Угрозы в сети Интернет

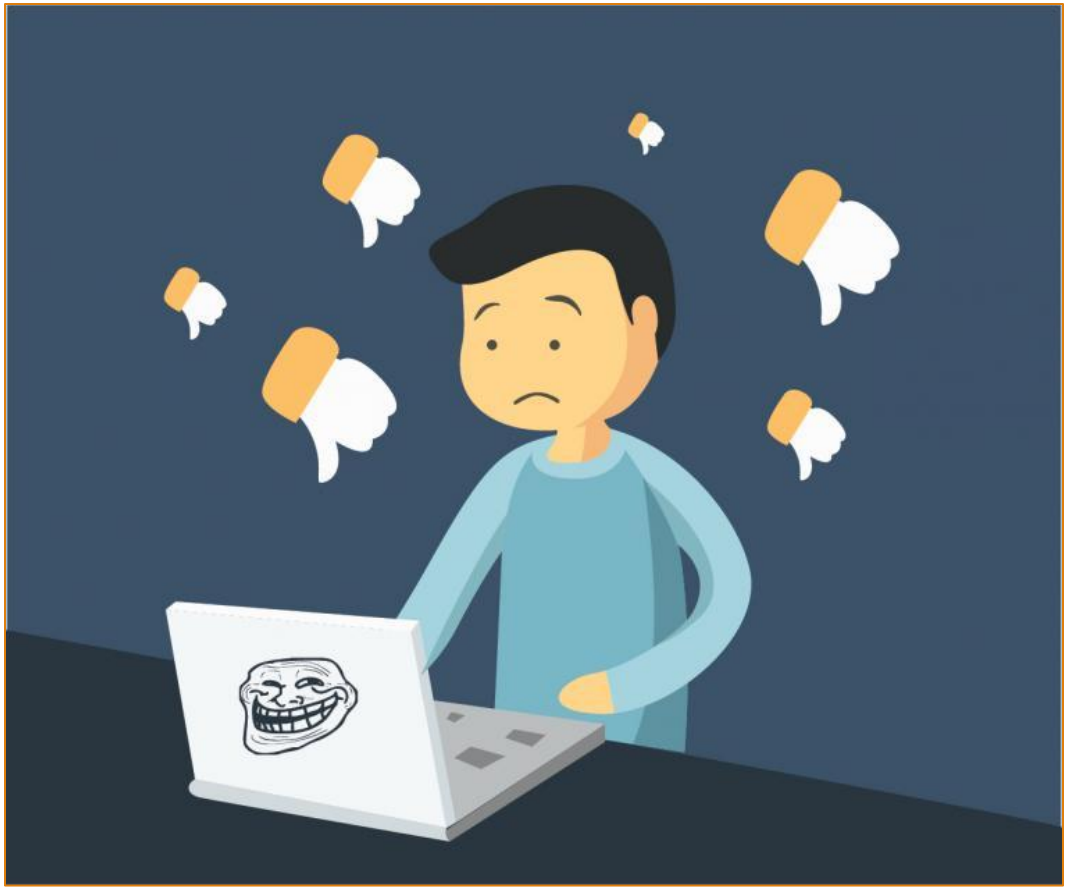
Классификация угроз при работе в сети Интернет

Угрозы личной безопасности

Угрозы безопасности компьютера

Угрозы личной безопасности

1. Неприличный контент - нежелательная информация: фотографии, видео, сайты.



Угрозы личной безопасности

2. Киберхулиганы - запугивание, преследование, агрессия со стороны других пользователей Интернета.

Угрозы личной безопасности

3. Люди – «хищники» используют Интернет, чтобы заманить детей на личную встречу.

