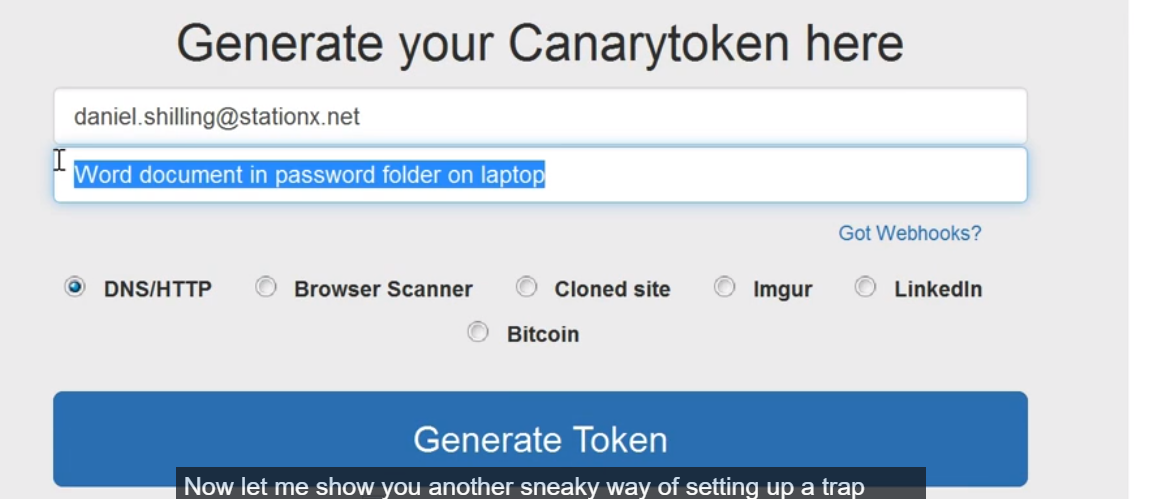
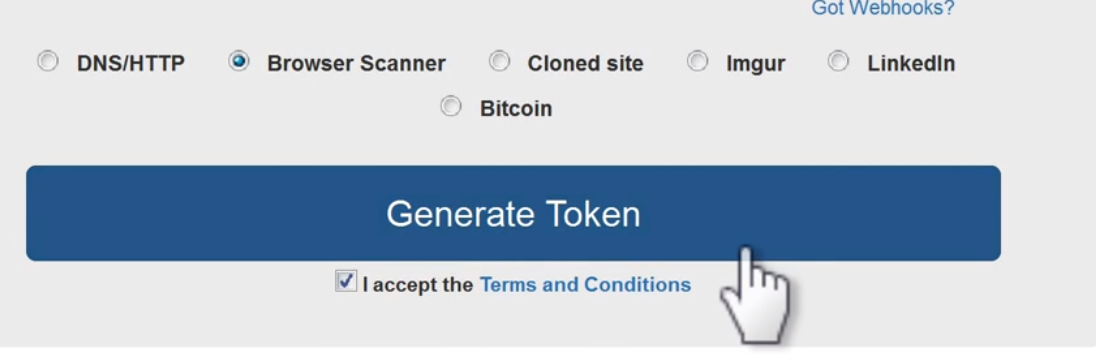
Hacking

