Социальная инженерия

Узнайте о том, как распознать манипуляционные методы социальной инженерии и избежать их.

1. Как работают психологические атаки с помощью социальной инженерии?

Социальная инженерия — это методы и приемы, которые используют мошенники, чтобы обманом вынудить вас сделать что-то опасное, например передать вашу персональную информацию или перечислить деньги. Социальная инженерия существует не одно столетие и уже приспособилась к эре Интернета.

Главная цель социальной инженерии — манипулировать вами. Вот как работает психологическая атака с помощью социальной инженерии:

- Злоумышленник определяет жертву и собирает о ней информацию.
- Затем он выбирает метод социальной инженерии, который будет использовать.
- Злоумышленник связывается с жертвой и использует различные приемы, чтобы ею манипулировать.
- Злоумышленник убеждает жертву передать ему информацию или деньги.
- Злоумышленник прекращает спектакль и исчезает.

2. Каковы распространенные методы социальной инженерии?

Целью атак с помощью социальной инженерии является манипулирование вами. Вот распространенные методы и приемы:

- **Приманка.** В этом случае жертву пытаются соблазнить ложными обещаниями, такими как бесплатные загрузки, бесплатные услуги или призы.

- **Поддельные антивирусы.** Они часто выглядят как всплывающая реклама с тревожными сообщениями, которые должны вас запугать и вынудить передать вашу информацию или данные.
- **Фишинг.** Очень распространенная разновидность социальной инженерии, когда вашими эмоциями манипулируют посредством текстовых или электронных сообщений и пытаются убедить вас на что-то нажать, что-то загрузить или переслать информацию или деньги. При фишинговых атаках в качестве стимула часто используется срочность, но вас также могут попытаться запугать, сыграть на вашем сочувствии или заманить вас каким-нибудь призом.
- **Претекстинг.** С помощью этого метода злоумышленник может выдавать себя за человека, которому вы доверяете, или за сотрудника государственного органа, чтобы завоевать ваше доверие и вынудить вас передать информацию.
- **Адресный фишинг.** Этот вид фишинга направлен на одного человека или небольшую группу людей, при этом злоумышленник часто выдает себя за кого-то знакомого.

Помните, что социальная инженерия может осуществляться вне сети, а также при помощи телефонного спама и личного взаимодействия. Например, злоумышленники могут рыться в мусорных баках, чтобы получить вашу персональную информацию из мусора, или попытаться проникнуть в здание, чтобы похитить данные или технологии.

3. Каковы признаки социальной инженерии?

Будьте осторожны в следующих случаях:

- Запрос или сообщение приходит неожиданно.
- Запрос очень срочный.
- Вам кажется, что на вас давят, чтобы вынудить сделать что-то быстро.
- Предложение кажется уж слишком хорошим.
- Вы замечаете странные орфографические или грамматические ошибки.
- Сообщение кажется пугающим или угрожающим.

Помните, что «социальные инженеры» пытаются манипулировать вами и вынудить вас действовать без промедления, обдумывания и критического мышления. Не позволяйте вынудить вас что-то сделать!

4. Как избежать социальной инженерии?

- Знайте о методах, которые используют мошенники.
- Проверьте запрос, не отвечайте сразу же и не вступайте в прямой контакт.
- Проанализируйте свою эмоциональную реакцию: кажется ли вам, что вас торопят или вам угрожают?
- Сообщайте минимум данных и будьте осторожны, когда вы публикуете информацию в Интернете и делаете ее общедоступной.
- Создавайте надежные пароли, используйте многофакторную аутентификацию и менеджер паролей.
- Не открывайте вложения и не нажимайте на ссылки из незнакомых источников.
- Контролируйте настройки безопасности в учетных записях и очистите ваши профили в социальных сетях, чтобы в них не было личной или конфиденциальной информации.
- Обновляйте свои устройства и устанавливайте последние обновления для системы безопасности.
- Уничтожайте конфиденциальные документы.
- Создавайте резервные копии данных на случай взлома или атаки программы-вымогателя.

5. Составьте план

Подумайте о том, что вы можете сделать, чтобы повысить защищенность ваших учетных записей и информации и не стать жертвой социальной инженерии. Запишите свои мысли здесь: