د شمیرونو ډیجیټلي امنیت (خوندیوب) بنسټونه

د زده کړې هدف: د ډاټا د امنیت (خوندیتوب)او دآنلین حسابونو اود کار د وسایلو د ساتنې زده کړه

هروخت او په هرځای کې د خپلې ډاټا د ساتلو هڅه، ستومانوونکې او ډیره عملي نه ده. امنیت یو بهیر دی، چې یوازې په وسایلو اوڈ سافټ ویرونود باړولو(نصبولو یا loading) نشي خلاصه کیدلی. امنیت له هغو ګواښونو څخه په درک چې ورسره مخ کیږئ او پر وړاندې یې چې کوم میتودونه غوره کوئ پیلیږي.

د ګواښونو ډولونه

د ګواښونو د کتنې لپاره باید پنځه پوښتنې له خپل ځان څخه وپوښتو:

۱- کوم معلومات باید وساتو ؟

۲- دا معلومات د کومو کسانو لپاره په زړه پورې/ مهم دي؟

۳- دغو معلوماتو ته د لاس رسي لپاره د کومو وسایلو څخه کار واخیستل شي ؟

۴- دغو معلوماتو ته د لاس رسي پایلې څه دي؟

۵- له کومو وسایلو کولی شو کار واخلو؟

له کومو معلوماتو باید ساتنه وکړو

ایمیلونه، خبرې، تیلیفوني مکالمې، عکسونه، فلمونه، ادرسونه، هویت اود تماس لرونکو مشخصات او ذې ته ورته موارد.

یادونه: په یاد باید ولرئ چې یوازې کوډ (CODE) یا رمز د پیغامونو څخه ساتنه کولی شي نه د پیغام د استوونکي اویا ذ ترلاسه کوونکي نوم.

دا معلومات د کومو کسانو لپاره جالب / مهم دي؟

- سازمانونه یا هغه کسان چې مقاله کې یې غوښتنه شوې
- یو دولت
- یو قاضي یا پولیس
- یو خصوصی شرکت

معلوماتو ته د لاس رسي لپاره له کومو وسایلو ګټه اخیستلی شو؟

- فني: کتنه ،هک کول (سایبري بریدونه)
- قانوني: اوریدل، احضار
- ټولنیز: ټولنیزه مهندسي
- فیزیکي: غلا کول، د ناسمو وسایلو نصبول

دغو معلوماتو ته د لاس رسي پایلې کومې دي؟

- موضوع افشا کیدل/ د خپرولو له لارې د معلوماتو سوزول
- حقوقي مشکلات/ عدلي د یوې منبع لپاره
- فیزیکي ګواښونه

زه له کومو وسایلو کولی شم کار واخلم؟

• تخنیکي

• حقوقي عدلي

د فشینګي بریدونو څخه ساتنه

فشینګ (Phishing) څه شی دی؟ لاره وهوونکی یا مهاجم د ایمیل له لارې یوه هیله "طعمه" (لومه کې د نښلیدو لپاره) استوي. دا طعمه دا شخص هڅوي ترڅو خپله محرمه ډاټا خپره کړي.

پر کمپیوټر باندې د ویروس ضد د یو سوفټ ویر نصبول یو ښه مهم اقدام دی، خو همدارنګه دا هم مهمه ده چې د لینک ترلاسه کولو یا د ایمیل سره غوټه شوی فایل د ترلاسه کولو پر مهال چې د ایمیل، مسنجر، پیغام، سکایپ او د اړیکو نیولو د نورو وسایلو له لارې استول کیږي خپله لازمه هوښیاري وښیوو. ټولنیزې شبکې او د هغوی اړوند وسایل د ویروسونو د انتقال اصلي عامل ګڼل کیږي.

په ویروس د ککړو پیغامونو سره د مقابلې لپاره څو اساسي سپارښتنې:

• له ناپیژاندو استوونکو څخه چې کوم فایلونه او یا لینکونه ترلاسه کوئ مه ډونلوډوئ اویا پرې کلیک مه کوئ.