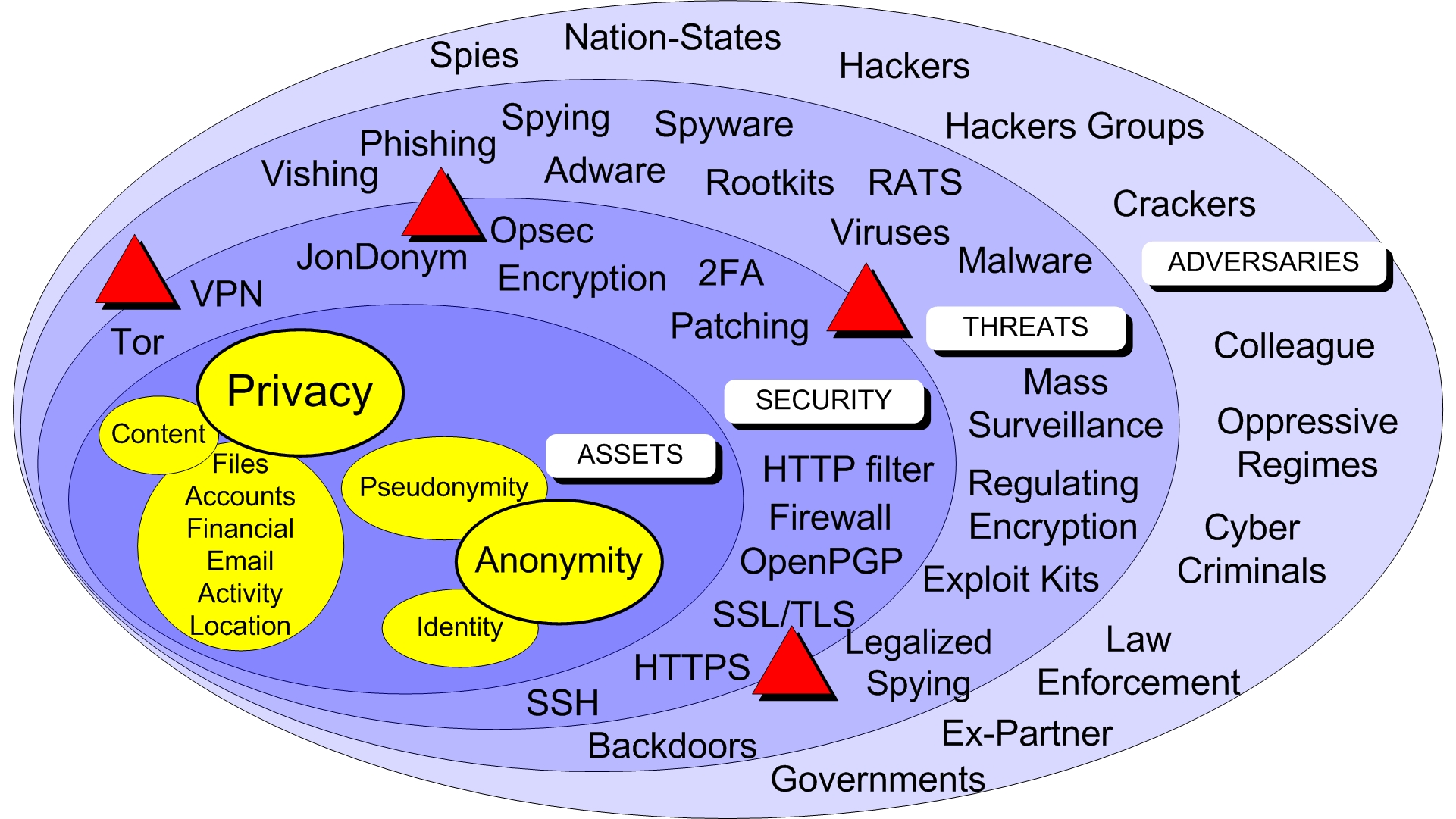
[www.stationx.net/canarytokens/](http://www.stationx.net/canarytokens/)

**Je gebruikt je eigen email waar je de melding gaat krijgen.**

om een melding te krijgen als iemand in je pc komt of iemand zoekt je gegevens en die zit in een document en die document kan je ook beveiligen als iemand het bestand open maakt kan je diegene de ip adres vinden. Je vinkt dan **dns/http**.

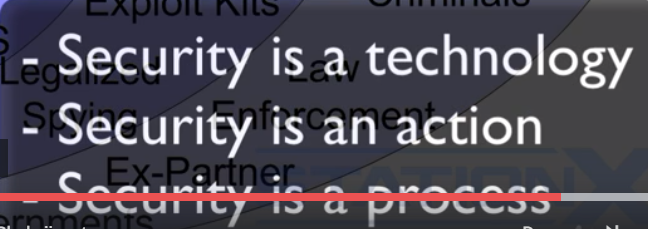
Als je een email stuurt naar iemand kan je ook de ip adres vinden. Dan vink je de **Browser Scanner.** E**n** dan klikt je op **WEB BUGS.** Je kan dan een email sturen naar iemand en als diegene de mail opent krijg je de gegevens van de persoon.

