

Кибербезопасность



Что такое кибербезопасность?

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Что такое медиаграмотность?

Медиаграмотность — это, согласно одному из определений, способность получать, анализировать, оценивать и передавать сообщения в разных формах.

Медиаграмотный человек свободно пользуется разными типами медиа — от интернета до телевидения — и понимает, как они устроены, критически оценивает сообщения из разных источников и может самостоятельно передавать эти сообщения другим людям. К медиаграмотности также относится понимание последствий того, что мы делаем онлайн.

Виды киберугроз

Кибербезопасность борется с тремя видами угроз.

1.Киберпреступление– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

2.Кибератака – действия, нацеленные на сбор информации, в основном политического характера.

3.Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Начать торопить пользователя, чтобы не дать разобраться в происходящем.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.
4. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
3. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
4. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего 19 телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

1. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
2. Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

1. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
2. Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
3. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

1. Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
2. Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
3. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
2. Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
3. Не переходите по ссылкам от малознакомых людей.
4. Защищайте всю информацию, даже если думаете, что она не важна.

Угроза: продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
3. Разослать спам-сообщение друзьям пользователя.

Пример защиты:

1. Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
2. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
3. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
4. Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза: мошенничество через подменные/анонимные профили.

Пример атаки:

1. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
2. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.
3. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
4. Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Не поддавайтесь агрессии и не ведитесь на провокации.
3. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
4. Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
5. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

1. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).
2. Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

1. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
2. Не переходите по ссылкам от малознакомых людей.
3. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
4. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
5. Защищайте всю информацию, даже если думаете, что она не важна

Задание. Гуляя по торговому центру, Таня увидела платье, которое ей очень понравилось, но оно было дорогим. Девочка решила проверить, сколько это платье стоит в интернет-магазине. Не задумываясь, она подключилась к одной из обнаруженных открытых сетей «FreeWiFi». Зайдя на сайт интернет-магазина, девочка обнаружила точно такое же платье её размера, но по цене в 3 раза дешевле. Обрадовавшись, Таня оформила онлайн-покупку, введя номер банковской карты и трехзначный код с обратной стороны карты. После этого она авторизовалась в социальной сети и своей радостной новостью поделилась с подружкой.

1.Какие ошибки совершила Таня?

2.Какие негативные последствия совершенного ею поступка могут возникнуть? Обоснуйте свой ответ.

3.Сформулируйте правила, которыми нужно руководствоваться при использовании общественной Wi-Fi сети.

1.Подключившись к общественной Wi-Fi сети, Таня передала конфиденциальные данные: ввела номер и код с банковской карты, авторизовалась в социальной сети – ввела логин и пароль.

2.Негативные последствия совершенного поступка: злоумышленники с применением введенного Таней логина и пароля могут «взломать» её страницу в социальной сети, тем самым узнать личную информацию, от лица Тани просить у «друзей» деньги, шантажировать саму Таню и т.д. Кроме того, так как при оплате покупки Таня ввела трехзначный код с карты, то теперь ее картой могут воспользоваться мошенники, оплачивая свои покупки в Интернете.

3.Правила: не доверять сетям с подозрительными названиями (FreeInternet или FreeWiFi), не совершать онлайн-покупки и банковские переводы в общественных сетях, не передавать конфиденциальную информацию, не вводить логины и пароли от различных сайтов.