Угрозы личной безопасности

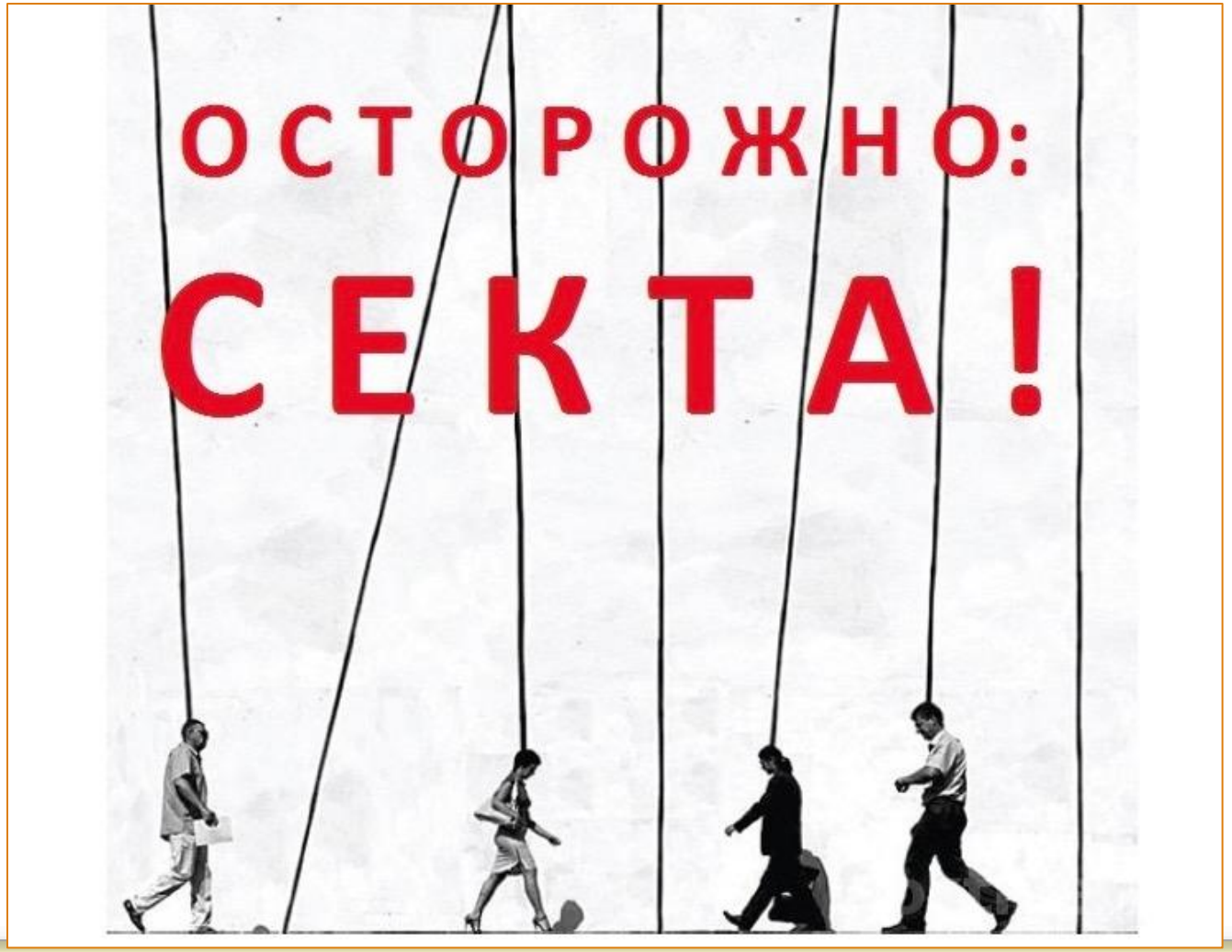
4. Фишинг - сообщения электронной почты, которые отправлены мошенниками, с целью получить ваши личные данные: номер телефона, домашний адрес, логин и пароль от вашего аккаунта, номер пластиковой карты и ПИН-код, или заманить на сайт – дублер.

Угрозы личной безопасности

5. Информация экстремистской или террористической направленности.

Угрозы личной безопасности

6. Секты и оккультные организации.



Угрозы личной безопасности

7. Мошенничество с пластиковыми картами.

Угрозы личной безопасности

8. Телефонные мошенники.

Угрозы безопасности компьютера

1. Вредоносное программное обеспечение - специально созданное программное обеспечение, чтобы причинить вред компьютеру или серверу, к такому ПО относятся программы – «трояны», сетевой червь, компьютерный вирус.