**Thunderbird** software is een email programma.

**Pseudonymity**: wat 'valse naam' betekent, is een vermomde identiteit. Dat wil zeggen een of meer menselijke wezens die wel eigenaar zijn van , maar hun echte namen niet bekend maken. De meeste houders van pseudoniemen gebruiken pseudoniemen omdat ze anoniem willen blijven , maar anonimiteit is moeilijk te bereiken en is vaak beladen met juridische kwesties.

**Anonymity:** Bij informeel gebruik wordt 'anoniem' gebruikt om situaties te beschrijven waarin de naam van de persoon niet bekend is. Het belangrijke idee hier is dat iemand niet-identificeerbaar, onbereikbaar of niet-traceerbaar is.

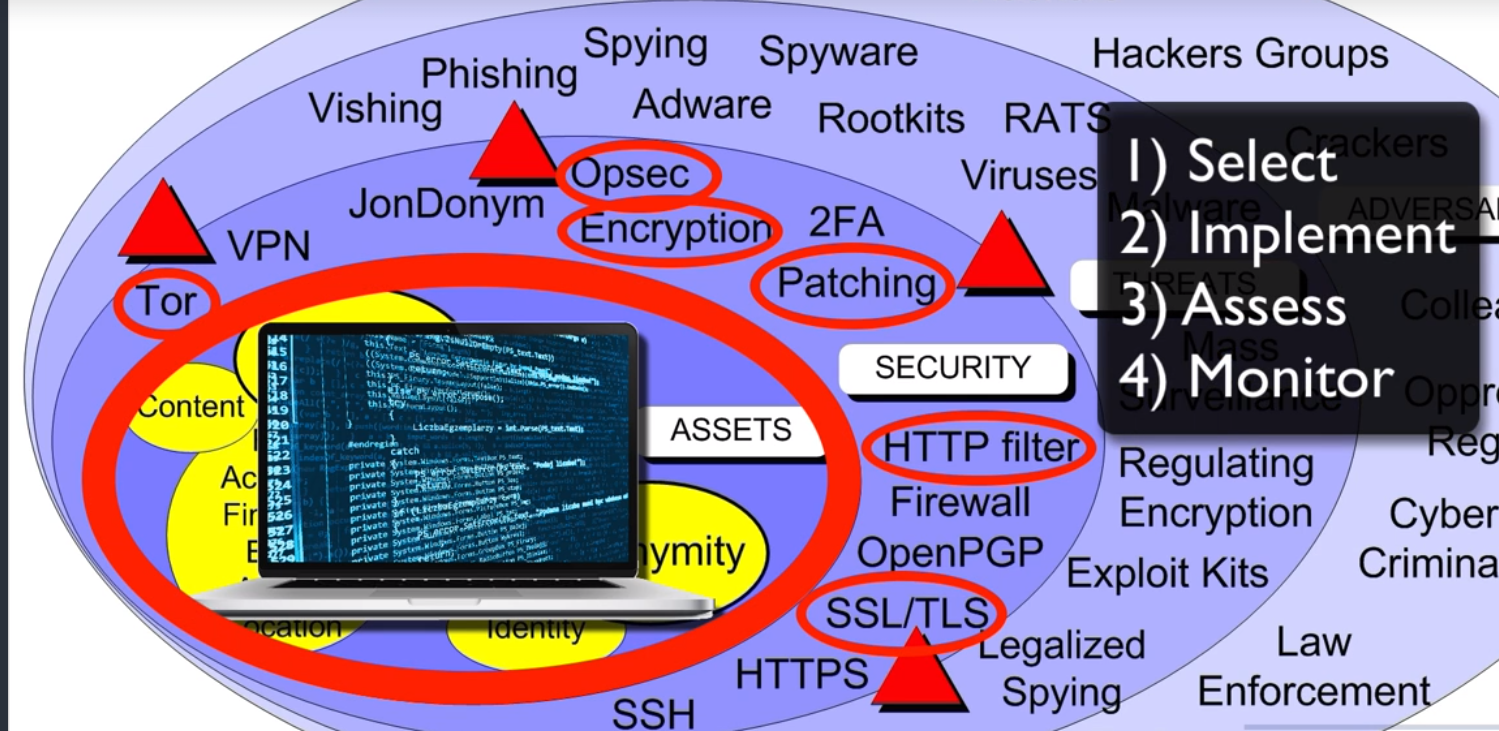
**risk = threat x vulnerability x consequence**



