

Шын ба?

Фактчекинг и дезинформация:
как защититься.



Фактчекинг и дезинформация: как защититься

Дезинформация - это намеренное введение в заблуждение, а **мисинформация** - распространение неверной информации по ошибке. Оба ведут к недоверию, поляризации и вреду обществу.

Чтобы избежать распространения фейков:

- **Проверяйте новости в официальных источниках и на платформах фактчекинга, таких как [Factcheck.kz](https://factcheck.kz) и [StopFake.kz](https://stopfake.kz).**
- **Развивайте критическое мышление и медиаграмотность.**
- **Будьте внимательны к защите личных данных.**

07

Wi- Fi бар ма?

Все способы использовать
Wi- Fi безопасно.

Публичные точки доступа Wi-Fi - это удобно, особенно на отдыхе или в поездках, но они могут быть небезопасными. Давайте разберем проблемы, риски и как защитить себя.

Проблемы и риски публичных точек доступа:

Отсутствие шифрования:

Многие публичные сети не шифруют данные, что делает их уязвимыми для перехвата. В результате ваша личная информация, включая пароли и финансовые данные, **может быть украдена**.

Атаки "человек посередине":

Мошенники могут перехватывать данные, передаваемые между вами и сетью, что позволяет им изменять или красть вашу информацию.

Фальшивые точки доступа:

Мошенники могут создавать поддельные сети, которые выглядят как легитимные. Подключившись к такой сети, вы невольно предоставляете им доступ к своим данным.

Решения

- 1 Используйте VPN:** Защищённый канал через VPN скрывает вашу активность и предотвращает перехват данных.
- 2 Проверяйте сеть:** Перед подключением убедитесь, что сеть действительно принадлежит публичному учреждению, а не злоумышленнику.
- 3 Отключите автоматическое подключение:** Не подключайте устройства автоматически к открытым сетям, чтобы избежать случайных подключений к фальшивым точкам доступа.
- 4 Используйте мобильный интернет:** Временно переключитесь на мобильные данные, если Wi-Fi сеть небезопасна.
- 5 Избегайте конфиденциальных операций:** Не совершайте банковские операции или покупки через публичные сети.
- 6 Используйте двухфакторную аутентификацию:** Включите двухфакторную аутентификацию для всех важных аккаунтов.

Example

08

Получите -
распишитесь!

Узнайте, как защитить ваши персональные
данные и активы с помощью наших советов.

item count:
total:

card: ****5677987

auth: 586843379

cardholder:



Персональные данные

— это любая информация, которая идентифицирует вас как личность.

- 1. Общедоступные данные:** информация, которая может быть доступна другим с вашего согласия (например, ФИО, ИИН, адрес).
- 2. Данные ограниченного доступа:** информация, которая охраняется законом (например, медицинская, финансовая или коммерческая информация).

Идентификационные данные: ИИН, ФИО, дата рождения, паспортные данные.

Контактные данные: адрес проживания, номер телефона, электронная почта.

Финансовые данные: банковские счета, информация о доходах и расходах.

Медицинские данные: история болезни, результаты анализов.

Образовательные данные: дипломы, сертификаты, уровень образования.

Профессиональные данные: место работы, должность, профессиональные навыки.

Данные о семейном положении: информация о браке, детях, родственниках.

Информация о перемещениях: история посещений, геолокация.

Внимание!

Перед тем как передать свои данные, обратите внимание:



- **Цели сбора и обработки данных:** зачем их собирают?
- **Срок хранения данных:** как долго ваши данные будут использоваться?
- **Возможность передачи данных третьим лицам:** кому и зачем они могут быть переданы?
- **Трансграничную передачу:** могут ли ваши данные быть переданы за границу?
- **Общедоступность данных:** будут ли ваши данные опубликованы?

Ваши права защищены законом

В Казахстане защита персональных данных регулируется несколькими законами:

- Закон РК "О персональных данных и их защите" — регулирует сбор и обработку данных, а также и права граждан.
- Закон РК "Об информатизации" — защищает данные в информационных системах.
- Гражданский кодекс — гарантирует право на защиту личной и семейной тайны.
- Уголовный кодекс и Кодекс об административных правонарушениях — устанавливает ответственность за нарушение законодательства о персональных данных.

Ваши права

Получать информацию о том, кто и как обрабатывает ваши данные.

Изменять или удалять свои данные.

Отозвать своё согласие на их обработку.

Что делать при нарушении прав?

Если ваши данные были незаконно собраны или использованы:

1 Обратитесь к организации, допустившей нарушение, с требованием уничтожить данные.

2 Подайте жалобу в Комитет по информационной безопасности МЦРИАП РК через портал **e-otinish**.

В жалобе укажите:

- ФИО и контактные данные.
- Подробное описание нарушения.
- Доказательства (скриншоты, письма, наименование организации и т.д.).

