لارښود سند

آنلاین خوندیتوب او ډیجیټل امنیت:

د بشر حقونو د مدافعینو لپاره لارښود

انځور: د ښځو لپاره د ملګرو ملتونو دفتر/ پلوي پهتپنګ

UNAMA

UN WOMEN

منځپانګه

د دی سند په اړه ٤

د مسؤلیت رفع کول ٤

I. پیژندنه ٥

II. د کمپیوټر او موبایل د خوندیتوب «لس غوره» اصول ٧

III. د غښتلو پاسورډونو ایجادول او د ګڼ-فکتوري تصدیق فعالول ١١

غښتلي پاسورډونه (Strong passwords) ١١

ګڼ-فکتوري تصدیق (Multi-factor authentication) ١٢

IV. د ملویر له منځه وړل ١٣

ملویر (Malware) څه شی دی؟ ١٣

له ملویر څخه د وسایلو د ساتلو طریقه ١٣

V. په خوندي توګه د انټرنیټ کارول ١٤

د روټر (Router) خوندي کول ١٤

د عامه وایفای هاټسپاټونو کارول ١٤

د عامه وایفای کارولو پر مهال ځان خوندي ساتل ١٥

د خوندي براوزرونو کارول ١٥

د خوندي لټون انجنونه وکاروئ ١٥

خوندي براوزر زیاتوني (extensions/add-ons) وکاروئ ١٦

VI. د انکرپشن په اړه (Encryption) ١٧

«انکرپشن» څه شی دی؟ ١٧

الف. په خوندي توګه اړیکې نیول ١٧

«خوندي اړیکې» څه شی دی؟ ١٧

امنیتي معیارونه ١٨

د خوندي اړیکو د اپلیکېشنونو لپاره سپارښتنې ١٨

له پي جي پي (PGP) سره د خوندي (انکرپټ) برېښنالیکونو لېږلو طریقه ١٩

ب. په خوندي توګه د معلوماتو ذخیره کول او ساتل ۱۹
په یوه وسیله کې د انځورونو، ویډیوګانو او ډیټا ساتل ۱۹
د کلاوډ خدمتونو په کارولو سره د فایلونو انکرپټ کول او ذخیره کول ۲۰
د انکرپشن سافټویر ۲۰

VII. په خوندي توګه د ډیټا پاکول ۲۱
د وسایلو د پاکولو طریقه ۲۲
په دایمي توګه د ډیټا له منځه وړلو طریقه ۲۲

VIII. د فیشینګ مخنیوی کول ۲۳
د فیشینګ ډولونه ۲۳
له ډیجیټل فیشینګ څخه د ځان ژغورلو طریقه ۲٤

IX. مأخذونه او د لوست نور مواد ۲٦

X. بیړنۍ غبرګون (Emergency Assistance) ۲۷

XI. د سایبري امنیت د اصطلاحاتو لړ ۲۷

د دی سند په اړه

دا سند په اصل کې د عراق لپاره د ملګرو ملتونو د مرستندویه ماموریت له خوا تیار شوی وو او موخه يې په ډيجيټلی ساحه کې د بشري حقونو د مدافعينو، د مدني ټولنې فعالانو او د رسنيو کارمندانو ته د آنلاین خطرونو په اړه د پوهاوی لوړول او خطرونو کمول دي. دا متن د افغانستان د شرايطو لپاره د يوناما د بشري حقونو (يوناما) او په افغانستان کی د ښځو لپاره د ملګرو ملتونو دفتر لخوا ترتيب شوی دی.

د مسؤلیت رفع کول

په افغانستان کې د ملګرو ملتونو مرستندويه ماموريت او په افغانستان کی د ښځو لپاره د ملګرو ملتونو دفتر د دې فرصت هرکلی کوي چې د خپلو همکارانو په مرستې خپل فعالیتونه او خپروني ترويج کړي. مهرباني وکړئ په پام کې ونيسئ چې معلومات، مشوري او سپارښتني (د سپارښت شوي سافټويرونو او اپليکيشنونو په ګډون) د دې لارښود ليکوالانو لخوا يوازي د عمومي معلوماتو په پار چمتو شوي، او لزوما د يوناما/په افغانستان کی د ښځو لپاره د ملګرو ملتونو دفتر نظرونه نه څرګندوي.

پداسی حال کې چې د دې سند ليکوالانو هڅه کړې چې د خپرولو په وخت کې تازه او سم معلومات چمتو کړي، معلوماتي ټيکنالوژي او ډيجيټل امنيتي ګواښونه په چټکی سره بدليږي او له همدې امله دقت په هر وخت کې تضمين کيدی نشي. په دې توګه، يوناما/ په افغانستان کی د ښځو لپاره د ملګرو ملتونو دفتر د معلوماتو د بشپړتوب، کره توب، اعتبار، مناسب توب يا شتون، او د محصولاتو يا خدماتو په اړه هيڅ ډول استازيتوب يا تضمين نه کوي.

کاروونکي بايد د کارولو دمخه د معلوماتو يا سافټوير اوسنی کره توب او امنيت وګوري. د دې لارښود په پای کې حوالې چمتو شوي ترڅو کاروونکو سره مرسته وکړي چې په خوندي ميتودونو او سافټوير په اړه تازه معلومات ترلاسه کړي.

I. پیژندنه

په افغانستان کې ډیجیټلي امنیت او بشري حقونه

ډیجیټلي ټیکنالوژي کولی شي د بشري حقونو مدافعې، دفاع او عملي کیدو ته زمینه برابره کړي. ډیجیټلي ټیکنالوژي په زیاتیدونکي ډول دا وړاندې کوي چې خلک څنګه معلومات ترلاسه کوي او شریکوي یې او دا د بحث او مناظرې لپاره یوه موضوع ګڼل کیدی شي. دا فرصتونه په ځانګړي ډول هغه مهال مهم کیږي کله چې په فزیکي یا "افلاین" حالاتو کې حقونه او بنسټیزې آزادۍ له ګواښ سره مخ او محدودې شي. په هرصورت، ډیجیټلي ټیکنالوژي همدارنګه د بشري حقونو د پایمالولو، محدودولو او نقض لپاره کارول کیدی شي، د بیلګې په توګه د څارنې او سانسور له لارې. دوی [ډیجیټلي ټیکنالوژي] د دولتي چارواکو او خصوصي اتباعو لخوا د ناوړه ګټه اخیستنې او ځورونې د آسانتیا برابرولو لپاره هم کارول کیدای شي، دا ډیری وختونه موجوده سیسټماتیک تبعیض او ګوښه کیدل لا پیاوړي کوي.

د ۲۰۲۱ کال د اګست په ۱۵ د طالبانو له خوا د افغانستان د نیولو راهیسې، د برحاله چارواکو د اقداماتو په پایله کې د ښځو د خوځښت آزادۍ، کار او زده کړې ته د هغوی لاسرسي او نورو اساسي حقونو او ازادۍ عملي کولو باندی د محدودیتونو په لګولو سره په ورځني او عامه ژوند کې د ښځو ونډه کی د پام وړ کموالی راغلی دی.[1] په موازي ډول، مدني فضا او د رسنیو ازادی کی هم د پام وړ کموالی راغلی دی.[2] په دې ډول، ډیجیټلي فضا افغانانو ته په ځانګړي ډول ښځو او انجونو لپاره یو باارزښته انتخاب وړاندی کوي ترڅو دوی خپل لیدلوری او تجربې سره شریکې کړی، راټول شي، او په هغه موضوعاتو کی چې ورته مهمه دي ونډه واخلي او خپلو حقونو مدافعه وکړي. له دې سره سره، ډیجیټلي فضا لکه څنګه چې نورو ځایونو کی لیدل کیږي د خطر او محدودیت نه خالي نه ده. د راپورونو له مخې د طالبانو د واکمن کیدو راهیسی،[3] د جنسي نفرت وینا کې، چې وتلې افغان میرمنې هدف ګرځوي دری ځله زیادت راغلی دی او په آنلاین ډول د هغه محتوا په پست کولو سره چې انتقادي ګڼل کیږی، د برحاله چارواکو له لوری افراد نیول شوی دي.

د افغان میرمنو لپاره د ډیجیټلي امنیت خطرات

۲۰۲۳ کال په نومبر کې، د ملګرو ملتونو د مرستندویه ماموریت (یوناما) د بشر حقونو څانګې او په افغانستان کی د ښځو لپاره د ملګرو ملتونو دفتر په رسنیو او مدني ټولنو کې د ښځو سره سلا مشورې ترسره کړې تر څو ډیجیټلي فضا ته د افغان ښځو لاسرسي په اړه ښه پوهاوي ترسره شي، په ګډون د خطرونو او ننګونو چې دوی ورسره مخ دي، او هغه سپارښتنې چې دوی خپلو حقونو او آزادۍ ګانو څخه په ډیجیټلي فضا کی څنګه ساتنه وکړي.