**De Parkerian hexad** is een set van zes elementen van informatiebeveiliging.

de drie klassieke beveiligingsattributen van de **CIA-triade (vertrouwelijkheid, integriteit, beschikbaarheid).**

**De Parkerian Hexad-kenmerken** zijn de volgende:

* Vertrouwelijkheid
* Bezit of controle
* Integriteit
* echtheid
* Beschikbaarheid
* Nut

**Vertrouwelijkheid** verwijst naar grenzen aan wie welke informatie kan krijgen.

**Bezit of controle**: stel dat een dief een verzegelde enveloppe met een bankpas en zijn persoonlijk identificatienummer zou stelen . Zelfs als de dief die envelop niet heeft geopend, is het redelijk dat het slachtoffer zich zorgen maakt dat de dief dit op elk moment kan doen. Die situatie illustreert het verlies van controle over of het bezit van informatie, maar houdt geen schending van de vertrouwelijkheid in.

**Integriteit** verwijst naar correct zijn of consistent zijn met de beoogde informatiestatus.

**Authenticiteit** verwijst naar de juistheid van de claim van oorsprong of het auteurschap van de informatie.

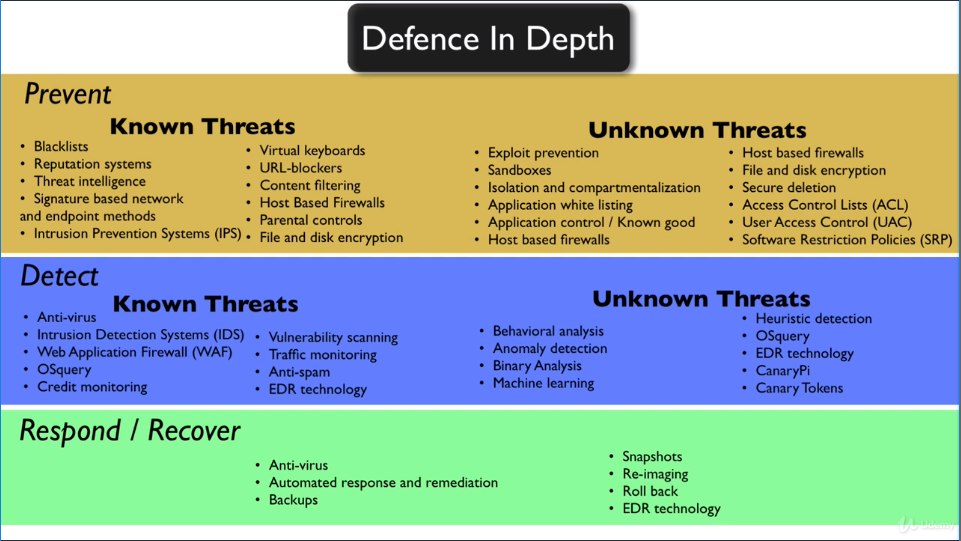
**Beschikbaarheid** betekent tijdige toegang tot informatie.

**Nut** betekent bruikbaarheid.

**Authentication** de identiteit van een persoon of ding bevestigt, is authenticatie het proces van het daadwerkelijk bevestigen van die identiteit.

