

Безопасный интернет – ключ к вашей цифровой жизни

Как защитить себя в онлайн- пространстве

**Тренеры-преподаватели отделения дзюдо МБУ ДО
«СШ РМО»:**

**Богданов Константин Сергеевич и Булдаков Игорь
Николаевич**

10 марта 2026 год



Введение: Почему безопасность в интернете важна?

Цифровой мир:

ВОЗМОЖНОСТИ И РИСКИ

Основные тезисы:

- Интернет — это огромный ресурс для обучения, работы, общения и развлечений.
- Онлайн-мир стал неотъемлемой частью нашей жизни.
- Но вместе с возможностями появляются и угрозы: кража личных данных, мошенничество, кибербуллинг, вирусы.
- Важно понимать эти риски и знать, как от них защититься.

Негативное воздействие компьютера на подростка



Основные угрозы онлайн-безопасности

С чем мы можем столкнуться?

Основные угрозы (кратко):

Вирусы и вредоносное ПО: Программы, которые могут повредить ваши устройства или украсть данные.

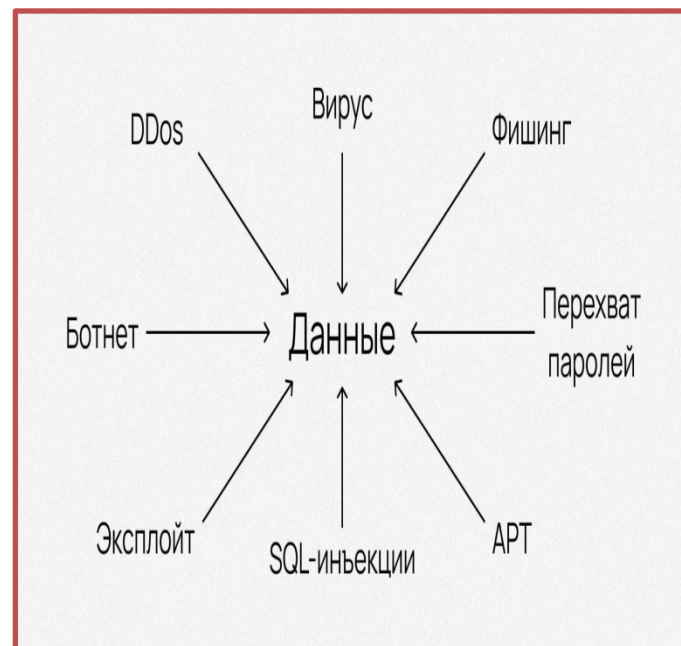
Фишинг: Попытки выманить ваши личные данные (пароли, номера карт) через поддельные сайты или письма.

Мошенничество: Обман с целью получения денег или ценной информации.

Кибербуллинг: Преследование, угрозы или оскорбления в интернете.

Кража личных данных: Получение доступа к вашей конфиденциальной информации.

Недостоверная информация: Дезинформация, фейковые новости.



Защита личных данных: Основа безопасности

- **Ваши данные – ваша крепость**

Ключевые правила:

- **Крепкие пароли:** Используйте комбинации букв, цифр и символов. Не используйте простые и очевидные пароли.
- **Уникальные пароли:** Для каждого аккаунта – свой пароль.
- **Двухфакторная аутентификация (2FA):** Включайте её везде, где возможно (дополнительный уровень защиты).
- **Не делитесь лишней информацией:** Осторожно относитесь к тому, что публикуете в социальных сетях.
- **Проверяйте настройки приватности:** Регулярно просматривайте, кто имеет доступ к вашей информации.



Как распознать фишинг и мошенничество?

- **Ловушки в сети: Будьте бдительны!**
- **Признаки подозрительной активности:**
 - **Неожиданные письма/сообщения:** С просьбой срочно перейти по ссылке или предоставить данные.
 - **Сомнительные ссылки:** Адреса сайтов, которые выглядят странно или не совпадают с официальными.
 - **Грамматические ошибки и опечатки:** В официальных письмах таких ошибок быть не должно.
 - **Давление и срочность:** Уведомления о блокировке аккаунта, выигрыше в лотерее, которое вы не участвовали.
 - **Запросы конфиденциальной информации:** Банки и известные сервисы никогда не просят пароли или полные номера карт по электронной почте.
- **Совет:** Если сомневаетесь – лучше не нажимайте и не отвечайте. Свяжитесь с официальной службой поддержки другим способом.

