د آنلاین فعالیت خوندیتوب

د زده کړې د یادولو هدف په آنلاین بڼه د خپلو فعالیتونو ساتنه ده

- د براوزر (Browser) او https د اهمیت په اړه
- د وي پي این VPN او تور Tor په اړه

تاسو به حتمآ تراوسه د https اصلاح په هکله اوریدلي وي ایا پوهیږئ چې معنی یې څه ده؟

ایا پوهیږئ چې د دغه اینټرنیټي * پروتوکول په پای کې د S د توري زیاتول څه معنی ورکوي

- ایا د هغې د جوړونکي په نوم یعنی د **S**afran شرکت دی؟
- ایا په انګلیسي ژبه کې جمع نوم شته دی؟
- ایا **د** Secure یا خوندیوب په معنی دی؟

په خوندي ډول د (HTTPS) پروتوکول (Hypertext Transfer) د HTTP او SSL یو ترکیبي پروتوکول دی. هدف یې د رمزي خوندي اړیکو برابرول او د یو خوندي دلال په توګه د ویب پیژندل دي.

ستاسو د خبرتیا لپاره :

[د پروتوکول (Hypertext Transfer) انتقال چې اختصار یې ایچ ټي ټي پي (http) کیږي یو پروتوکول یا یو ارتباطي تړون دی چې د معلوماتو د انتقال او تبادلې لپاره په ویب کې ورڅخه کار اخیستل کیږي. له دغه پروتوکول څخه د اسنادو د پیوند لپاره چې په نورو اسنادو کې پرې استناد شوی وي کار اخیستل کیږي].

د SSL مخفف Secure Socket Layer په "خوندی ډول د طبقی نښلولو" په معنی دی چی پروتوکول(قوانینو مجموعه) ده چی په اینټرنیټ کې د خدماتو د وړاندې کوونکي اود خدماتو ترلاسه کوونکي ترمنځ خوندي اړیکې ټینګیدوي.

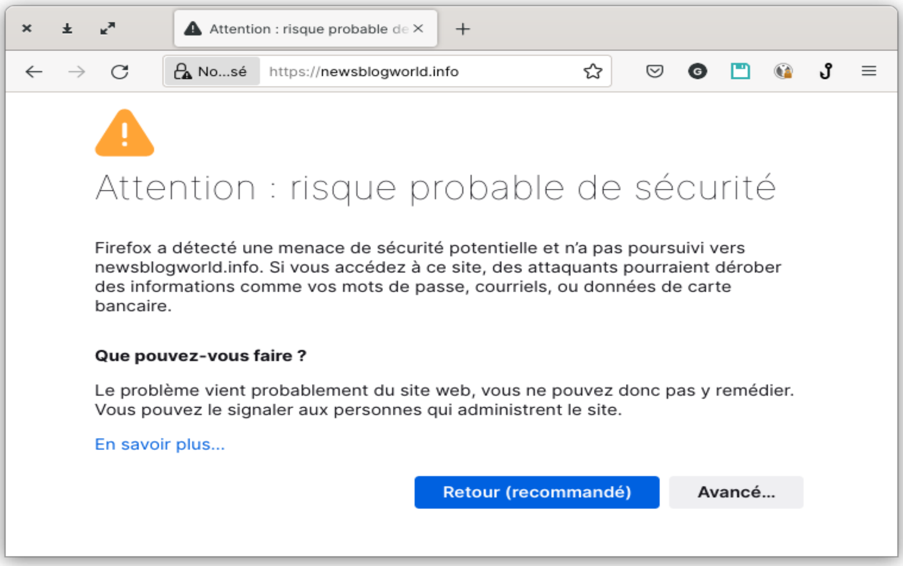
کله چې د (URL) په اینټرنیټي ادرس د یو ویب سایټ په https باندې پیلیږي، کولی شو له دري مهمو نکتو ډاډ ولرو:

۱- د ویب سایټ واقعي اعتبار: د https په پروتوکول کې هر ویب سایټ د یوامنیتي یا خوندي تصدیق (certificate) لرونکی دی، کله چې ورته لاس رسی پیدا کوئ ستاسو د اینټر نیټي پاڼې په براوزر (Browser) کې ښودل کیږي. ستاسو براوزر (Browser) د ډاټا یو مرکز(Database) لرونکی دی چې د اعتبار د تصدیق د ارزولو امکان لري.دا تصدیق د یو ویب سایټ د پیژندلو د کارت معادل دی او د هر ویب سایټ لپاره https په یو ډول کاراخیستل کیږي.