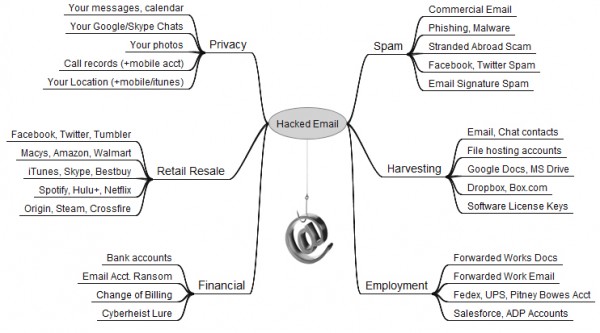
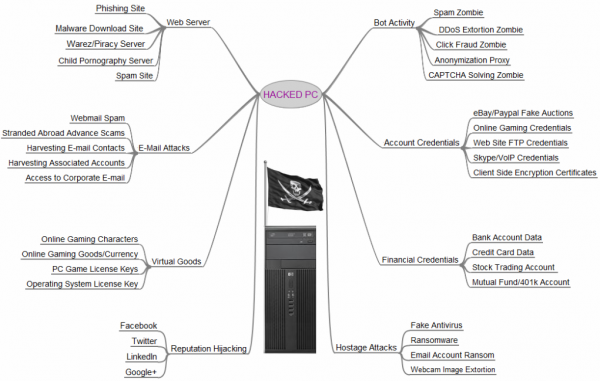
**Authorization** is de functie om toegangsrechten / privileges te specificeren voor bronnen met betrekking tot informatiebeveiliging en computerbeveiliging in het algemeen en voor toegangscontrole in het bijzonder. [1] Formeler is "autoriseren" om een ​​toegangsbeleid te definiëren.

Er zijn 3 type van defensie **Defense in depth = prevention l detection l recovery**.

**Prevention:** defense to stop people compromising those files and accessing confidential information.

**Detection:** could be you set up something called the canary which is planting a deliberate trap so that a hacker or malware triggers this canary or trap so you are notified that something is amiss.

Recovery: is like back-up or having a ability to recover a lost file or lost account.



EK landscape map software

**Exploit database** je kan hier allemaal dingen downloaden om te kunnen hacken.

**Malware:**

**Macro virus:** is written in a macro language such as the Abs. the programs may be run automatically when that document is open.

**Stealth virus:** hides the modifications is made virus tries to trick ant-virus. Its request to the os and providing false some bogus information.

**Polymorphic viruses:** copies of itself.

**Self-garbling virus:** to hide from anti-virus software by modifying its code.

**Bot or zombie**:

**Worms:** spread from one machine to another to another to another.

**Rootkits:** worst software based malware that you can get. They can hide and go in the kernel of the OS.

**Firmware rootkit:** these are the worst of all. Your hard drives firmware chip you could have some of malware even formatting. Or reinstall the OS won’t shift it.

**Keyloggers**: they find your passwords etc.

**Trojan horses**: simply programs that appear to be one thing but are actually also malware.

**Rats**: these are programs that run on your system and allow to access your system remotely. Like TeamViewer.

**Ransomware**: take your pc.

**Fishing** as a type of attack that typically attempts to trick the victim into clicking on a link or executing. Most successful.