د ښځو لخوا یاد شوي مهم خطرات دا وو:

- د برحاله چارواکو د غړو او عامو خلکو له خوا د ټولنیزو رسنیو د حسابونو او پیغامونو څارنه او هک کول د دواړو آنلاین او آفلاین ګواښونو او ځورونې لامل کیږي.
- د جنسیت څخه آنلاین ناوړه ګټه اخیستنه، ډیری وختونه په ځانګړي ډول ښځې، د دوی د عمومي مشخصاتو له وجی چې رسنیو او مدني ټولنې سره کار کوي، په نښه کوي.

---

۱ د لا زیاتو معلوماتو دپاره: د ښځو لپاره د ملګرو ملتونو د دفتر راپورونه، د هیواد دننه د یوناما او د کډوالو نړیوال سازمان سلا مشورې د افغان ښځو سره. ترسره شوی په نومبر ۲۰۲۳، جولای ۲۰۲۳، اپریل ۲۰۲۳ او آګست/سپتمبر ۲۰۲۲: د بشري حقونو وضعیت په افغانستان کی: د ملګرو ملتونو د بشري حقونو د عالی کمیشنر دفتر راپور، ۲۰۲۳ کال د سپتمبر ۱۱، A/HRC/٥٤/٢١.

۲ د ملګرو ملتونو، د هغوي له استازو او میکانیزمونو سره همکاري (۲۱ اګست ۲۰۲۳)، A/HRC/٥٤/٦١: ګیهریګ، ام. ۲۰۲۲. د رسنیو محدودیتونه او په افغانستان کې د جنسیتي برابرۍ اغیزې. کابل: د ښځو لپاره د ملګرو ملتونو دفتر.

۳ افغان شاهد. ۲۰۲۳. د پردې ترشا تاوتریخوالی: د آنلاین ناوړه ګټه اخیستنې زیاتوالی او د افغان میرمنو چوپتیا.

- ډاکسینګ (Doxing)، چیرې چې شخصي معلومات لکه پته او د تلیفون شمیره موندل کیږي او په عام ډول آنلاین شریک کیږي.
- د ټولنیزو رسنیو د پروفایل (Profile) جعل، چیرې چې یو څوک په ټولنیزو رسنیو کې جعلي پروفایل په جوړولو سره، د بل شخص غلا شوي شخصي پیژندل شوي معلومات د دوی په نوم د هغوی د بی اعتباره کولو په منظور خپروي.

ښځو د هغه ګامونو په اړه چې د دوی ډیجیټلي امنیت ښه کولو لپاره اخیستل کیدای شي یو لړ وړاندیزونه وکړل. پدې کې لاندی موارد شامل دي:

- د روزنیزو برنامو په لار اچول چې نه یوازې د ډیجیټلي امنیت خطرونو پروړاندې د هغوی د ځان ساتنې ظرفیت ښه کوي بلکی په عموم کی د ډیجیټلي ټیکنالوژی په کارولو کی د هغوی باور او تسلط هم لوړوي.
- په دري او پښتو ژبو کې اضافي ملاتړ او سرچینې، ښځو د دی یادونه وکړه چی د ټولنیز رسنیو او پیغام رسونې پلاټفورمونه (فېسبوک، انسټاګرام، X ، واتساپ، سیګنال) په دی ژبو کی معلومات یا سرچینې نلري.
- د سافټ ویرونو او برنامو د ګټې اخیستنې اړوند مالي او تخنیکي ملاتړ ډیجیټلي امنیت پیاوړی کوي،د بیلګې په توګه په خوندي ډول د اسنادو شریکولو او ذخیره کولو خدمات، د ډیجیټلي امنیت خطر شننه او مجازي خصوصي شبکې (VPNs).

II. د کمپیوټر او موبایل د خوندیتوب «لس غوره» اصول

دا برخه د کاروونکو د ډیجیټلي امنیت د ښه والي لپاره «لس غوره لارښوونې» وړاندې کوي. دا اساسي ټکي د اصلي عنوانونو پوهیدو لپاره چې په راتلونکو څېرکیو کې په تفصیل سره لیکل شوِي دي، اړین دي.

لومړۍ لارښوونه: په منظم ډول سره خپل عملیاتي سیستم، هارډویر، اپلیکېشنونه،موبایل او سافټویر اپډېټ کړئ.

شرکتونه د خپلو عملیاتي سیستمونو او اپلیکېشنونو لپاره مهالنی اپډېټونه (periodic updates) وړاندې کوي چې امنیتي تشې پرې ډکې کړي. په منظم ډول اپډېټ کول د امنیتي سرغړونو په وړاندې د کاروونکو خوندیتوب لوړوي.

په ویندوز ۱۱ کې، کاروونکی تشخیصوي چې کله او څنګه تازه اپډېټ ترلاسه کړي چې خپل وسایل په آرامه او خوندي توګه وکاروي. د غوراویو د مدیریت او د لاسرسي وړ اپډېټ د کتلو لپاره، (Check for Windows updates) کلیک کړئ. یا **(Start > Settings > Windows Update)** غوره کړئ.

- په مک کې، دلته وړاندې شوې لارښوونې تعقیب کړئ
- د اندروایډ فون اپډېټ کولو لپاره، دلته موجودې لارښوونې تعقیب کړئ
- د (iOS) آیفون د اپډېټ کولو لپاره اپ سټور ته ورشئ او دلته موجودې لارښوونې تعقیب کړئ

چې هر عملیاتي سیستم، اپلیکېشن او سافټویر کاروئ، په منظم ډول اپډېټ کول یې خپل لومړیتوب وګڼئ.

دویمه لارښوونه: ټولو وسایلو ته غښتلي پاسورډونه ورکړئ

کاروونکي باید داډه اوسي چې ټول پاسورډونه:

- اوږده دي (له ۱۲ تورو څخه زیات)
- پېچلي دي (غټ او واړه توري، عددونه او نښې په کې دي)
- تصادفي دي، عام یا شخصي لغتونه، د شمېرو سلسلې، او داسې نور نه دي.
- ځانګړي دي (د هر حساب لپاره جلا پاسورډ دی)
- محرم دي (پر کاغذونو یا وسایلو په اسانۍ سره نه موندل کېږي)

د ټولو پاسورډونو د ایجادولو، مدیریت کولو او په محرمه توګه خوندي کولو په اړه د نورو معلوماتو لپاره ۳ برخه وګورئ.

دریمه لاربنوونه: که شونې وي، ګڼ-فکتوري تصدیق (Multi-Factor Authentication) وکاروئ

- ګڼ-فکتوري تصدیق په ښه کچه ډیجیټلي امنیت لوړوي.
- د ګڼ-فکتوري تصدیق لپاره په ځانګړې توګه طرحه شوي اپلیکېشنونه، لکه Duo Mobile, Aegis Authenticator او Google Authenticator د لنډکیو پیغامونو تر تصدیق ډېر خوندي دي.

د نورو معلوماتو او د تجویز شوو اپلیکېشنونو د لینکونو لپاره ۳ برخه وګورئ.

څلورمه لاربنوونه: د وروستي ټکي کشف او غبرګون (Endpoint Detection and Response) انټي-ملویر سافټویر نصب کړئ

- مخرب سافټویر یوه وسیله تخریبولی شي، د یو چا شخصي معلومات یا مالي شتمنۍ غلا کولی شي، یا یوه وسیله له لرې څخه کنټرولولی شي.
- د (EDR) سافټویر پر انټرنېټ باندې له ملویر (مخرب سافټویر) څخه خوندیتوب وړاندې کوي.
- د (EDR) سافټویر مجوزې نسخې پر هره وسیله چې وینډوز، مک، لاینکس، آی او ایس یا انډرواېډ کاروي، نصب کړئ. «مات شوی» یا ”cracked“ سافټویر مه کاروئ.
- دا مهمه ده چې وړیا سافټ ویرونه یواځې د باوري سرچینو څخه ترلاسه شي.
- د Malwarebytes او Avira په څېر پروګرامونه نصب کړئ.

د نورو معلوماتو لپاره ۴ برخه وګورئ.

پنځمه لاربنوونه: خوندي براوزر browser وکاروئ

- براوزر د انټرنېټ لپاره د وینډوز په څېر کار کوي. که وینډوز خوندي نه وي، لاسرسی او حرکت یې خوندي نه دی او ښایي د مخرب سافټویر څخه د ککړتیا لپاره یوه لاره اوسي.
- ډېری براوزرونه د معلوماتو راغونډولو، ډېټا څارلو او د بازارموندنې لپاره تر هدف لاندې نیولو لپاره سوداګریزې وسیلې دي.
- د Firefox, Brave, Firefox Focus, Ghostery Dawn, او DuckDuckGo په څېر خوندي براوزرونه وکاروئ؛ د براوزر سافټویر مو په منظم ډول سره اپډېټ کړئ.
- مخکې له دې چې خپل براوزر ته یې ور اضافه کړئ، د براوزر د پراختیاوو/اضافي غوراویو (add-ons/browser extensions) امنیت وارزوئ.