۲- د معلوماتو یا ډاټا محرمیت: ستاسو د براوزر (Browser) او د لیدونکي ویب سایټ ترمنځ مختلف اتصالات وجود لري؛ د اینټرنیټي خدمتونو د چمتو کوونکي، سرور server یا سرورنو servers اود پراسکیز (Proxies) شتون احتمال شته دی، حتی د ښه نیت نلرونکي شخص پورې (په ځانګړي ډول د عمومي واي فایې " WIFI" اینټرنیټ سره دنښلیدو پر مهال). خو د ویب سایټ د اعتبار د تصدیق وروسته یو رمز لرونکي ارتباطي کانال ستاسو د براوزر (Browser) او یب سایټ ترمنځ رامنځ ته کیږي ترڅو دا ډاډ ترلاسه شي چې ستاسو او د ویب سایټ د نښلولو ترمنځ هیڅ لیدونکی نشي کولی د غوښتل شوي پاڼې په څېړون تاسو ته د انتقالیدونکو معلوماتو د محتوا څخه یا د استوونکو عبوري رمزونو ته لاس رسی پیدا کړي.

۳- د معلوماتو او د ډاټا ربښتونالی: د https پروتوکول څخه کار اخیستل همداشان دا تضمینوي چې هیڅوک نشي کولی استول شوي معلومات بدل کړي.