Угрозы безопасности компьютера

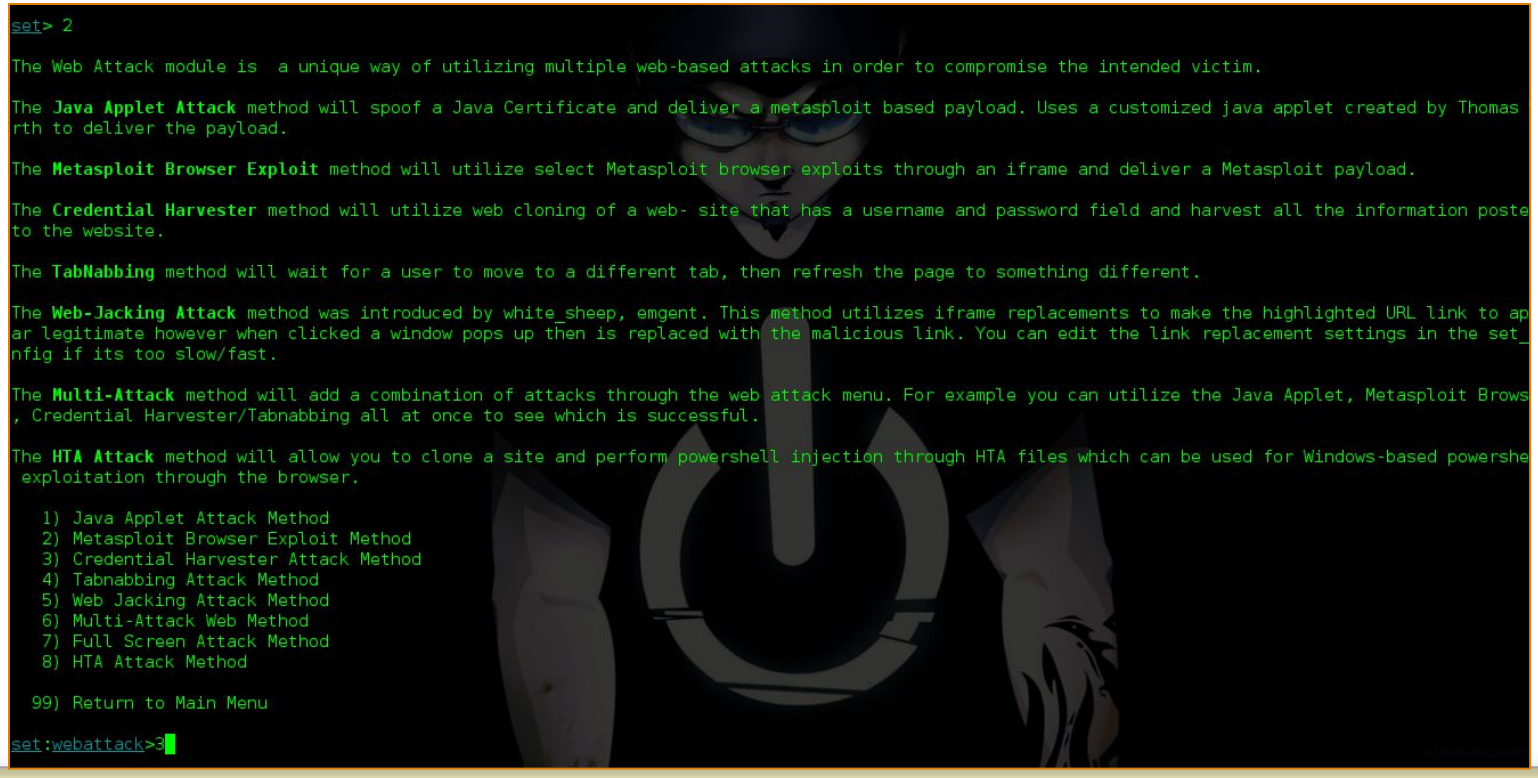
2. Рекламное программное обеспечение - нежелательное ПО, содержащее рекламу, которое также собирает информацию о компьютере и пользователе с целью проведения рекламных акции.

Угрозы безопасности компьютера

3. Шпионское программное обеспечение - это несанкционированно установленный программный продукт, целью которого является скрытое отслеживание поведения пользователя в сети.

Угрозы безопасности компьютера

4. Браузерный эксплойт - это форма вредоносного кода, которая использует уязвимость в браузере или компоненты системы, с целью изменить настройки пользователя сети Интернет.



Будьте осторожны на просторах Интернета!