د نورو معلوماتو لپاره لاندې ۵ برخه وګورئ.

شپږمه لارښوونه: یوه مجازي خصوصي شبکه (VPN) نصب کړئ

- VPN د «virtual private network» لنډیز دی – دا یو داسې خدمت دی چې د کاروونکو د ډېټا او د کاروونکي د آی پي ادرس IP address د پټولو لپاره د یو اینکریپټ شوي تونل (encrypted tunnel) په ایجادولو سره د کاروونکي د انټرنیټ اتصال او محرمیت په آنلاین توګه خوندي کوي. دا چاره د عامې وایفای کارول خوندي کوي. د خوندیتوب لپاره له وي پي این پرته، ښایي تجهیزات او یا یې موقعیتونه وځارل شي یا یې ښایي ډېټا ترلاسه کړل شي.
- په احتیاط سره وي پي این غوره کړئ. داسې وړیا او وړاندې شوي خدمتونه شته چې مخرب سافټویر لري، د کاروونکو معلومات پر درېمګړو ډلو پلوري، یا له حکومتونو سره همکاري کوي چې د کاروونکو معلومات ورته وړاندې کړي.
- د دې لارښود د خپرېدلو ترمهاله خوندي ګڼل شوي وي پي این کې Psiphon, TunnelBear, یا Riseup VPN شامل دي.

د نورو معلوماتو لپاره لاندې ۳ برخه وګورئ.

اوومه لارښوونه: د پرانیستو سرچینو سافټویرونو او اپلیکېشنونو خوندي کارول

- د «پرانیستې سرچینې Open-source» سافټویر او اپلیکېشنونه د اختصاصي پروګرامونو په پرتله په عمومي توګه ډېر خوندي وي، ځکه چې دا د خپلو کاروونکو لپاره د سرچینې کوډ وړاندې کوي. دا د سرچینې کوډ بیا په دوامداره توګه اپډېټ کېږي چې امنیتي زیانمنونه ته ځواب ووایي.
- د پرانیستې سرچینې سافټویر او اپلیکېشنونو کارول کاروونکي د غلاشوو یا «مات شوو» اختصاصي سافټویرونو له کارولو څخه ژغوري چې جواز ونه لري. غلا شوو یا «مات شوو» پروګرامونو کې ښایي داسې عناصر موجود وي چې وسایلو ته زیان رسوي او باید هیڅکله ونه کارول شي.
- خبردار اوسئ چې د پرانیستې سرچینې ټول پروګرامونه خوندي نه وي: د نوي سافټویر یا اپلیکېشن له نصبولو وړاندې د ډیجیټل امنیت له متخصصینو سره مشوره وکړئ. دا غوره ده چې هغه برنامې وکارول شي چې د کارونې قوي مخینه ولري، او په روښانه ډول د مسایلو او خصوصي حریم په اړه امنیتي برنامې او پالیسۍ وپېژني.

اتمه لارښوونه: یوازې له تائید شوي اپ سټور څخه اپلیکېشنونه او سافټویر ښکته کړئ

- ناتائید شوي اپ‌سټورونه په درجنونو داسې اپلیکېشنونه او پروګرامونه لري چې له مخرب سافټویر څخه ډک وي چې ایجادوونکي ته یې دا وړتیا ورکوي چې وسایل مدیریت او کنټرول کړي.
- د ښکته کولو لپاره یوازې تائید شوي اپ سټورونه او د اپلیکېشنونو رسمي ویب سایټونه وکاروئ: Google Play، Amazon Appstore او Apple App Store.

نهمه لاربنوونه: کمپیوټرونه او موبایلونه مو انکرپټ (Encrypt) کړئ

- انکرپټ کول محرمیت وړاندي کوي او د معلوماتو د خوندیتوب لپاره اساسي کار دی.
- د انکرپټ شوو پیغامونو د لېږلو، د معلوماتو د خوندي ساتلو، په پټه سره د انټرنیټ لټولو او په خوندي توګه د معلوماتو د شریکولو لپاره له انکرپشن څخه کار واخلئ.

د انکرپشن د وسایلو په اړه د لا ډېرو معلوماتو لپاره ۴ برخه وګورئ.

لسمه لاربنوونه: د خپلې ډیټا پشتیبانه (Backup) واخلئ

- د پشتیباني پروسه داسې وي لکه ارزښتناک معلومات چې په سیف کې وساتل شي، چې په هغه وخت کې بېرته راخیستل کېږي چې اصلي ډیټا ورکه شي، تخریب شي یا هیک کړل شي.
- د پشتیباني وسیله په لاسي توګه فعاله کړئ چې له عملیاتي سیستم سره (په وینډوز او مک سافټویر کې) وړاندې شوي وي او ډاډه اوسئ چې بک اپ په مهالنۍ توګه بشپړېږي.
- د ذخیره کولو لپاره د ډیټا د پشتیباني نسخې انکرپټ کړئ.
- خپله پشتیبانه مو یا پر بهرني هارډ ډرایو یا د کلاوډ پر بنسټ خدمتونو، Google Drive له لارې ذخیره کړئ.

د نورو معلوماتو لپاره ٦ برخه وګورئ.

اضافي لاربنوونه: د بیړني قفل کولو حالت

- د آی فون کاررونکي بیړني قفل کولو حالت اختیار/خوښه لري تر څو د پیچلو او هدفي سایبري بریدونو څخه ځان وساتي.
- د قفل کولو حالت د ځینو اپلیکشنونو، ویب پاڼو او خاص بڼو فعالیت محدودوي تر څو د دې احتمال کم کړي چې سپای ویر وکولای شي وسیلې ته ورننوزي او هغه ډیټا ته چې هلته زیرمه ده لاسرسی پیدا کړي.

III. د غښتلو پاسوردونو ایجادول او د ګڼ-فکتوري تصدیق فعالول

غښتلي پاسوردونه (Strong passwords)

غښتلي پاسوردونه د ډیجیټلي خوندیتوب بنسټ جوړوي. د دوی غښتلتیا تاسو جوګه کوي چې د هغو بریدونو په وړاندې مقاومت وکړئ چې پر پاسوردونو برید کوي لکه د فیشینګ (phishing) عملیات، کی‌لاګر (keyloggers) او داسې نور بریدونه چې موخه یې د ډیټا ترلاسه کول یا خوندي حسابونو یا ډیټا ته د غیرمجاز ننوتلو ترلاسه کول وي.[٤]

د دې بریدونو په وړاندې تر ټولو غوره دفاع د غښتلو پاسوردونو په جوړولو او په دوامداره توګه بدلولو له لارې د دوی مخنیوی دی.

غښتلی پاسورډ لاندې ځانګړتیاوې لري:

۱. اوږد

له ۱۲ تورو څخه زیات پاسورد وکاروئ. څومره چې پاسورډ لنډ وي، هومره په چټکۍ سره پېژندل کېدلی شي.

۲. پېچلي

غټ او واړه توري، عددونه او نښې وکاروئ.

۳. تصادفي

په مسلسل ډول د عددونو یا تورو له کارولو یا د شخصي یا کورنیو معلوماتو له کارولو ډډه وکړئ. په پاسوردونو کې د زېږېدنې د نېټې، د کورنۍ د غړو د نومونو یا د څارویو نومونو له کارولو څخه ډډه وکړئ.

٤. په اسانه یادېدل

د پاسوردونو هېرول د یادولو یو دوران پیلوي، چې ډېرو معلوماتو ته اړتیا لري. که د ګڼو پاسوردونو یاد ساتل درته ستونزمن وي نو (لاندې) پاسورډ منیجر وکاروئ.

۵. محرم

پاسوردونه ایجاد او ثبت کړئ، خو یوازې په خوندي ځایونو کې. په ناخوندي ځایونو کې په مستقیم ډول په براوزر، د فون د یادښتونو اپلیکېشن، د فون د رایادولو اپلیکېشن، د کمپیوټر یادښتونو یا په کتابچې/اجنډا کې ساتل شامل دي. دا ځایونه ټول ناخوندي دي ځکه چې په اسانۍ سره ورته لاسرسی کېږي.