د https د خطر خبرداری

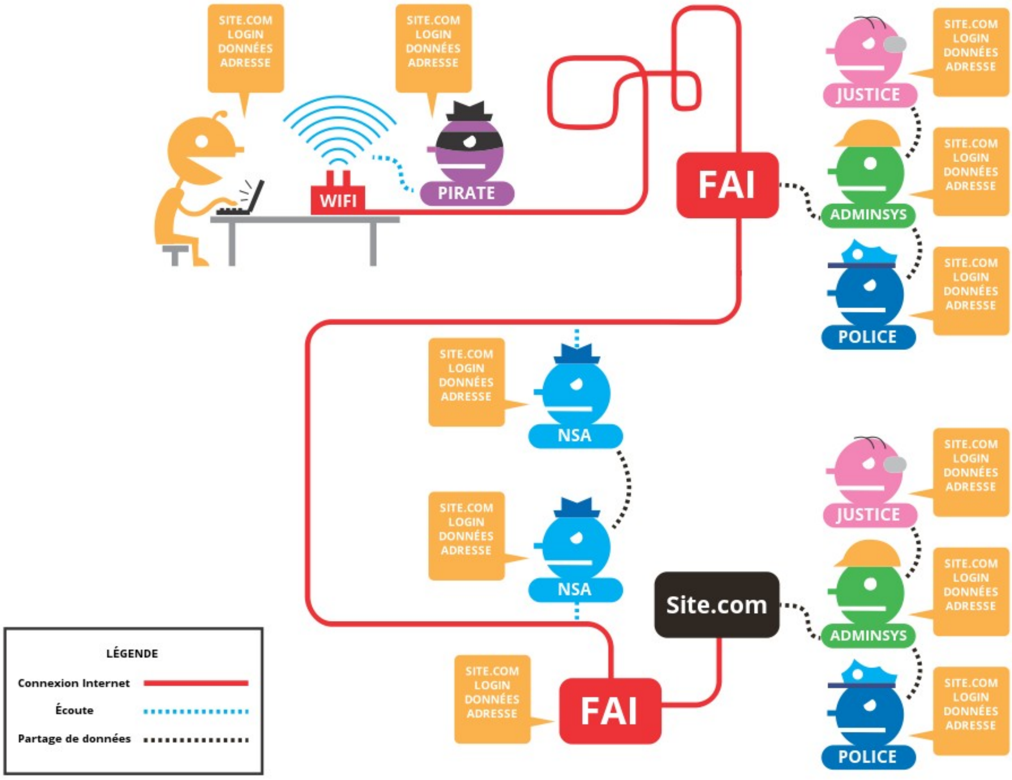


د HTTPS خبرداری

که چیرې دا خبرداری په کوم ویب سایټ کې چې ورځخه لیدنه کوئ وکتل شي، په دې معنی دی چې ستاسو براوزر (Browser) د ویب سایټ د واقعي هویت څخه د ډاډ د ترلاسه کولو وړنه دی. دا خبرداری دا ښیي چې د HTTPS ویب سایټ تصدیق معتبر نه دی او براوزر (

(Browser) تاسو ته امنيتي خبرداری درکوي:" زه نشم کولی ددی ویب سایټ هویت تائید کړم، امکان لري یوه غلوونکې کاپي اوسي".

په عین حال کې د ناامنه (غیرخوندي) د خطر نښلیدو باندي پوهیدو سره تاسو کولی شئ هڅي ته لاس ږسی پیدا کړئ. ددي له امله چې د ویب سایټ هویت مشخص نه دی، ستاسو د کمپیوټر او یا د ځیرک تیلیفون ترمنځ اړیکه او د ویب سایټ ترمنځ خوندي نه ده او **د اینټرنیټ له لاري چې ستاسو د وسیلي (کمپیوټر یا ځیرک تیلیفون) او ویب سایټ ترمنځ ټول معلومات حرکت کوي په رمزي بڼه نه دي بدل شوي،**



د HTTPS د براوزر (Browser) څخه کار اخیستل

په سم ډول د HTTPS له کارولو څخه د ډاډ لپاره د خپل د براوزر (Browser) لاندي پړاونه تعقیب کړئ:

• د Firefox، IE Edge یا Chrome له براوزرونو (Browsers) څخه کارواخلئ.

• پلاګین "Plugin" (یو سوفټ ویر دی چې د کمپیوټر د پروګرامونو قابلیت زیاتولی شي) Duck Duck Go Privacy Essentials د Firefox یا Chrome پرمخ نصب کړئ.

• د Android یا iOS، څخه د کار اخیستني لپاره د Duck Duck Privacy Browser براوزر (Browser) څخه کار واخلئ.

تمرین:

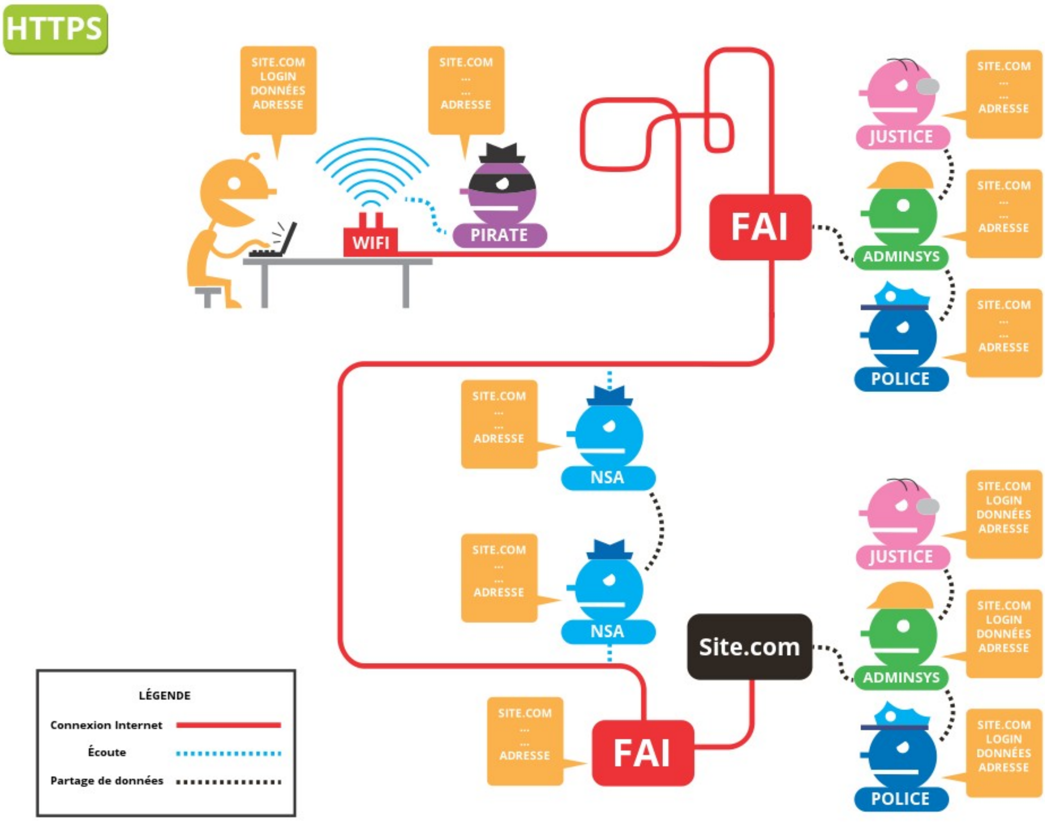
1. د Duck Duck Go Privacy Essentials پلاګین "Plugin" د Firefox یا Chrome پرمخ نصب کړئ

