Обеспечение кибербезопасности обучающихся

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Современный человек использует интернет для решения повседневных задач: для общения, учебы, профессиональной деятельности, творчества.

Подключение к интернету предоставляет нам огромную пользу, однако как и в реальной жизни, в интернете можно столкнуться с различными угрозами.

Кибербезопасность – это совокупность мер, нацеленная на обеспечение защиты пользователей их информационных систем, программ от атак злоумышленников.

Кибербезопасность играет важную роль в обеспечении безопасного и ответственного поведения детей в цифровом мире, а также в защите их интересов и данных. Это навык, который дети должны освоить с раннего возраста и поддерживать в повседневной жизни.

Ситуации по кибербезопасности могут быть разнообразными и могут включать в себя различные угрозы и вызовы для школьников.

Онлайн-жертвы мошенничества

СИТУАЦИЯ:

Школьники могут получать электронные сообщения или видеть в интернете предложения участвовать в лотерее, опросе или другой схеме, которая может быть мошеннической.

РЕШЕНИЕ:

Не доверяйте подобным предложениям. Не разглашайте личные данные и не отправляйте деньги незнакомым людям.

Кибербуллинг:

СИТУАЦИЯ:

Дети могут столкнуться с онлайн-насмешками, угрозами и другими формами цифрового насилия со стороны сверстников.

РЕШЕНИЕ:

Сообщите об инциденте взрослым, таким как родители или учителя. Не отвечайте на агрессию и блокируйте или удаляйте действующие учетные записи.

Утечка личной информации:

СИТУАЦИЯ:

Дети могут случайно или ненамеренно раскрывать личные данные в интернете.

РЕШЕНИЕ:

Будьте осторожными с информацией, которую вы публикуете онлайн, и обучитесь удалять нежелательные данные. Не делитесь личными данными в чатах и социальных сетях.

Вредоносные программы и вирусы:

СИТУАЦИЯ:

Скачивание файлов с ненадежных источников или открытие вредоносных вложений может привести к заражению компьютера вредоносными программами.

РЕШЕНИЕ:

Устанавливайте антивирусное программное обеспечение и не открывайте незнакомые файлы и ссылки.

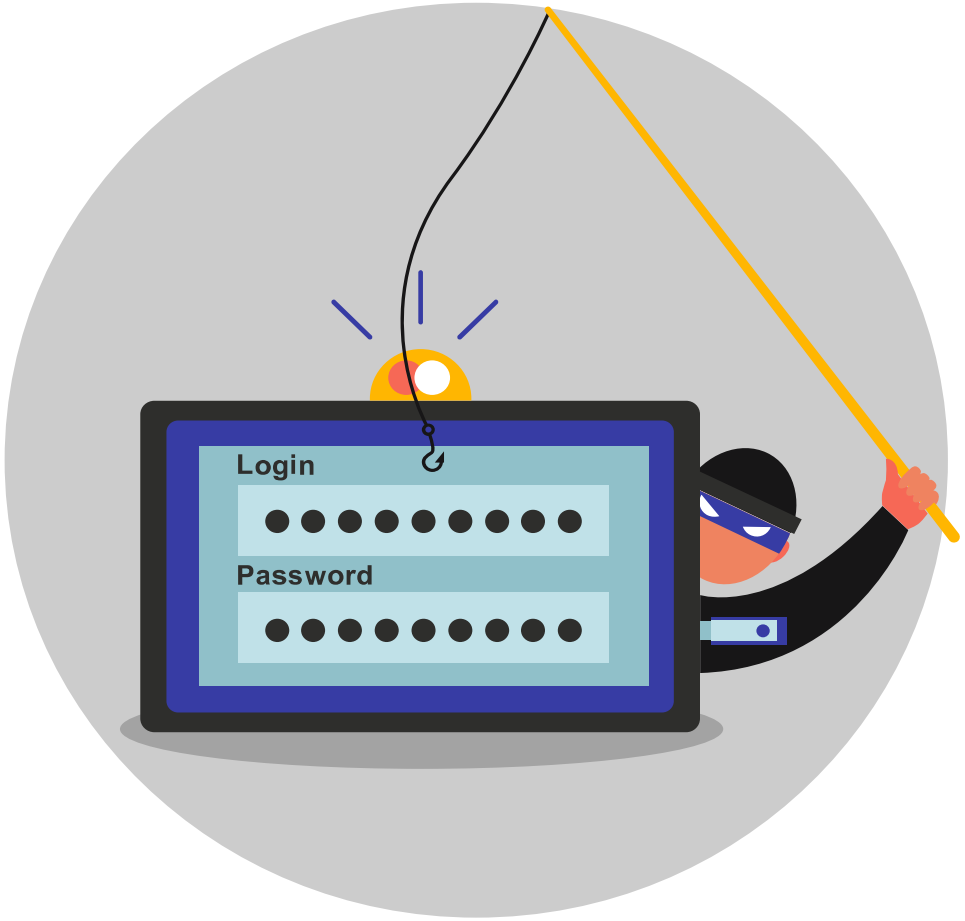
Фишинг:

СИТУАЦИЯ:

Мошенники могут выудить у детей пароли, номера родительских банковских карт и прочую конфиденциальную информацию.

РЕШЕНИЕ:

Не открывайте вложения или ссылки в электронных сообщениях от незнакомых или подозрительных источников. Внимательно смотрите на адрес отправителя. Фишеры часто используют похожие адреса, но с небольшими отличиями.



Рекомендации информационной безопасности в интернете

01 Используйте длинные пароли, включая буквы верхнего и нижнего регистра, цифры и специальные символы.

02 Никогда не давайте свой пароль другим людям, даже близким друзьям.

03 Будьте осторожными с информацией, которую вы публикуете в социальных сетях. Не раскрывайте личные данные, такие как адрес, номер телефона и школу.

04 Будьте осторожны с электронными сообщениями и ссылками от незнакомых отправителей. Они могут содержать вредоносное ПО.

Рекомендации информационной безопасности в интернете

05 Используйте безопасные сети Wi-Fi и не подключайтесь к открытым или ненадежным сетям.

06 Будьте осторожны в онлайн-играх и чатах, избегайте общения с токсичными игроками и не раскрывайте личные данные.

07 Установите антивирусное программное обеспечение на свой компьютер или устройство и регулярно обновляйте его.

08 Если вы столкнулись с кибержестокостью, угрозами или другими проблемами в интернете, немедленно сообщите об этом родителям, учителям или доверенным взрослым.