٤ هغه بریدونه چې هدف یې د پاسوردونو څرګندول دي: په مینځ کې شخص (man-in-the-middle) یا (MITM)، بی رحمه ځواک بریدونه (brute force)، د لغتونو د فرهنګ (dictionary attacks)، او د اعتبار پر بنسټ بریدونه (credential stuffing) شامل دي. د عام پاسورډ بریدونو په اړه د نورو معلوماتو لپاره وګورئ (Password Cracking 101: Attacks & Defenses Explained.)

٦. ځانګړی

هر حساب یا خدمت باید خپل پاسورډ ولري. د یو حساب د پاسورډ پیدا کیدل نور حسابونه هم زیانمنوي، که چېرته ورته همغه پاسورډ کارول شوی وي.

٧. په مهالنی توګه بدل شوی

یو پاسورډ باید له بدلولو مخکې د خومره وخت لپاره وکارول شي، دا چاره په هغه خطر پورې اړه لري چې کاروونکي ورسره مخ دي. په عادي حالتونو کې سپارښتنه کېږي چې پاسورډونه په هرو دربو میاشتو کې بدل شي. د پاسورډ د بدلولو پر مهال باید یو کاروونکی په بشپړ ډول له اپلیکېشن یا خدمت څخه په ټولو وسایلو کې ووځي.

٨. اصلی

د کیبورډ عمومي تڼیو سلسله مه کاروئ لکه 'Qwerty١٢٣٤٥' یا ’Password١٢٣‘.

پاسورډونه په سختۍ سره د لاسرسي وړ پټو ذخیرو (caches) یا پاسورډ منیجر (password managers) کې ساتل کیدلی شي. دا پټې ذخیرې د پاسورډ پیاوړي ایجادوونکي دي، او پراخ شمېر پاسورډونه په کې ساتل کیدلی شي.

د دې لاربنود د خپرولو پر مهال لاندې پاسورډ منیجر خوندي ګڼل شوي دي:

١. KeePassXC

٢. Bitwarden

ګڼ-فکتوري تصدیق (Multi-factor authentication)

په حسابونو کې د ګڼ-فکتوري تصدیق غوراوی فعالول له هک کیدلو یا فیشینګ څخه جدي خوندیتوب وراندې کوي. ګڼ-فکتوري تصدیق یوه اضافه ځانګړنه ده چې کاروونکي هڅوي چې یو ځل-کاریدونکی پاسکوډ (single-use passcode) داخل کړي چې وروسته له هغه څخه رامنځ ته کېږي چې دوی خپل عادي پاسورډ داخل کړي. دا یو ځل کاریدونکی پاسورډ کاروونکي ته د لنډکي پیغام، برېښنالیک له لارې لېږل کېږي، یا ورته د تصدیق د ځانګړي اپلیکېشن له لارې لاسرسی کېږي.

د دوه- پړاوونو تائید د فعالولو لپاره تر ټولو غوره لاره د بهرني اپلیکېشن د کارولو له لارې فعالول دي. د دې لاربنود د خپریدلو تر وخته لاندې اپلیکېشنونه خوندي ګڼل شوي دي.

١. Duo Mobile

٢. Aegis Authenticator (یوازې د اندروایډ لپاره)

٣. Google Authenticator (iOS یا Android)

١٧. د ملویر له منځه وړل

ملویر (Malware) څه شی دی؟

مخرب سافټویر، یا ملویر یوه اصطلاح ده چې د هغه سافټویر لپاره کارول کېږي چې د دې لپاره طرحه شوی وي چې وسایل، عملیاتي سیستمونه، یا شبکې تخریب، ناوره کټه، یا یې له کټې اخیستلو وغورځوي. ملویر د دې لپاره کارول کېږي چې ډیټا غلا کړي، غیرمجاز لاسرسی ترلاسه کړي، ځینې وسایلو یا اړوندو شبکو کې ځینې برخې غیرفعالې کړي یا یې تخریب کړي.

وایروسونه د مخرب سافټویر د کورنۍ یوه کوچنۍ برخه تشکیلوي، په داسې حال کې چې ځینې نور زیان رسوونکي ملویر نبایي د انټرنیټ د کارولو پر مهال ځینو وسایلو ته نفوذ وکړي یا یې تخریب کړي.

د ملویر د له منځه وړلو پروسه د مخنیوي ګامونو ته اړتیا لري. د مخرب سافټویر د کړنیتیا او نفوذ په وړاندې خنډونه جوړول کاروونکي جوګه کوي چې ګواښونه مخکې له دې چې د دوی وسایلو ته ننوځي، له منځه یوسي.

مخرب سافټویر ډېر ډولونه لري چې Trojans، worms، ransomware، adware، spyware او داسې نور په کې شامل دي.

له ملویر څخه د وسایلو د ساتلو طریقه

له ملویر څخه د وسایلو د ساتلو لپاره باید لاندې ګامونه تعقیب کړل شي:

١. د ټولو کمپیوټرونو او موبایلونو په شمول، د هرې وسیلې لپاره چې وینډوز، مک، لاینکس، آی او ایس یا انډروایډ سیستمونه په کې چلېږي د (EDR) باوري سافټویر نصب کړئ. په یاد ولرئ چې یوازې یو (EDR) پروګرام باید نصب شي.

٢. یوازې له رسمي ویب سایټونو څخه پروګرامونه او اپلیکېشنونه ښکته کړئ.

٣. په منظم ډول سره د وسایلو عملیاتي سیستمونه او اپلیکېشنونه اپډیټ کړئ.

٤. د عامې او/یا ناخوندي وایفای شبکو له کارولو څخه ډډه وکړئ چې مناسب خوندیتوب (لکه وي پي این) نه لري.

٥. له نابلدو یا مشکوکو برېښنالیکونو یا پیغامونو څخه پر لینکونو باندې کلیک مه کوئ، حتی که رالېږونکي یې پېژنئ هم.

٦. د شخصي معلوماتو له شریکولو ډډه وکړئ.

٧. د انټرنیټ د لټولو پر مهال خوندي براوزر وکاروئ.

٨. د براوزر لپاره د امنیت تجویز شوې زیاتونې (add-ons) وکاروئ.

د دې لاربښود د خپریدلو پر مهال د (EDR) دوه پروګرامونه خوندي ګڼل کېږي (چې هم وړیا او هم په تادیه کیدونکې بڼه موجود دي) Malwarebytes او Avira. په یاد ولرئ چې وړیا د ویروس ضد سافټویر د عام ویروس پروړاندې لومړنې محافظت وړاندې کوي پداسې حال کې چې اخیستل شوی د ویروس ضد سافټویر ډېر پرمختللی محافظت وړاندې کوي.

۷. په خوندي توګه د انټرنیټ کارول

د کاروونکو لپاره خطر هغه وخت پیلیږي چې کله یې کمپیوټر یا موبایل له انټرنیټ سره وصل شي او کاروونکی لټون پیل کړي یا له نورو سره اړیکې ونیسي.

د خوندیتوب د لوړاوي لپاره انټرنیټ ته د لاسرسي خوندي وسایل وکاروئ. دا چاره د خدمت وړاندې کوونکو، چارواکو یا هیکرانو مخه نیسي چې د کاروونکي فعالیت وڅاري.

د روټر (Router) خوندي کول

په لومړي ګام کې د روټر د تنظیماتو په بدلولو سره په کور یا دفتر کې د وایفای هاټسپاټ خوندي کول شامل دي. که درته ناآشنا وي نو د دې ګامونو لپاره د تخنیکي مرستې غوښتنه وکړئ. د روټر تنظیم کولو څرنګوالي په اړه لومړني معلوماتو لپاره، مهرباني وکړئ په بکس کې امنیت وګورئ، "د مالویر پرضد خوندي اوسئ: خپل روټر خوندي کړئ"، دلته د لاسرسي وړ دي: https://securityinabox.org/en/phones-and-computers/malware/.

۱. د روټر د اداره کوونکي د حساب نوم او پاسورډ (پټنوم) بدل کړئ.

۲. د روټر آی پي ادرس بدل کړئ.

۳. د وایفای (Wi fi) لپاره غښتلی او خصوصي پاسورډ وکاروئ.

٤. د انکرپشن تنظیمات وټاکئ او WPA2-PSK (AES) غوره کړئ.

٥. د روټر فرموير (firmware) اپډیټ کړئ.

٦. د وایفای شبکې نوم پټ کړئ.

د عامه وایفای هاټسپاټونو کارول

د وایفای عامه شبکې (په پلورنځیو، مارکیټونو، عامه ترانسپورټ، هوټلونو، او داسې نورو کې) ډیرې وختونه له امنیتي لحاظه کمزورې وي او کاروونکي ته لاندې ګواښونه پېښولی شي:

۱. د پاکټ د کشف ګواښ (Threat of packet discovery) بریدکوونکي (هیکران) په ناخوندي شبکو باندې لېږل شوې یا ترلاسه شوې انکرپټ شوې ډیټا څاري او ترلاسه کوي.

