Угроза

Кража профиля пользователя через взлом логина/пароля

Пример атаки:

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

Пример защиты:

- Запросите больше информации о том, что вам предлагают.
- Проверьте официальный сайт компании, от лица которой вам пишут, и уточните информацию по контактам службы поддержки.
- Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
- Используйте разные пароли на различных сервисах.
- Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
- Настройте двухфакторную аутентификацию в социальных сетях, 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.

Угроза

Манипуляция, чтобы пользователь самостоятельно передал свои данные

Пример атаки:

- 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.
- Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
- Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

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

Угроза

Получение доступа к сохраненным личным данным/данным банковской карты

Пример атаки:

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

Пример защиты:

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

Угроза

Продуманное мошенничество на основе доступной информации о человеке

Пример атаки:

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

Пример защиты:

- Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
- Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фотографиями паспорта и других документов, билетов, посадочных талонов и др.
- Настройте двухфакторную аутентификацию в социальных сетях, 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.
- Не поддавайтесь агрессии и не ведитесь на провокации.

Угроза

Мошенничество через подменные/анонимные профили

Пример атаки:

- Проследить за открытой информацией в профиле, изучить подробности жизни человека.
- 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.
- 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.
- Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

- Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут, и уточните информацию по контактам службы поддержки.
- Не поддавайтесь агрессии и не ведитесь на провокации.
- 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.
- Выделите время и разберитесь в настройках приватности своего профиля во всех социальных сетях.
- 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:

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

Пример защиты:

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