Памятка



Как определить фишинговое письмо:

- **сомнительная тема письма.** Чаще всего это «выигрыш», «приглашение» на работу с высокой зарплатой, «уведомления» из госструктур
- **ссылка.** Получателю фишингового письма предлагают перейти на сайт или скачать файл из вложения
- **контакты.** Если в письме указан телефон незнакомой компании-отправителя, его можно проверить в приложении для определения номера. Скорее всего, контакты несуществующие
- **в тексте есть ошибки и опечатки,** слова или предложения написаны транслитом
- **универсальное, неличное обращение** — например, «дорогой клиент»

Защита устройств: Антивирусы и обновления

- **Ваш цифровой щит**
- **Важность антивирусного программного обеспечения:**
 - Устанавливайте надежный антивирус и регулярно обновляйте его базы.
 - Регулярно сканируйте свои устройства на наличие вирусов.
- **Своевременные обновления:**
 - Операционная система, браузеры и приложения должны быть обновлены до последней версии. Обновления часто содержат исправления уязвимостей.
- **Безопасность Wi-Fi:**
 - Избегайте использования публичных Wi-Fi сетей для передачи конфиденциальной информации.
 - Используйте VPN при подключении к незнакомым сетям.



Безопасное поведение в социальных сетях

- **Социальные сети: Правила общения**

Рекомендации:

- **Контроль над информацией:** Что вы публикуете? Как часто? Кто это видит?
- **Правила приватности:** Настройте, кто может видеть ваши посты, фотографии, список друзей.
- **Осторожность с незнакомцами:** Не добавляйте всех подряд. Не переходите по подозрительным ссылкам, полученным от незнакомцев.
- **Кибербуллинг:** Не участвуйте, сообщайте о случаях. Помните о последствиях своих слов в интернете.
- **Фальшивые аккаунты:** Будьте внимательны к подозрительным профилям.



Безопасный шопинг и онлайн-платежи

- **Покупки онлайн: Без риска!**

Ключевые моменты:

- **Надежные сайты:** Покупайте только на проверенных интернет-магазинах. Проверяйте наличие HTTPS в адресной строке (замочек).
- **Безопасные платежные системы:** Используйте надежные способы оплаты.
- **Не сохраняйте данные карт:** Если не уверены в надежности сайта.
- **Двухфакторная аутентификация:** При оплате, если доступна.
- **Осторожность с акциями:** Слишком выгодные предложения могут быть обманом.



Дети и интернет: Как защитить юное поколение

- Интернет для детей: Безопасно и познавательно

Родителям и опекунам:

- **Открытый диалог:** Говорите с детьми о правилах поведения в интернете, рисках и опасностях.
- **Контроль и фильтрация:** Используйте программы родительского контроля.
- **Совместное изучение:** Проводите время в интернете вместе с детьми.
- **Учите критическому мышлению:** Обсуждайте информацию, которую они находят.
- **Установите правила:** Время, проведенное онлайн, допустимый контент.



Что делать, если вы стали жертвой?

- **Произошла беда? Не молчите!**

Ваши действия:

- **Не паникуйте.**
- **Смените пароли:** Сразу же смените пароли от всех затронутых аккаунтов.
- **Обратитесь в службу поддержки:** Платформы, где произошел инцидент (соцсети, банк, интернет-магазин).
- **Сообщите в правоохранительные органы:** Если речь идет о мошенничестве или других преступлениях.
- **Обратитесь к специалистам:** При заражении вирусами или технической помощи.
- **Расскажите близким:** Не оставайтесь с проблемой один на один.

Заключение:

Безопасность – в наших руках

- **Ваш безопасный интернет**
- **Ключевые выводы:**
 - Интернет – это мощный инструмент, но он требует ответственного подхода.
 - Будьте бдительны, используйте надежные инструменты защиты.
 - Постоянно обновляйте свои знания о новых угрозах и методах защиты.
 - Безопасность в интернете – это не разовая акция, а постоянный процесс.
- **Призыв к действию:** Сделайте безопасность в интернете своим приоритетом!