2. د پلاګین "Plugin" له نصبولو وروسته " 🔒 " په بټنه باندې کلیک وکړئ ترڅو د نښلیدو له بهیر څخه ډاډ ترلاسه کړئ چې اتصال خوندي دی او کوم دریمګړی ویب سایټونه بند شوی دی.

کومې ډاټا (Datas) کیدای شي وڅارل شي او ضبط شي

د HTTPS څخه کار اخیستل تاسو پورې تړاو نلري، بلکې د ویب سایټ پورې چې تاسو یې د لیدلو په حال کې یاست تړاو او مطابقت لري. که څه هم ډیر ویب سایټونه امنیتي تصدیقونه یا نسخې وړاندې کوي، دا موضوع په ټولو مواردو کې صدق نه کوي. نږدې ۲۰٪ ویب سایټونه امنیتي تصدیقونه یا نسخې نه وړاندې کوي.

HTTPS تاسو اود هغه ویب سایټ څخه چې لیدنه کوئ ترمنځ اړیکې خوندي کوي، خو په ویب سایټ کې ستاسو د براوزر (Browser) د امانتدارۍ تضمین نه کوي. د کومو ویب سایټونو څخه چې لیدنې کوئ د هغوی د لمنو نومونه همداشان د اینټرنیټ د خدمتونو د وړاندې کوونکي له خوا (FAI)، د کار ګمارونکي یا د اینټرنیټ د کافي (Internet cafe)څخه چې تاسو یې د انیټرنیټ څخه کار اخلئ لیدل کیدلی شي.

