

Угрозы в сети Интернет



Классификация угроз при работе в сети Интернет



Угрозы личной безопасности

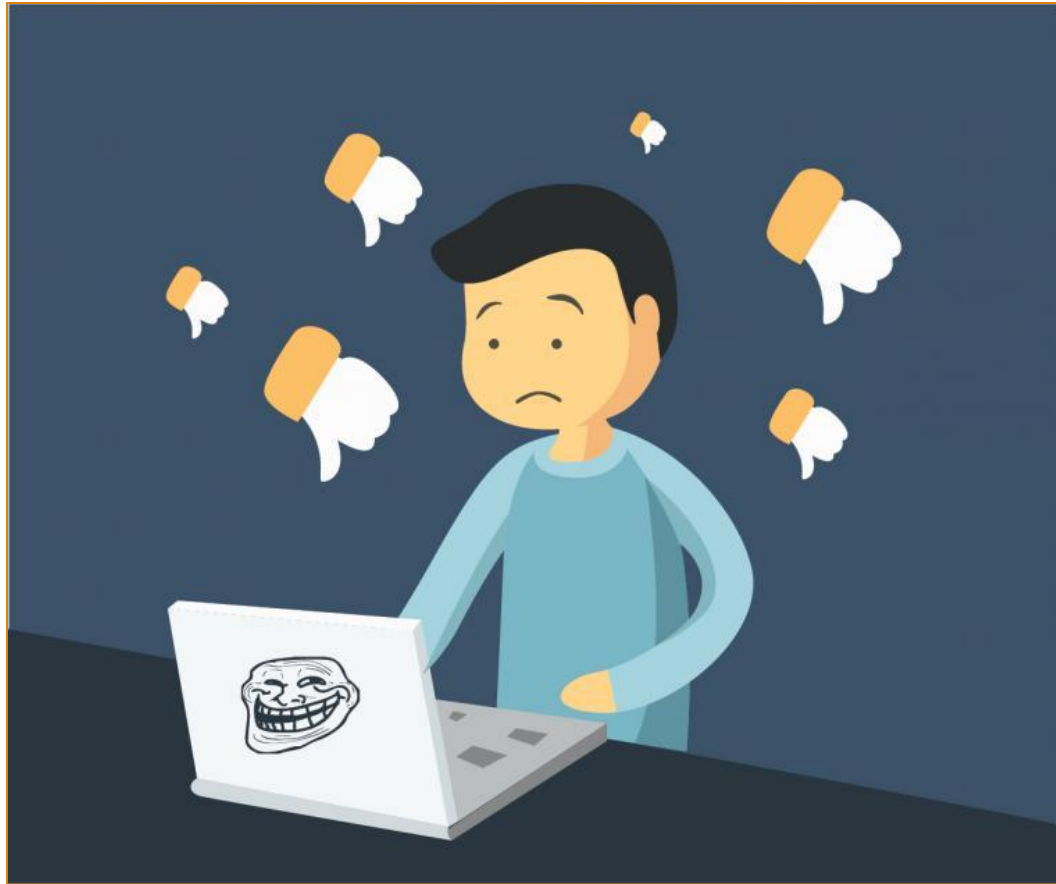


Угрозы безопасности компьютера



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.



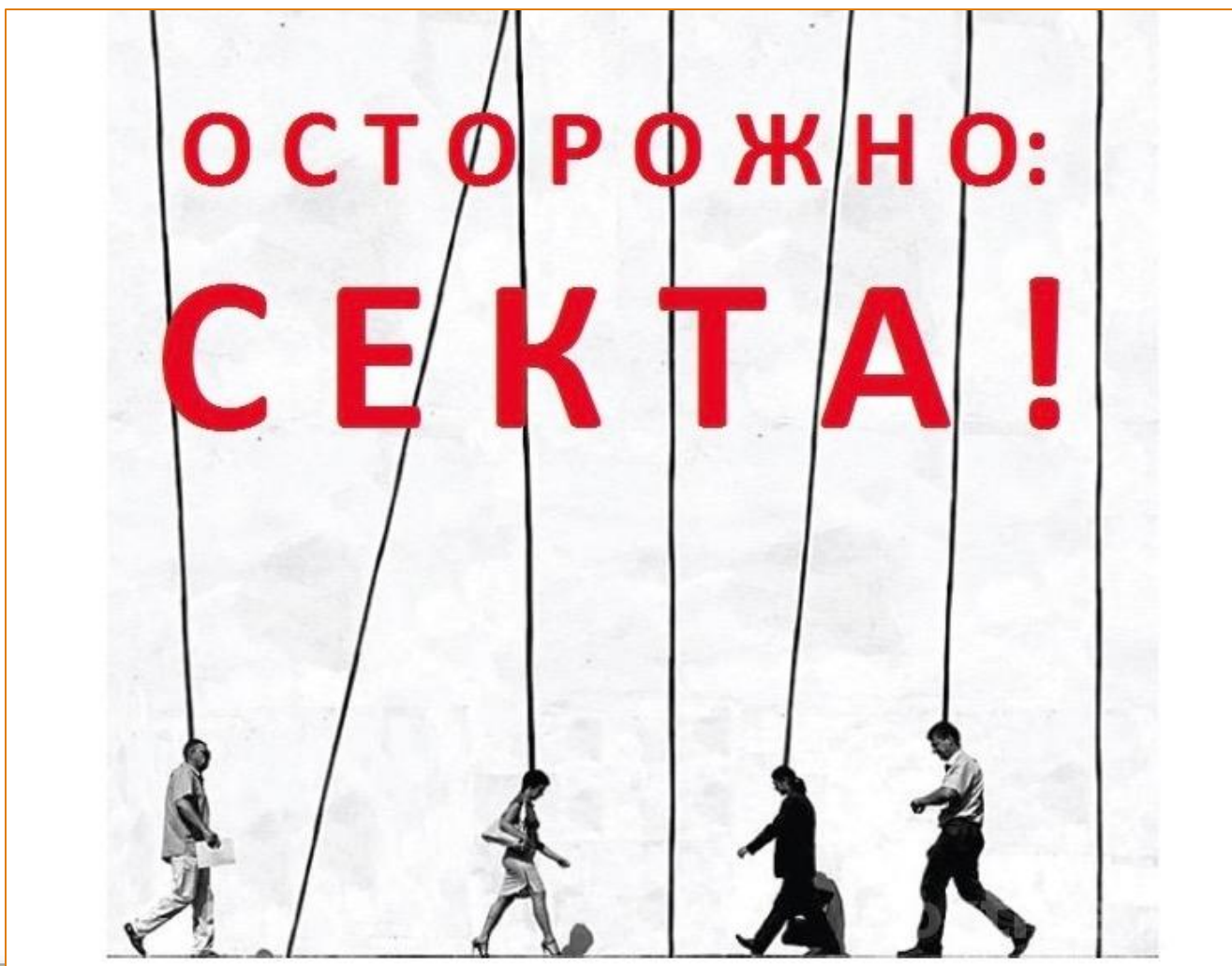
Угрозы личной безопасности

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.

```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas rth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_nfig if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser Exploit, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

**Будьте осторожны на просторах
Интернета!**