• د ایمیل د استوونکي ادرس یا د استوونکي د ټویټر لینک په دقت سره وارزوئ.

• د استوونکي د هویت په اړه د شک په صورت کې د نورو مخاطبانو (دفتري همکارانو او یا د استوونکي اداري سره د اړیکو نیولو له لارې)او یا هم د لټون د نورو لارو په کارولو سره ډاډ ترلاسه کړئ.

• همداشان کولی شئ چې یو ترلاسه شوی اینټرنیټي فایل یا ادرس د آنلاین خدمتونو په کارولو لکه [Virustotal](https://www.virustotal.com) وارزوئ ترڅو ډاډ ترلاسه کړئ چې استول شوی فایل زیان لرونکی دی او که نه.

• که چیرې د کوم فایل په اړه شک لرئ په اسانۍ سره کولی شئ چې په دې برخه کې له متخصصینو سره اړیکې ونیسئ او ورڅخه مرسته وغواړئ.

څنګه کولی شو د یو malware یا ککړ سوفټ ویرلینک وپیژنو؟

تمرین : تمرین: دا لینک د چا پورې تړاو لري

/https://www.facebook.secure.com/friends

ځواب: دا لینک مونږ د فیسبوک سره نه نښلوي پرځای یې مونږ د secure.com سره نښلوي!

د URL اینټرنیټي نښې لوستل د فیشینګ اینټرنیټي برید د مخنیوي لپاره ډېر زیات مهم دي. ((/https://freedom.press/training/email-security-tips

https://fa.wikipedia.org/wiki/%D9%81%DB%8C%D8%B4%DB%8C%D9%86%DA%AF

(https://webcade.ir/view/articleid/474)

ادرس بار Address Bar

اینټرنیټ ډومین (لمن) Internet domain

URL یا اینټرنیټي ادرس

URL د Universal Resource Locator مخفف دی.

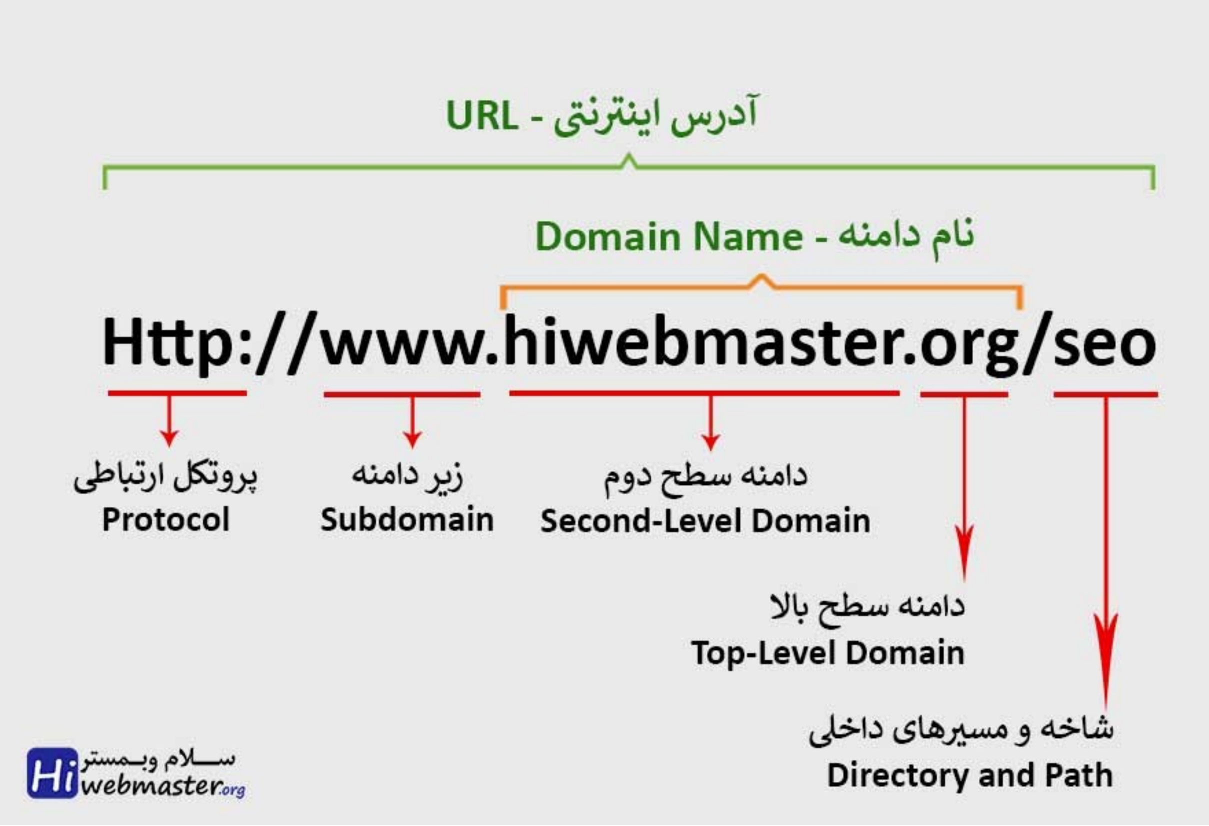
د اینټرنیټ په نړیواله فضا کې د منابعو د محل د ځانګړي کیدو لپاره په نړیواله کچه یو معیاري نښه ده