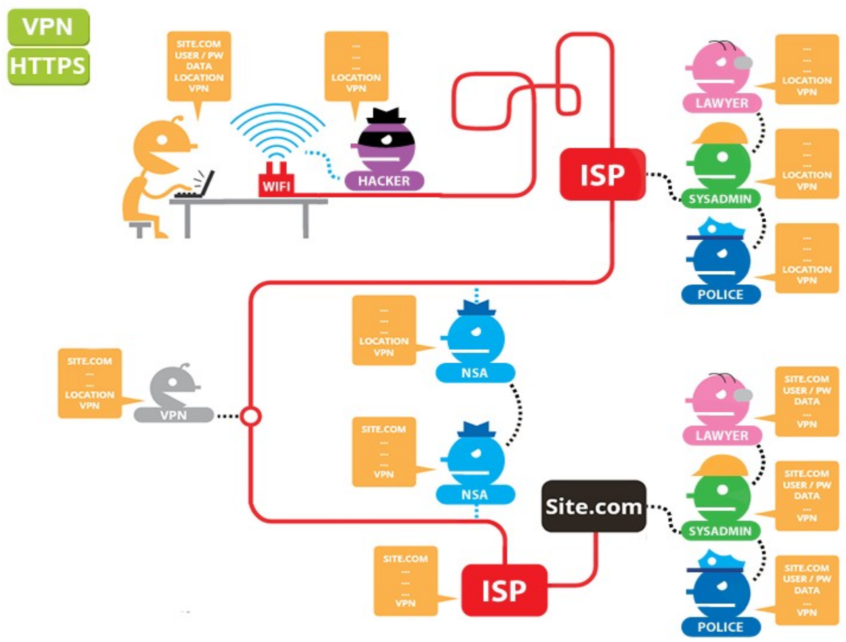


د نښلیدو (اتصال) ساتنې لپاره VPN څخه کار اخیستل

وي پي این (VPN) یو سوفټ ویر دی چې تاسو ته ددې امکان درکوي چې ستاسود کمپیوټراو یا ځیرک تیلیفون او د یو سرور (Server) ترمنځ یو خوندي تونل په هره نقطه کې چې کولی شي اوسي (بڼه ده چې په یو هیواد کې چې اینټرنیټ نه سانسوریږي او نه کنټرولیږي) رامنځ ته کړئ.

دغه سوفټ ویرتاسو ته دا امکان درکوي چې د فیلټرینګ او د بندیدو څخه تیر شئ. ددغه تونل له لارې تېولې استول شوې ډاټا (Datas) رمز بانديې بدلیږي. دا د وي پي این "VPN " کارونکو ته داډ ورکوي چې ستاسو د کمپیوټر او د وي پي این "VPN " د سرور ترمنځ د کومې تخریبي لاس وهنې په صورت کې (جاسوسي، تجاوز او نور) دغې ډاټا ته دریيمګړي کسان لاس رسی نلري.

ددې سربیره چې وي پي این "VPN " له سانسور څخه د تیریدو امکان برابروي، ستاسو د کمپیوټر ټول خروجي اتصالاتو ساتنه هم کوي، همداشان ستاسو پر اینټرنیټ کې ستاسو حرکت، ستاسو د ایمیل د وړاندې کوونکې سره نښلیدل، د وریځو د خدمتونو (Cloud Services) فایلونو ته لاس رسی اونور، ستاسو ټول اینټرنیټي ترافیک د وي پي این "VPN " له خوا د رامنځ ته شوې تونل له لارې حرکت کوي او د همدې له امله ننجکاوان په رښتو رښتو سترګو په عمومي ځایونو کې تاسو ته د واي فای اینټرنیټ (WIFI) د خدمتونو وړاندې کوونکې او یا په هربل ممکن پړاو کې د یو دریيمګړې فرد په بڼه د لاس رسي وړ به نه وي. ستاسو د اینټرنیټ ترافیک رمز په بڼه جوړ شوي ترڅو وي پي این "VPN " او ددې سرور(Server) له خوا رمز (Code) پرانیستل شي.



د وي پي این "VPN " براوزر (Browser) څخه کار اخیستنه

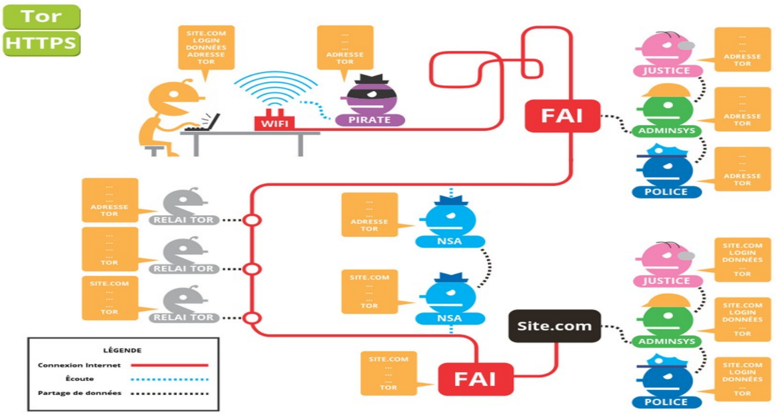
تمرین:

1. د VPN Nothing2Hide سوفټ ویر د خپل کمپیوټر او ځیرک تیلیفون پرمخ نصب کړئ او لاندې لارښوونې له مخې دوام ورکړئ

2. د نصبولو لارښود
د نصبولو لارښود ترجمه شي

2. https://www.whatismyip.net/ ته مراجعه وکړئ.