۲. په منځ کې سرې بریدونه (Man-in-the-Middle Attacks) بریدکوونکي کمزوري وایفای هاټسپاټ ته نفوذ کوي چې په ننبه شوي قرباني او د هاټسپاټ ترمنځ د اړیکو برخه شي، چې ډیټا ترلاسه کړي او ځینې وختونه یې د انتقال پر مهال تغیر کړي.

۳. غولوونکې وایفای شبکې بریدکوونکي د عامو خلکو لپاره یو وړیا او پرانیستی هاټسپاټ ایجادوي او تنظیموي چې ورسره وصل شي، چې وروسته یې د کاروونکي د ډیټا راغونډولو لپاره د دهلېز په توګه کاروي.

د عامه وایفای کارولو پر مهال ځان خوندي ساتل

که امکان ولرئ، د عامه وای فای پرځای ګرځنده یا موبایل هاټس پاټ وکاروئ. د ارتباطاتو د عامه نقطو د کارولو پر مهال له بریدکوونکو څخه د خپلو شخصي معلوماتو د خوندي کولو لپاره دا لارښوونې تعقیب کړئ:

- که شونې وي د نامعلومو/ناخوندي هاټسپاټونو یا عامه انټرنیټونو له کارولو څخه ډډه وکړئ.
- که عامه شبکه کاروئ، ډاډه اوسئ چې له کارولو وړاندې مو د ټولو حسابونو لپاره ګڼ-فکتوري تصدیق فعال کړی دی.
- فایروال (firewall) وکاروئ. دا خدمت په ډېرو عملیاتي سیستمونو کې شامل وي، لکه څنګه چې په کې د ملویر ضد/ (EDR) پروګرامونه وي. د دې لارښود د خپرولو پر مهال خوندي ګڼل شوي اپلیکېشنونه په لاندې ډول دي:
  Avira Comodo GlassWire
- په وینډوز کې، د مایکروسافټ مدافع د اور دیوال (Microsoft Defender Firewall) تنظیم کړی. لارښوونې دلته موندل کیدی شي.
- د انټرنیټ د اتصال د انکرپټ کولو لپاره د وي پي این خدمتونه (VPN service) وکاروئ او پر هره شبکه باندې خپل آنلاین فعالیت خصوصي وساتئ. هغه وي پي این چې د خپرولو په وخت کې خوندي ګڼل کیږي، په لاندې ډول دي:
  Windscribe ProtonVPN Psiphon TunnelBear Riseup

د خوندي براوزرونو کارول

براوزرونه انټرنیټ ته د لاسرسي لومړنۍ دروازې دي، او له همدې امله په آنلاین امنیت کې مهم نقش لوبوي. د غلا د مخنیوي یا د ډیټا د محرمیت له سرغړونو څخه د خوندیتوب لپاره د خوندي براوزر انتخابول اړین دي.

هغه براوزرونه چې د خپرولو په وخت کې خوندي ګڼل کیږي، په لاندې ډول دي:

Firefox Brave Ghostery Dawn DuckDuck Go (د آیفون لپاره iPhone) Firefox Focus

د مختلفو براوزرونو د ګټو او زیانونو په اړه د نورو معلوماتو لپاره، د مطبوعاتو د ازادۍ بنسټ لخوا خپور شوی لارښود بیاکتنه دلته وکړئ

د خوندي لټون انجنونه وکاروئ

لټون باید د لټون د خوندي انجنونو په کارولو سره ترسره شي چې محرمیت ساتي. د ګوګل، بینګ، امازون او یانډیکس په شمول د لټون ډېری عامه انجنونه د محرمیت له معیارونو سره سم نه دي.

هغه د لټون انجنونه چې د خپرولو وخت کې ډېر امنیت او محرمیت چمتو کوي په لاندې ډول دي:

DuckDuck Go Qwant StartPage

خوندي براوزر زياتونې (extensions/add-ons) وکاروئ

د براوزر زياتونې، په بل پروګرام کې د برنامو فعاليت پراخوي، لکه براوزر. زياتونې معمولا د سافټوير بشپړه نسخه نه وي بلکه د کوډ ټوټې دي چې يو ځانګړی رابط، بدلوي. د براوزرونو لپاره تر ټولو عام زياتونې هغه ټولبارونه (toolbars) دي چې کاروونکو ته آنلاين خدمات په سملاسي ډول وړاندې کوي.

د براوزرونو يوازې هغه زياتونې بايد ښکته کړل (download) شي چې د کاروونکي امنيت او محرميت زياتوي.

د دې لارښود د خپريدلو تر وخته، لاندې پراختياوې کاروونکو ته ښه امنيت وړاندې کوي:

HTTPS Everywhere | Virus Total | Ghostery | Malwarebytes | Cookie AutoDelete

NoScript | Privacy Badger

VI. د انکرپشن په اړه (encryption)

«انکرپشن» څه شی دی؟؟

په ساده اصطلاح، انکرپشن له لوستلو وړ بڼې څخه خوندي کوډ شوې بڼې ته د معلوماتو د اړولو پروسه ده چې د هغو کاروونکو له خوا «بېرته پرانیستل» کیدلی شي چې پټه «کیلي» یا پاسورډ ولري.

انکرپشن شپږ ګټې لري

- د ډیټا یوځای‌والي او محرمیت په ساتلو کې مرسته کوي.
- له اداري سره مرسته کوي چې د محرمیت او امنیت له مقرراتو سره مطابقت وکړي.
- ډیټا خوندي ساتي څکه چې پر مختلفو وسایلو باندې انتقالېږي.
- له ادارو سره مرسته کوي چې دفترونه خوندي وساتي.
- معنوي شتمنۍ خوندي ساتي.
- کلاوډ ذخیرې ته د انتقال پر مهال ډیټا خوندي ساتي.

انکرپشن د دې لپاره کارول کیدلی شي چې په خوندي توګه:

۱. انځورونه، ویډیوګانې، او ډیټا وسایلو کې ثبت کړو.
۲. فایلونه او اسناد شریک کړو.
۳. په خصوصي توګه برېښنالیکونه ولېږو.
٤. د کلاوډ (Cloud) خدمتونو په کارولو سره فایلونه ذخیره کړو.
٥. د پیغامونو یا زنګونو له لارې اړیکې ونیسو.

الف. په خوندي توګه اړیکې نیول

«خوندي اړیکې» څه شی دی؟

خوندي اړیکې د یو یا ګڼو امنیتي پروتوکولونو په کارولو سره د یو کاروونکي د اړیکو د انکرېپټ کولو پروسه ده چې ډاډ ورکړي چې ډیټا پرته له دې چې درېمګړي لوري ته ورسېږي، د لېږونکي او ترلاسه کوونکي ترمنځ تبادله کېږي. انکرپشن ساده متن په پټو کوډونو اړوي چې نور یې لوستلی نه شي، که څه هم دوی یې مخکې تر دې چې تر هدف لاندې ترلاسه کوونکي ته

ورسېږي، ترلاسه کړي. کله چې پيغام اصلي ترلاسه کوونکي ته رسېږي، د دوی وسيله خپله کيلي کاروي چې معلومات بېرته په ساده، د لوستلو وړ متن باندې واړوي.

که چېرته اتصال انکرپټ شوی نه وي، حکومتونه، ډلې او افراد چې تخنيکي پوهه ولري يادو اړيکو ته غوږ نيولی او لوستلی يې شي او منځپانګې ته يې لاسرسی لرلی شي، ترلاسه کولی او تعديلولی يې شي، ملوير په کې ځای پر ځای کولی شي او د سيستم دننه ځان ته يو څه لار پرېښودلی شي چې ډيټا ورته يا ورڅخه انتقال کړي.

امنيتي معيارونه

د اړيکو نيولو د پروګرامونو او اپليکېشنونو د انتخابولو لپاره لاندې معيارونه تجويز شوي دي چې ډېر ورکړل شي چې اړيکې له ځارنې، جاسوسۍ او شخصي معلوماتو ته د غيرمجاز لاسرسي څخه خالي دي.