**Phishing** is by sending fake emails or instant messages.

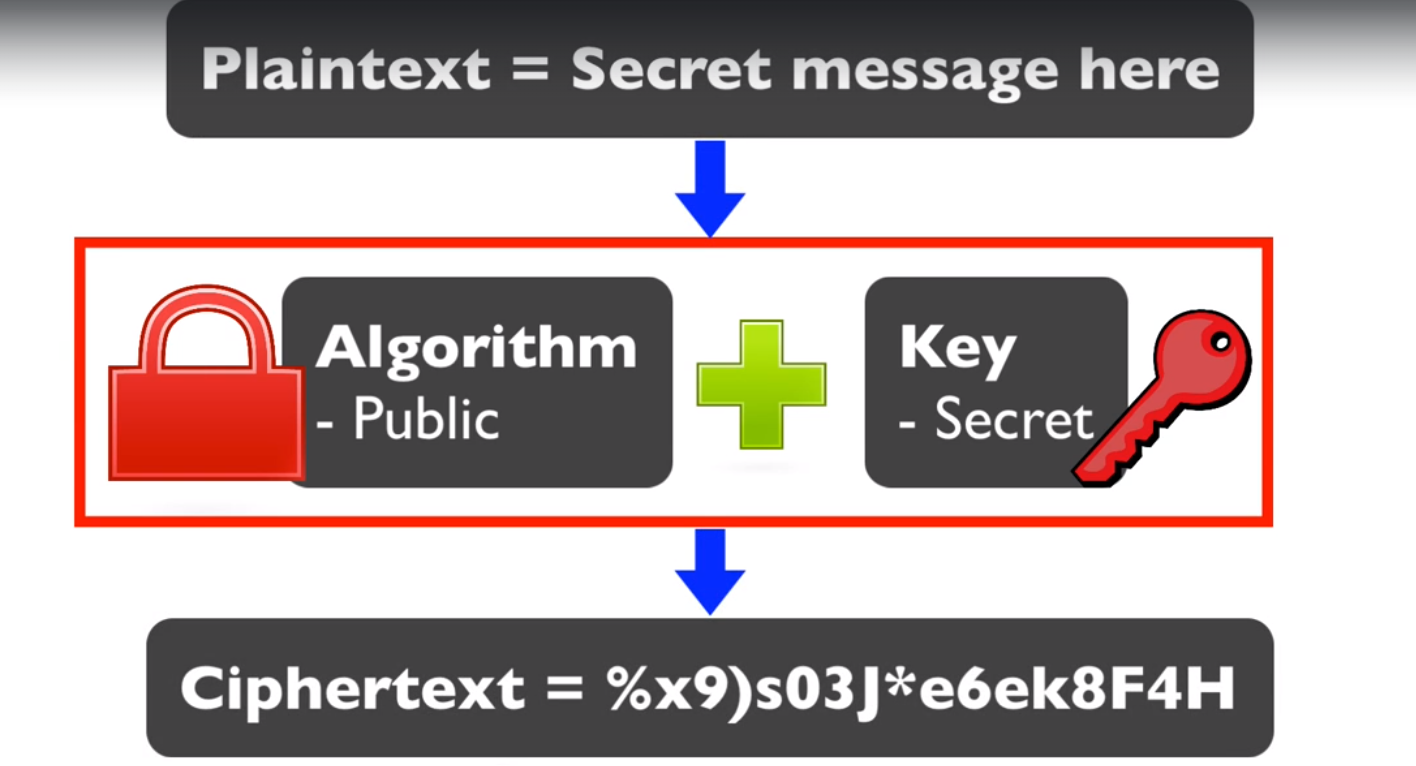
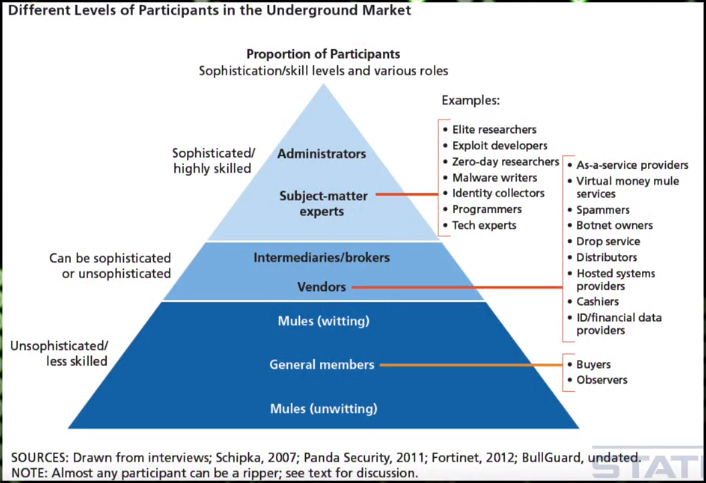
**Real domain** = the domain name to the left of the HLD that has no / to the left.(not including http://)

**Sperm** is unsolicited messages coming in e-mail.

**Doxing** is to research on an individual or it can be an organization or company to find personal and private information.

The darknet: tor.

https://wikileaks.org/-Leaks-.html



AES = symmetrix encryption Alogorithms (uses 1 key)

256 or 128 = bit length & key space.

**symmetrix encryption Alogorithms:**

* Data encryption standard (DES)
* Triple-DES (3DES)
* Blowfish
* RC4
* RC5
* RC6
* Advanced Encryption Standard (AES)

Asymmetric = 2 keys (public & private)

Symmetric = 1 key (private)

Examples of asymmetric keys is:

* RSA
* ECC
* DH
* El Gamal

Asymmetric

* Better key distribution
* Scalability
* Authentication and nonrepudiation
* Slow
* Mathematically

Symmetric

* Fast
* Strong