3. VPN فعال کړئ او https://www.whatismyip.net/ ته ستانه شي او پایلې یې مقایسه کړئ.



د Tor براوزر څخه په کار اخیستنې د نښلیدو (اتصال) او هویت څخه ساتنه

که چیرې ستاسو اینټرنیټي ټرافیک د وي پي این VPN پراساس په رمز (Encryption) بدل شي، دا په دې معنی نه دي چې پیژندل شوي نه یاست. حتي په یو VPN، سره تاسو په انلاین کې خپلې زیاتې نښې له ځان څخه پریږدئ او د "آی پي" IP ادرس یا(Internet Protocol Address) ستاسو د لاس د ډیجیټلي ګوتې پیژندګلوي کوي.

د AmIUnique ویب سایټ تاسوته په آنلاین بڼه د پیژندګلوئ د قابلیت د ازمایښت امکان درکوي.

ددې سربیره د انلاین کیدو پر مهال د ناپیژندلي په توګه د پاتې کیدو د پیاوړتیا لپاره د Tor براوزر څخه کار واخلئ. د Tor براوزرهڅه کوي ټول کارونکو ته په یوه سترګه وګوري، ترڅو ستاسو لیدنه (مشاهده) او تعقیب یو شخص پورې د اړوند ګوتې ډیجټلي نښې معلومول د براوزراو ستاسو د کمپیوټر یا ځیرک تیلیفون معلومات لا سخت شي.

ددې سربیره برخلاف له دې چې VPN ممکن د VPN مدیردی هممهاله په دې پوه شي چې له کوم ځای له کوم ځای سره نښلول کیږي او دا ډول په ناپیژندلي ډول ستاسو پاتې کیدل تر ګواښ لاندې راولي، Tor په شبکه کې ناپیژندلي پاتې کیدو ته اجازه نه ورکوي چې د یو اینټرنیټي نښلولو یا اتصال نقطه، مبدا او هدف وګڼل شي.

که چیرې یو څوک ستاسو د سیاحت پر عادتونو باندې د اینټرنیټ له لارې څارنه وکړي یوازې کولی شي چې دا وګوري چې تاسو د Tor له براوزر څخه کار اخلئ.

Tor یا یو VPN تاسو د تل لپاره په بشپړ ډول یو ناپیژاند په توګه نه ساتي. د مثال په توګه کله چې د یو VPN یا Tor سره د خپل فیسبوک له لارې په خپل نوم یا د کورنۍ په نوم نښلول کیږئ دا ستاسو د ناپیژند کیدو څخه د سرغړونې په معنی ده.

Tor د کمپیوټر، وینډوز، مک، لینوکس،انډروید او آیفون پرمخ د لاس رسي وړ دی.

تمرین:

1. Tor ددغه لینک له لارې https://www.torproject.org/fa/download/ نصب کړئ.

2. amiunique.org ته د Tor له لارې د خپل ورځیني براوزر ته ورشئ او پایلې یې وارزوئ.

3. د https://www.iplocation.net/find-ip-address ځخه په استفادې د Tor له لارې خپل ورځیني براوزرونو ته ورشئ او پایلې یې وارزوئ.

4. د آیکون پرمخ د پټۍ د چپ اړخ په ادرس باندې کلیک وکړئ او Tor مسیر وارزوئ.

5. د آیکون پر پاڼې کلیک وکړئ او د اوسنۍ غونډې (session) ټوله ډاټا پاکې کړئ او یوه نوې غونډه (session) پیل کړئ.

د نورو زیاتو ګامونو پورته کولو لپاره:

- د یو حمل وړ عامل سیستم ځخه په ځانګړي ډول د خپل خصوصي حریم د ساتنې لپاره کار واخلئ: Tails.
- د Totem آنلاین در مورد دور زدن سانسور کورس (په فارسی ژبه) تعقیب کړئ.