هر ادرس چې تاسو یې د ادرس لیکلو پر ځای کی یا (Address Bar) داخلوئ یو URL یا اینټرنیټي ادرس دی او **لمن (Domain) یې هم د URL برخه ده.** مثلا:

http://www.google.com

یا د همدې پاڼې ادرس URL دی :

https://hiwebmaster.org/urls



د اینټرنیټي ادرس لومړنۍ برخه د هغه پروتوکول دی، پروتوکول، معیار او قوانین دي چې دا ځانګړې کوي چې څنګه په یوه شبکه کې دننه کمپیوترونه یود بل سره او یا هم د شبکې څخه بهر د کمپیوټر سره اړیکې ټینګې کړي.

پروتوکول زیات ډولونه لري چې ترټولو مهم پروتوکولونه یې http او https ډولونه دي. دا پروتوکولونه په ادرس کې **د اړیکو د رامنځ ته کولو، ترلاسه کولو او د ډاټا په استولو کې** ورځخه کار اخیستل کیږي.

دا ادرس د کوم ځای پورې اړه لري

https://drive.google.com.downlaod-photo.sytez.net

اودا؟

http://aiju.af/about

د لا زیات پوهاوي لپاره کولی شئ دغه ادرسونه وګورئ

https://learn.totem-project.org/courses/course-v1:Totem+TP_PM_FA+001/about

https://hiwebmaster.org/urls

د خپلو انلاین کاروونکو حسابونو څخه ساتنه

ترټولو زیات د اینټرنیټي خدمتونو څخه چې مونږ کار اخلو لکه ایمیل، ټولنیزي شبکي او نوروانیټرنیټي خدمتونو څخه د **رمزي کلماتو** (PASSWORD) په واسطه ساتنه کیږي. دا ډیره مهمه ده چې ډیر قوي او سخت رمزي کلمات جوړ کړو چې پیداکول یې یا اټکل کول یې ستونزمن اوسي. کولی شئ د خپلو **رمزي کلماتو** قوي کیدل د رمزي کلماتود ارزونې [ګذرواژه ما](#) په کارونې سره په اینټرنیټي پاڼه کې nothing2hide وازمایي.

د یوې رمزي کلمي اوږدوالی د یو قوي رمزي کلماتو رامنځ ته کولو لپاره اصلي عامل ګڼل کیږي چې د یوي قهرجن څواک د برید پر وړاندې د مقاومت وړتیا لري. ددې سربیره عددونه، ځانګړې لیکنې، واړه او لوی توري، معمولاً د یوې کمزوري رمزي کلماتود رامنځ ته کیدو سبب ګرځي چې یادول یې سختیږي. که چیرې د رمزي کلماتو پر ځای د "رمزي جملې" څخه استفاده وکړئ، د یو لړاسانو کریکټرونود یادولو او په زیات اوږدوالي سره د خپلو تیرو رمزي کلماتو په نسبت به ښه رمز(Passsword) په لاس راوړئ.