Как защитить свои данные?

- Читайте условия политики конфиденциальности перед тем, как соглашаться на обработку данных.
- Не публикуйте чувствительную информацию в соцсетях.
- Используйте сложные пароли и не передавайте их третьим лицам.
- Регулярно проверяйте, кто имеет доступ к вашим данным.

Все о безопасности ЭЦП

Электронная цифровая подпись (ЭЦП) — это цифровой аналог рукописной подписи, подтверждающий подлинность, целостность данных и идентификацию подписавшего лица.

Риск

Если злоумышленники получают доступ к личному ключу ЭЦП, они смогут подписывать документы от вашего имени.

Меры защиты:

- +** Храните ключи в защищённом месте (смарт-карты, USB-токены).
- +** Обновляйте ПО для работы с ЭЦП.
- +** Используйте сложные пароли и меняйте их регулярно.
- +** **Отзывайте неиспользуемые или утерянные ключи ЭЦП!**
-Это очень важно, ведь именно эти ключи чаще всего обычно похищают злоумышленники.

Ответственность:

Административная — за непринятие мер по защите и передаче ЭЦП (ст. 640 КоАП РК).

Уголовная — за неправомерный доступ к системе (ст. 205 УК РК).

При нарушениях обращайтесь в Комитет по информационной безопасности МЦРИАП РК.

09

Покажи мне деньги!

Финансовая безопасность: как защитить
свои деньги от мошенников.



Проблемы

- Фишинг — поддельные сайты/письма для кражи данных.
- Скимминг — установка устройств на банкоматах для копирования данных с банковских карт.
- Мошенничество с кредитами — незаконное оформление кредитов на ваше имя.

Решения

- +** **Осторожность с банкоматами**
Проверяйте банкоматы на наличие скиммеров (подозрительные элементы на клавиатуре или месте ввода карты).
- +** **"Стоп-кредит" через egov**
Подключите функцию для предотвращения оформления кредитов без вашего согласия (через egov или мобильное приложение).
- +** **Безопасные онлайн-платежи**
Делайте покупки на проверенных сайтах. Используйте отдельную карту для онлайн-платежей с ограниченной суммой.
- +** **Правила пользования картами**
3D Secure: Подключите защиту через банк, чтобы получать SMS-коды для подтверждения операций.
- +** **Двухфакторная аутентификация (2FA):**
Настройте дополнительную защиту в банковских приложениях и на сайтах.

10

Детки-конфетки

Простые способы защитить своих детей от киберугроз и мошенников в интернете.

Кибербезопасность для детей

История о технологиях ИИ: Недавно был случай, когда мошенники использовали ИИ для создания фальшивого голосового сообщения от имени родителей ребенка. Ребенок получил звонок с просьбой выйти со школы и поехать с незнакомым человеком. Якобы его отправила мама. Благодаря бдительности и правильному обучению, ребенок понял, что что-то не так, и сообщил об этом взрослым, избежав серьезных последствий.



Ограничение контента:



Совет: Используйте настройки DNS и роутера для ограничения доступа к нежелательным сайтам.

Пример: Установите DNS-сервисы, такие как OpenDNS, DNS-сервер Яндекса или Google SafeSearch, для фильтрации контента.

Родительский контроль:



Совет: Установите приложения для родительского контроля, такие как Google Family Link, чтобы следить за активностью ребенка в интернете.

Использование технологий ИИ:



Совет: Следите за развитием современных технологий, таких как подмена голоса или лица с помощью ИИ. Объясните детям, что не всему в интернете можно доверять.

История: Расскажите историю о том, как мошенники могут использовать ИИ для создания фальшивых видео или голосовых сообщений, чтобы обмануть их.

Кодовое слово с ребенком:

code

Совет: Создайте специальное кодовое слово, которое ребенок может использовать в экстренных ситуациях, чтобы сообщить вам о проблеме безопасно и незаметно.

1

Постоянный диалог:

Совет: Регулярно обсуждайте с детьми их онлайн-активности и объясняйте возможные угрозы.

2

Обучение безопасности:

Совет: Научите детей распознавать опасные ситуации, такие как подозрительные сообщения или предложения.

3

Проверка контактов:

Совет: Внимательно проверяйте, с кем общаются ваши дети в интернете. Объясните им, что не все люди в сети являются теми, за кого себя выдают.

4

Создание безопасной среды:

Совет: Создайте в доме безопасное пространство для обсуждения любых вопросов или проблем, связанных с интернетом. Пусть дети знают, что могут обратиться к вам за помощью в любой ситуации.

citizensec - кибергигиена и методология

citizensec

powered by

MSSP
GLOBAL



AI & DIGITAL
MINISTRY

citizensec