- **اړيکې بايد** د لېږونکي او ترلاسه کوونکي ترمنځ، د (End-to-end (E2EE)) په کارولو سره **انکرپټ شوې وي**، چې حتی خپله شرکت يا د خدمتونو وړاندې کوونکی ونشي کولی چې د پيغامونو منځپانګې ته لاسرسی ولري. پيغامونه د لېږونکي له خوا انکرپټ شوي صادرېږي او تر هغه پورې بېرته نه ډيکرپټ کېږي چې د ترلاسه کوونکي وسيلې ته رسيدلي نه وي.
- **ځارل کيدونکي نه وي**، په دې مانا چې هغه شرکت چې ياد اپليکېشن يې توليد کړی دی د اړيکو معلوماتو يا د کاروونکو ډيټا نه راغونډوي. ډېری سوداګريز شرکتونه د کاروونکو په اړه معلومات راغونډوي او پر نورو شرکتونو يا هيوادونو يې پلوري، لکه د تبليغاتو او بازارموندنې شرکتونه.
- اپليکېشن يا پروګرام بايد **پرانيستې سرچينه** ولري، لکه پورته مو چې بحث پرې وکړ. د پرانيستې سرچينې سافټوير تخنيک کارانو ته د ارزونې او د کمزورتياوو د کشفولو په موخه د اپليکېشنونو او پروګرامونو کوډونه وړاندې کوي. همدا ډول د پرانيستې سرچينې کوډ تاسو جوګه کوي چې وګورئ چې آيا توليدوونکی شرکت د کاروونکو معلومات او ډيټا راغونډوي که نه. دا غوره ده چې هغه برنامې وکارول شي چې د کارونې قوي مخينه ولري، او په روښانه ډول د مسايلو او خصوصي حريم په اړه امنيتي برنامې او پاليسۍ وپيژني.
- **د پټتيا (Anonymity) يو غوراوی بايد موجود وي**، ه دې مانا چې پروګرام يا اپليکېشن د کاروونکي شخصي معلومات (نوم، د موبايل شمېره، برېښناليک، جغرافيوي موقعيت، او د وسيلې آی ډي/device ID) پټولی شي، حتی د پيغامونو او زنګونو د لېږلو رالېږلو پر مهال، او د ضميمو د (.doc, .pdf, .jpeg, .mp3) په شمول، د لېږلو او رالېږلو پر مهال.

ډېری کاروونکي نه پوهېږي چې آيا عام اپليکېشنونه لکه فيسبوک مسينجر، وايبر، ټيليګرام، وټساپ او نور له پورته معيارونو سره سم دي که نه. د شفافيت راپورونو ته کتنه چې شرکتونه يې په مهالني ډول توليدوي او د امنيتي تخنيک کارانو له خوا ارزونې ښيي چې له بده مرغه دا اپليکېشنونه پورته ځينې معيارونه مراعاتوي، خو ټول معيارونه نه پوره کوي.

د خوندي اړيکو د اپليکېشنونو لپاره سپارښتنې

Signal

د سيګنال خصوصي مسينجر د محرميت ساتلو لپاره له تر ټولو غوره اپليکېشنونو څخه ګڼل کېږي او له يوې استثناء پرته له پورته ټولو معيارونو سره برابر دی چې هغه پټتيا ده. سيګنال د فعالولو لپاره د فون شمېرې ته اړتيا لري؛ په هر حال، سيګنال معلومات نه ځاري او د کاروونکو معلومات نه راغونډوي.

Wire

دا اپليکېشن د کاروونکو لپاره د اسانه رابط په لرلو سره، له پورته معيارونو سره سم دی. دا اپليکېشن د موبايلونو او کمپيوټرونو لپاره موجود دی. دا د پروګرام يا اپليکېشن په څېر نصبولو ته اړتيا نه لري – بلکې د براوزر دننه د پراختيا په شکل کارول کيدلی شي.

Jitsi

جيټسي مېټ د اړيکو نيولو يا د آنلاين ناستو ترسره کولو لپاره يو پليټفارم دی. د ويب-پربنسټ د ناستو پر نورو پروګرامونو باندې د دې برتري دا ده چې دا د اړيکو لپاره يو انکرپټ شوی چينل ايجادوي، او پټتيا ساتي. اړينه نه ده چې د دې لپاره تاسو حساب جوړ کړئ يا خپل شخصي جزئيات په کې داخل کړئ. کاروونکي کولی شي د براوزر له لارې له ويبپاڼې څخه ليدنه وکړي، چټ پرانيزي، او له هر هغه چا سره يې لينک شريک کړي چې دوی يې خبرواترو ته رابلل غواړي. د جيټسي اپليکېشن پر کمپيوټرونو او موبايلونو هم نصبيدلی شي.

Tresorit

دا خدمت هم له يو اړخ څخه بل ته معلومات انکرپټ کوي. دا يو ساده رابط لري او د معلوماتو محرميت ساتي، چې د انتقال پر مهال يې انکرپټ کوي.

له پي جي پي (PGP) سره د خوندي (انکرپټ) برېښناليکونو لېږلو طريقه

د دې لپاره چې ډاډه اوسو چې برېښناليکونه مو خوندي دي، تر ټولو غوره لاره دا ده چې له «PGP» سره يې انکرپټ کړو. PGP د «Pretty Good Privacy» يا ډېر ښه محرميت لنډيز دی. دا د انکرپشن يو سيستم دی چې د انکرپټ شوو برېښناليکونو او د حساسو فايلونو د انکرپټ کولو لپاره کارول کېږي. پي جي پي د معلوماتو د پرانيستلو لپاره د اړينو خصوصي او عامه کيلي‌ګانو په ايجادولو سره برېښناليکونه او د دوی ضميمې انکرپټ کوي چې د اړيکو محرميت لوړوي.

د برېښناليکونو د انکرپشن په اړه ډېر معلومات دلته ترلاسه کيدای شي.

يادونه:

پي جي پي يوازې هغه وخت د کار وړ دی چې لېږونکی او ترلاسه کوونکی دواړه داسې اپليکېشنونه او پروګرامونه کاروي چې د پيغامونو د انکرپټ کولو او ډيکرپټ کولو (Decrypt) لپاره کارېږي. ډېری پروګرامونه او اپليکېشنونه شته چې (OpenPGP) معيار کاروي، نو ځکه هر کاروونکی اړ دی چې دقيقاً همغه پروګرام وکاروي؛ په هر حال، دا ښايي «د تبادلې په کيلي‌ګانو» سمبال وي. د انکرپټ برېښناليکونو له لېږلو وړاندې له خپلو اشخاصو سره اړيکه ونيسئ چې د خوندي اړيکو نيولو لپاره تر ټولو غوره لاره کومه ده.

Mailvelope يو تجويز شوی پروګرام دی چې د مشهورو ويبميل وړاندې کوونکو لکه هاټميل، اوټلوک، جي‌ميل او ياهو سره کارول کيدلی شي. دا د ګوګل کروم او فايرفوکس په څېر براوزرونو ته د پراختيا يا زياتونې په توګه ور اضافه کيدلی شي. دا د اړينو عامه او خصوصي کيلي‌ګانو جوړې رامنځ ته کوي، بيا عامه کيلي له نورو کاروونکو سره شريکوي چې هغوی هم ورسره يوځای شي.

ب. په خوندي توګه د معلوماتو ذخيره کول او ساتل

کاروونکي بايد يوازې هغه معلومات انکرپټ نه کړي چې له نورو سره يې شريکوي، بلکې خپل معلومات هم انکرپټ کړي چې په خوندي توګه يې ذخيره کړي. دا برخه د انکرپشن د بېلابېلو طريقو په اړه لارښوونې وړاندې کوي چې د کاروونکي په وسيلو کې او په کلاوډ کې د ډېټا د ذخيره کولو لپاره کارول کيدلی شي.

په يوه وسيله کې د انځورونو، ويډيوګانو او ډېټا ساتل:

Tella د هغه اپلیکېشن یوه بېلګه ده چې ډیټا نبه خوندي ساتلی شي. دا په بشردوستانه کارونو او مستندولو کې د فعالانو، د بشري حقونو د مدافعینو، د مدني ټولنو، رسنیو، او متخصصینو له خوا کارول کېږي. د اوس مهال لپاره یوازې د انډروایډ موبایلونو لپاره د لاسرسي وړ دی، خو د آی او ایس نسخه یې هم د جوړېدو په حال کې ده.

- ساده رابط (interface) لري او په اسانۍ سره کارول کېدلی شي.
- د یو شکل په جوړولو سره، کاروونکي کولی شي د "pattern method" له لارې اپلیکېشن قفل کړي.
- کاروونکي د اپلیکېشن آیکن/څېره بدلولی شي چې ونه پېژندل شي.
- که چېرته کاروونکی له خطر سره مخ وي چې ښایي موبایل یې ضبط شي، نو په اسانۍ سره «چټک حذف» ځانګړنه لري چې ډیټا یې له منځه یوړل شي.
- د سملاسي خطر په حالت کې پخپله اپلیکېشن هم د تل لپاره له منځه وړل کېدلی شي

د کلاوډ خدمتونو په کارولو سره د فایلونو انکرپټ کول او ذخیره کول:

که څه هم ډېری خلک خپل حساس فایلونه په خپلو کمپیوټرونو یا په هارډ ډرایوونو کې (external hard drives) له انکرپټ کولو پرته ساتي، خو دا تکتیک خطرناک دی. که غیرمجاز لاسرسی ورته وشي، دا وسایل اخیستل کېدلی او ډیکرپټ کېدلی شي، یا افراد کاروونکی مجبورولی شي چې انکرپشن یې پرانیزي.