Th$jHTo%46 : دغه رمزي کلمه لنډه او یادول یې هم سخت دي.

خو دغه رمزي کلمه په اسانۍ سره په ذهن کې پاتې کیږي او لاس رسی هم ورته ستونزمن دی.

د لوی او بخښوونکي خدای په نوم! زموږ زخمت کښواو ږستکاروخلکو

(کولای شئ ددغو کلمو ځینې یې په نورو ژبو پښتو یا انګلیسي ولیکئ او...).

اساسي سپارښتنې:

١- عادي رمزي کلمې هیرې کړئ او د رمزي جملو څخه کار واخلئ.

٢- هرڅومره چې ستاسو جمله زیات ټکي او علامې ولري د پیژندلو امکان یې ډیر کم دی.

٣- د فیلمونو له نومونویا داستانونو او شخصي معلوماتو چې په اسانۍ سره پیژندل کیدلی شي کار مه اخلئ.

٤- د خپل هر حساب لپاره له بدلې جملې څخه کار واخلئ.

د رمزي کلمو لپاره کومې کړنلارې باید ولرو

تاسو دوه لوی انتخابه (options) په مخ کې لرئ چې ترډیره د امنیتي کچې پورې چې غواړئ ترلاسه یې کړئ تړاو لري.

لومړی انتخاب: د جملې د عبارت کموالی چې باید په ذهن کې یې وساتئ:

- خپل حساس او مهم کارونکی حساب لکه ایمیل، ټولنیزي شبکي مشخصې کړئ او ورته د رمزي جملو څخه کار واخلئ. په کار نه دي چې تاسو له لسو زیاتې جملې یادې کړئ.
- هغه پر یو کاغذ باندې ولیکئ، پرته له دې چې د اړوند خدمتونو سره یې وصل کړئ . دا کاغذ په خپل کور کې وساتئ.
- هیڅکله یې په یو ډیجیټلي ذخیره کې مه ساتئ. هر ډیجټلي اله ممکن هک شي. په اکثرو وختونو کې ستاسو د معلوماتو هک کیدو احتمال د پټیدو څخه زیات دی.

دوییم انتخاب: د رمزي کلمو د مدیریت وسایل

د هر کاروونکي حساب لپاره د یو بدل رمزي عبارت (PASSWORD) لرل ممکن د هغو کسانو لپاره چې کمزوري حافظه لري ستونزې راولاړې کړي. اندیښنه مه کوئ، ستاسو رمزي کلماتو د ذخیره کولو لپاره د اعتماد وړاو خونديي وسايل شته دی.

ددې له ډلې [1password](), [Bitwarden]() یا [DashLane]() په انلاین بڼه د رمز (PASSWORD) د مدیریت له وسیلو څخه شمیرل کیږي. دا وسایل مخ په زیاتیدونکي ډول د Chrome ، FireFox او Safariبروسرونو (Browsers) لپاره لاس رسی شته دی او تاسو ته ددې امکان درکوي چې خپلې ټول رمزي کلمې د رمز (PASSWORD) لیکنې په یوه ورکړل شوي مرکز کې ذخیره کړئ او د ځو دستګاګانو له لارې ورته لاس رسی ولرئ. دغه انلاین امانتي صندوق ته لاس رسی د یوې رمزي جملې په واسطه ساتل کیږي. که چیرې ددغو وسایلو څخه کار اخلئ په جدي ډول سپارښتنه کیږي چې یواوږد رمزي عبارت غوره کړئ او په دوو پړاونو کې د هویت د تائید له مخې یې تنظیم کړئ.

افلاین او د وسیلو (دستګاه ګانو) پرمخ

د طیف یا spectrum په بله خوا کې KeePass د رمز یو محلي افلاین مدیر دی. د یادو شویو خدمتونو برعکس KeePass رمزي کلمات د ډاټا په انلین مرکز کې نه ساتي، بلکې یوازې هغه ستاسو د کمپیوټر یا ځیرک تیلیفون پرمخ دخیره کوي.

	Keepass	Dashlane	Bitwarden
پرانیستی متن	بلې	نه	بلې
د ځو دستګاګانو ترمنځ همغږي	بلې	بلې	نه
درمزي جملو تولید کوونکی	بلې	بلې	بلې
وړیا	نه	نه	بلې

دوو پړاونو کې د هویت تائیدول

ډیر انلاین خدمتونه د یو اضافي امنیتي (خوندیوب) اقدام د ترسره کولو امکان هم برابروي :"دوو پړاونو کې د هویت تائیدول". په دوو پړاونو کې د هویت د تائید یا (Mutual Authentication) پر دوو کړنو باندي ولاړ دی : کوم څه چې تاسو یې پیژنئ(مثلآ ستاسو رمزي کلمه) او کوم څه چې تاسو یې لرئ (لکه ستاسو ځیرک تیلیفون). په همدې اساس د یو سرویس یا خدمت ته د ننوتلو لپاره چې دا سیستم مو فعال کړی تاسو لاندې مواردو ته اړتیا لرئ:

۱. د کارولو نوم

۲. رمزي کلمه

۳. کوم کود چې د کار اخیستونکي سوفټ ویر(اپلیکیشن) له لارې یې د ځیرک تیلفیون پرمخ د پیغام په بڼه ترلاسه کیږي او هرځل چې د یوې نوې دستګاه له لارې ورته ننوځئ.

په دې توګه ستاسو د ځیرک تیلیفون پرته ستاسو انلاین حسابونو ته لاس رسی ناممکن دی. د امنیت د لا خوندیتوب لپاره د ځیرک تیلیفون له لارې ترلاسه کیدونکی کودهمداشان کولی شي د فزیکي هویت Authentication)) لکه د یوبي کیلي ([YubiKey]()) ځای ونیسي.

په دي اړه د مشهورو پېژندل شويو خدمتونو لينکونه په مستقيم په دوو پړاونو کې د هويت د تائيد (Authentication) د فعالولو لپاره کتلی شئ:

- [Google]
- [Microsoft]
- [Twitter]
- [Facebook]
- [Instagram]

د کمپيوټر اړوند اساسي سپارښتنې :

ډيجيټلي روغتيا

د کمپيوټرونو د عملياتي سيستم د سوفټ ويرونو تازه کول (اپډيټ)

د کمپيوټريا ستاسو د ځيرک تيليفون لپاره دا اړينه ده چې عملياتي سيستم او خپل پروګرامونه په منظم ډول تازه يا اپډيټ کړئ. دا اقدام د مخربو سوفټ ويرونو د برېدونو مخنيوی کوی او ستاسو د دستګاه د امنيت د خونديوب د پياوړي کيدو سبب ګرځي.
همداشان سوفټ ويرونو اپډيټ په پروګرامونو کې د ستونزويا نقص د مخنيوي سبب ګرځي، چې تازه کشف شوي دي. د همدی له امله دا اړينه او مهمه ده چې په منظم ډول خپل کمپيوټر او ځيرک تيليفونونو پروګرامونه اپډيټ کړئ.

د پرګرامونو د تازه کولو يا اپډيټ لپاره

- [Windows]
- [Mac]
- [iPhone]
- [Android]

انتي ويروس

وينډوز

د کمپیوټر د وینډوز کارونکو لپاره د مایکرو سافټ د شرکت له خوا د کارونکي وینډوز ډیفنډر (Windows Defender) په نوم د انټي ویروس څخه کار اخیستل کفایت کوي.

مک

د مک کمپیوټر کارونکي په سنتي ډول د اپل په کمپیوټرونو کې د سختو امنیتي کنټرول له امله د وینډوز د کمپیوټر د کاروونکو پرتله د مخربو سوفټ ویرونو په واسطه د خپلو کمپیوټرونو د ککړیدوکم احساس کوي. خو په دې وروستیو کې یو شمیر مخربو سوفټ ویرونو مخ په زیاتیدونکي ډول د مک کمپیوټرونه هم په نښه کوي. یو ښه عادت دادی چې یوازې د اپل د رسمي پلورنځیو له لارې یې په مک کمپیوټر کې نصب کړئ. که چیرې فکر کوئ چې انټي ویروس نصبولو ته اړتیا لرئ نو Malwarebytes نصب کړئ. وړیا چمتو کیدونکي د سوفټ ویر نسخه به د مک کمپیوټر کاروونکو ته اکثره کفایت وکړي.