مهمه ده چې حساس معلومات په وسایلو کې پرېښنبودل شي، ځکه چې دا چاره، کاروونکی له آفلاین او آنلاین خطر سره مخ کولی شي. په خوندي توګه په کلاوډ کې د معلوماتو ذخیره کول دا ډاډمنوي چې غیرمجاز درېمګړي لوري حساسو معلوماتو ته لاسرسی نه شي لرلی. کاروونکي باید پر وسایلو باندې د ډیټا د تعقیب (traces) له پرېښنبودلو څخه ډډه وکړي چې د امنیتي ستونزو سبب ګرځېدلی شي.

د «کلاوډ خدمتونه» هغه زېربنایي پلټفارمونه یا سافټویر دی چې د درېمګړي لوري وړاندې کوونکو په کوربه توب د کاروونکو لپاره د انټرنېټ له لارې د لاسرسي وړ دي.

د کلاوډ لاندې خوندي خدمتونه د حساسو معلوماتو د ذخیره کولو لپاره وړاندیز کېږي چې فزیکي نښې نه پرېږدي:

- [Google Drive](#)
- [pCloud](#)

خو بیا هم مهمه ده چې کلاوډ ته له پورته کولو وړاندې ډیټا انکرپټ کړل شي.

د انکرپشن سافټویر:

VeraCrypt: د دې لارښود د خپرېدلو تر وخته، VeraCrypt یو خوندي د پرانیستې سرچینې پروګرام دی چې ډیټا انکرپټ کوي او فایلونه د کاروونکي پر کمپیوټر باندې ساتي. یوازې کاروونکی کولی شي چې د یوې کیلي په کارولو سره ډیټا وګوري. VeraCrypt ډیټا، فایلونه او فولډرونه انکرپټ کولی شي، بلکې مکمل حجمونه لکه یو ایس بي فلشونه، هارډ ډرایو یا د هارډ ډرایو یو څه برخې انکرپټ کولی شي. دا سافټویر پر وینډوز، مک او لاینکس (Windows, Mac and Linux) باندې کارول کېدلی شي.

VII. په خوندي توګه د ډیټا پاکول

کله چې یو کاروونکی له یو کمپیوټر، ځیرک موبایل، ډیجیټل کمرې یا بلې وسیلې څخه ډیټا حذف کوي، نو ډیټا له منځه تللې نه ده. حذفول په ساده توګه ډیټا له کاروونکي څخه پټوي، خو له وسیلې څخه یې نه پاکوي.

په دې برخه کې تشریح کېږي چې ډیټا څنګه په خوندي ډول او د تل لپاره پاکه کړل شي، او د امنیتي سکن کولو سره تړلې اساسي اړخونه تر پوښښ لاندې نیسي، چې پروسه څنګه ترسره شي، او د معلوماتو د پاکولو لپاره کوم خوندي پروګرامونه او اپلیکېشنونه کارول کیدلی شي چې بېرته راونه ګرځول شي.

د لاندې کلیدي اصطلاحاتو ترمنځ توپیر باندې پوهیدل مهم دي:

له منځه وړل (Deleting)	پاکول (Erasing)	مینځل (Wiping)	(Shredding)
کله چې یو شی له یوې وسیلې څخه حذف کړل شي، په ساده توګه پټېږي. موجودیت یې نه محوه کېږي – بېرته ترلاسه کیدلی شي.	د ډیټا پاکول، ډیټا له عملیاتي سیستم څخه ورکوي. له پاکولو وړاندې، ډېری وختونه کاروونکي یو اخطار ترلاسه کوي چې وایي دا ډیټا بېرته ترلاسه کیدلی نه شي. دا چې عملیاتي سیستم یاده ډیټا لیدلی نه شي، نو کله چې یې منځپانګه وکتل شي ډرایو تش وي. ډیټا د «wiping» یا «shredding» له طریقه پاکیدلی شي.	کله چې یو هارډ ډرایو یا د ذخیرې وسیله «ومینځل» شي، هر څه چې په کې وي پاکېږي، د هغې ډیټا په شمول چې کاروونکی مخکې له منځه وړې وي خو بیا هم بېرته ترلاسه کیدلی شي.	شلول یا ټوټه ټوټه کول، کله چې ډیټا (معمولاً یو یا ډېر فایلونه یا فولډرونه ټوټه کړل شي، یوازې ټاکلي شیان پاکېږي، نور څه نه.
"پټ مې کړه، خو که دې بېرته اړتیا شوه، همدلته به یم".	"ډاډه یاست؟ بیا مې هیڅکله لیډلی نه شې!".	"زه غواړه چې هر څه پاک کړم ".	"زه غواړم چې یوازې او یوازې همدا فایل پاک کړم".

عامې پوښتنې:

پوښتنه	
آیا له ډیسکټاپ (desktop) څخه د ډیټا حذفول او د ریسایکل بین (Recycle Bin) تشول په دې مانا دي چې فایلونه په دایمي او نه راګرځیدونکې توګه له کمپیوټر یا موبایل څخه حذف شوي دي؟	
نه	هو

نه. د ډیټا حذفول او د ریسایکل بین تشول یاده ساحه د «لاسرسي وړ» په توګه په نښه کوي، مګر تر هغه پورې چې «د لاسرسي وړ ساحه» په نویو معلوماتو سره ډکه نه کړل شي، یاده ډیټا بېرته راګرځول کیدلی شي.

پوښتنه

آیا د یو هارډ ډرایو فارمټ کول ډیټا په دایمي او نه راګرځیدونکې توګه حذفوي؟

نه	هو

نه. بیافارمټ کول (Reformatting) د ډیټا له منځه وړلو غوره طریقه ده – د پاکولو نه. د ریفارمټینګ پروسه پر یوه وسیله باندې ټوله ساحه د لاسرسي وړ په توګه په نښه کوي؛ په هر حال، یاده ډیټا بیا هم تر هغه وخته راګرځول کیدلی شي چې په نویو معلوماتو سره ډکه شوې نه وي. که چېرته همدغه کاروونکی پلان لري چې یاد ډرایو بیا وکاروي نو دا د منښت وړ پروسه ده، خو دا په اتومات ډول حساس معلومات له منځه نه وړي.

د حذف شوو فایلونو بیا راپیدا کولو تخنیکونه ورځ تر بلې پرمختګ کوي، او د فرضي «حذف شوو» فایلونو (انځورونو، اسنادو، ویډیوګانو، او داسې نورو) ډېر ډولونه راګرځول کیدلی شي. د ډیسک مینځل یا ټوټه کول ډاډ ورکوي چې د ساده حذفولو په واسطه ایجاد شوې «د لاسرسي وړ» ساحه ډکه شوې ده، چې یاده ډیټا له راګرځولو څخه وتلې ده.

د وسایلو د پاکولو طریقه:

د یو (وینډوز) کمپیوټر د پاکولو لپاره (مؤقت فایلونه حذف کړئ او د سیستم فایلونه پاک کړئ)، په لاندې طریقې سره د سیستم **د ډیسک د پاکولو وسیله** وکاروئ:

- (Start Menu) ته ورشئ، بیا (All Programs)، بیا (System Tools) ته، بیا «Disk Cleanup» انتخاب کړئ (یا «Disk Cleanup» د لټون بکس کې ولیکئ، چې د اپلیکېشن موقعیت پرانیزي).

په دایمي توګه د ډیټا له منځه وړلو طریقه:

د ډیټا له منځه وړلو تر ټولو مهمه برخه د معلوماتو د طبقو له منځه وړل او په نوې ډیټا سره یې ځای نیول دي. دا چاره په دایمي توګه د ډیټا د راګرځولو د امکان مخنیوی کوي.

- Eraser: پاک کوونکئ د وینډوز لپاره یوه امنیتي وسیله ده کوم چې تاسو ته اجازه درکوي چې په بشپړ ډول خپل له هارډ ډرایو څخه حساس معلومات لرې کړئ.
- BCWipe: د معلوماتو د پاکولو او لرې کولو پروګرام.

که تاسو د خپل کمپیوټر سیستم تصفیه کوئ، نو سپارښتنه کیږي چې تاسو هارډ ډرایو او RAM لرې کړئ او دا چې دوی په جلا او خوندي توګه ویجاړ شوي څکه چې کیدای شي ډیټا ولري.