ځیرک تیلیفون

په ځیرکو تیلیفونونو کې د ککړو سوفټ ویرونو پر ضد د پروګرامونو څخه د کار اخیستلو په اړه مختلف نظرونه خپاره شوي دي. دا پروګرامونه که څه هم د ککړو سوفټ ویرونو پر وړاندې د تیلیفونو د پروګرامونو ساتنه کوي، خو پخپله دا پروګرامونه هم په سیستم کې مداخله کوي او سربیره پر دې جواز ته هم اړتیا لري. که چیرې په رښتیا غواړئ چې د مالوېر Malware ککړ ویروس پر وړاندې یو پروګرام نصب کړئ د Malwarebytes یا Avira پروګرام څخه کار واخلئ.

فایروال

فایروال یو سوفټ ویر یا هارډ ویر دی چې د مجموعي امنیتي قوانینوپراساس ستاسو په کمپیوټرونو(یا په یوه شبکه) کې بهرني او دننه اړیکې کنټرولوي.

په وینډوز او مک کې د فایروال فعالول

وینډوز

د انټي ویروس د ارزوني یا فعالیدو لپاره او همدارنګه د فایروال لپاره د "Windows Defender" کلمه د مینو په پیل کې ټایپ کړئ:

Montrer avec les images en EN

د ځیرکو ټیلیفونونو لپاره اساسي لارښوونه

جوازونو اوعملي سوفټ ویرونو ته لاس رسی

د شخصي کمپیوټر په څیر د ځیرک تیلیفون پرمخ هم هر پروګرام په اسانۍ سره نه نصبول کیږي. باید په دې برخه کې د لاس رسي غوښتنې چې ستاسو ځیرک تیلیفون یو پروګرام یې غوښتنه کوي هم وڅیړئ. د مثال په ډول ایا دا به معقوله وي چې د یو قوي څراغ پروګرام له تاسو د مخاطبینو لاس رسی وغواړي؟

اوس مهال د اکوسیستم (Ecosystem) دوه اصلي پروګرامونه انډروید او آیفون دي:

ا-   آیفون د خپل کنټرول او اعتبار په دلیل له عرضې دمخه پیژندل شوی دی.

۲-	انډروید (ګوګل) متاسفانه دغو مسلو څخه په کمه کچه ساتنه کوي .

ecosystem

د انډروید پروګرامونه د مالور لرونکي

ستاسو د انډروید کڅوړه یا نسخه (د ۶ څخه پورته) ډیر وخت د تنظیم په مسیر> پروګرامونو > (کله کله په پرمختللو تنظیمات(settings) پر مهال) > د پروګرام لپاره اجازه ولټوئ.

د انډروید یو پروګرام ته د لاس رسي د ارزونې لپاره چې ستاسو تیلیفون ته یې ځانګړې کړی دی د Exodus Privacy څخه لیدنه وکړئ.

سالون

هیڅکله د کار پرمهال د کړکۍ شاته مه کښینئ.

محرم فیلټر

له یو محرم فیلټر څخه کار واخلئ.

 لباس په تن سره بهرته ووځئ.

یادونه: پاملرنه: هیڅکله خپل ځیرک تیلیفون مستقیماً په هوایي ډګر یا په عمومي محل کې د بریښنا چارچ لپاره ونه نښلوئ. دUSB د یو پوښ څخه کارواخلئ

ناآشنا/ دښمنانه / غیری دوستانه چاپیریال کې هیڅکله له خپلو دستګاګانو څخه لیرې نشئ. په لومه کې د نښلولو یا فیشینګ څخه د کار اخیستلو د چال خطر شته دی.