VIII. د فیشینګ مخنیوی کول

فیشینګ «Phishing» چې برېښنايي فریب، برېښنايي غوښتنه، او برېښنايي غلا هم ورته ویل کېږي د تکتیکونو او تکنیکونو یوه ټولګه ده چې د شخصي معلوماتو، پاسوردونو، سوداګریزو معلوماتو، مالي حسابونو او داسې نورو د غلا کولو یا ترلاسه کولو لپاره کارول کېږي.

فیشینګ د کاروونکو تر هدف لاندې نیولو لپاره تر ټولو عام لاره ده، او د فیشینګ مخنیوی تر ټولو اسانه لاره ده چې کاروونکي یې کارولی شي چې ځانونه یې له قرباني کېدلو څخه خوندي کړي.

په ساده ټکو سره، یو بریدکوونکی د یوې غولوونکې پروسې له لارې یو کاروونکی استماروي یا د ټولنیزې انجینرۍ تکنیکونه کاروي چې قرباني وهڅوي یا یې مجبور کړي چې د بریدکوونکي غوښتنې ته ځواب ووايي. په دې غوښتنه کې معمولاً کاروونکی هڅول کېږي چې:

- یو لینک کېکاږي
- معلومات شریک کړي
- اجازه ورکړي
- په مخرب سافټویر ککړ فایلونه ښکته کړي

بریدکوونکی معمولاً د هدف لپاره انتظار وباسي چې تېروتنه وکړي، بیا د قرباني معلومات ترلاسه کولی او د هغه□هغي حسابونو ته لاسرسی لرلی شي.

د فیشینګ ډولونه

فیشینګ ډېر ډولونه لري چې یو څو یې لاندې ذکر شوي دي:

نېزه يي فیشینګ (Spear phishing)

یو پیچلی تکنیک دی چې یو ځانګړی شخص یا یوه ډله تر هدف لاندې نیسي. بریدکوونکی د قرباني په اړه معلومات راټولوي او بیا یې کاروي چې یو داسې پیغام جوړ کړي چې حقیقي وبرېښي. دا ډول فیشینګ په عمومي توګه د برېښنالیک له لارې ترسره کېږي چې قرباني تر هدف لاندې نیسي.

غټ ښکار کول (Whaling)

د نېزه يي فیشینګ تکنیک دی چې په ځانګړې توګه په شرکتونو یا ادارو کې اغېزناک او ځواکمن خلک تر هدف لاندې نیسي.

(Pharming)

یو ډول فریب دی چې برید کوونکی په کې قرباني له یو اصلي/مشهور سایټ څخه یو جعلي سایټ ته رهنمایي کوي چې په مخرب سافټویر ککړ وي. کله چې قرباني سایټ ته ننوځي نو معلومات يې غلا کېږي.

ټکول (Smishing)

د لنډو پیغامونو کارول چې یو قرباني وغولوي او ویې هڅوي چې د حسابونو په اړه خپل معلومات افشاء کړي، د ګڼ-فکتوري تصدیق شمیرې ترلاسه کړي، یا د قرباني وسیلې ته مخرب سافټویر ښکته کړي.

د لټون انجن فیشینګ (Search engine phishing)

بریدکوونکی پر انټرنیټ باندې یو ویب سایټ جوړوي، د لټون پر انجن یا ټولنیزو رسنیو باندې يې خپروي، او ارزانه نرخونه وړاندې کوي، قرباني هڅوي چې د یو جنس لپاره تادیه وکړي. قرباني ورته د خپل بانک د حساب معلومات داخلوي چې دوی یې غلا کوي او کاروي.

غږیز فیشینګ (Voice phishing)

بریدکوونکی یو ټیلیفوني زنګ کاروي چې قرباني وغولوي چې باور وکړي چې زنګ وهونکی له یوې رسمي ادارې څخه زنګ وهي چې له قرباني څخه هغه معلومات ترلاسه کوي چې دوی یې غواړي.

له ډیجیټل فیشینګ څخه د ځان ژغورلو طریقه

د فیشینګ او د فیشینګ ایمیلونو په اړه نور معلومات دلته ترلاسه کیدای شي.

ټول کاروونکي باید محتاط اوسي او لاندې لارښوونې تعقیب کړي:

١. **هیڅ وخت خپل شخصي یا حساس معلومات** له نورو سره **مه شریکوئ**، او په هیڅ ډول شرایطو کې یې پر ټولنیزو رسنیو مه خپروئ.

٢. **په هیڅ ډول شرایطو کې** د پیغامونو، بریښنالیکونو، یا د ټولنیزو شبکو له سایټونو څخه **ترلاسه شوو ګواښونو ته ځواب مه وایئ.** له ګواښونکو سره له هیڅ لارې تعامل مه کوئ.

٣ **هیڅ وخت ترلاسه شوي لینکونه** له ارزولو وړاندې **مه پرانیزئ**، حتی که له نږدې کسانو څخه هم درته راغلي وي.

الف. د لینکونو او فایلونو د ارزونې لپاره Virus Total وکاروئ. له رارسیدلو سره سم لینک مه کېکاږئ – لینک کاپي کړئ، ویبسایټ پرانیزئ، لینک د «URL Links» کړکۍ کې پیسټ (Paste) کړئ، او «Enter» کېکاږئ. که چېرته پایله یې ۰ وي، لینک له ملویر څخه خالي دی. لینکونه په مستقیم ډول مه کېکاږئ – براوزر ته یې کاپي او پیسټ کړئ. که چېرته لینک د عادي منځپانګې لرونکی وي، منځپانګه به یې په براوزر کې ښکاره شي.

٤ **ډاډه اوسئ چې هغه سایټونه چې تاسو ورته لاسرسی لرئ امنیتي تصدیق لري او لینک یې په « https://» سره پیلېږي**. د براوزر په ادرس بار کې له URL سره نږدې د پډلاک آیکن (padlock icon) په دې مانا دی چې SSL هغه ویبسایټ خوندي کوي چې کاروونکی یې ګوري. SSL د انټرنیټ اتصالات خوندي ساتي او غیرمجاز کاروونکي د دوه سیستمونو ترمنځ د انتقالیدونکو معلوماتو له لوستلو یا تعدیلولو څخه منع کوي.

٥ **د برېښنالیکونو او لنډو پیغامونو ادرس او شمېره وګورئ**. ډېری وختونه بریدکوونکي په ادرسونو کې لاسوهنه کوي چې د مشهورو اړیکو په څېر ښکاره شي، څو که له نږدې وکتل شي له هغه ویبسایټ یا شخص سره سمون نه خوري چې دوی یې تمثیل کوي.

٦ **ټول خدمتونه چې تاسو په کې ګډون کړی ستاسو نوم پېژني، او د دوی اړیکو کې به ستاسو نوم شامل وي**. هر هغه پیغام چې د «ګرانه ګډون کوونکیه»، «مهربانه پېردونکیه» یا ورته جملې ولري ښايي غولوونکی پیغام وي: په اداره کولو کې یې احتیاط وکړئ.

٧ **هره تحفه یا انعام چې تاسو یې ترلاسه کوئ فریب دی**، که چېرته تاسو په کومه سیالۍ کې ګډون نه وي کړی. هیڅ وخت ورسره مه ښکېلېږئ.

٨ **که چېرته تاسو یو برېښنالیک یا نورې اړیکې ترلاسه کوئ چې د حساسو معلوماتو غوښتنه کوي، په مستقیمه توګه له لېږونکي سره له یوې بلې لارې اړیکه ونیسئ چې د پیغام په اړه معلومات ترلاسه کړئ.**

٩ **له انټرنیټي امنیت او د ملویر ضد پروګرامونو** سره مو وسایل خوندي کړئ، او **«مات شوي» یا غلا شوي سافټویرونه مه نصبوئ.**

١٠ پر ټولو حسابونو مو **دوه-پړاوه تائید فعال کړئ.**

IX. مأخذونه او د لوست نور مواد

د نورو معلوماتو، سرچینو، او دوامداره اپډیټ لپاره، لاندې سرچینې وګورئ:

١. **افغانستان دپاره دیجیتلی مصونیت لارښود** (پښتو)- دا لارښود خطر، د مخنیوی پړاوونه، د ځواب ورکولو پړاوونه او مهمو پریکړو په اړه مالومات وړاندی کوي.

٢. **د افغانستان د بشری حقونو مدافعینو دپاره د آنلاین خوندیتوب سرچینې** (پښتو)- دا مالومات تاسو سره مرسته کوي چې د کړکیچونو د زیاتوالي په وخت کې خپل آنلاین خوندیتوب ډاډه کړی.

٣. **د ټولنیزو رسنیو خوندیتوب** (پښتو)- د زیرکو تیلیفونونو او پیام لیږلو د اپلیکیشنونو د خوندیتوب په اړه مالومات.

٤. **د قوي پسورد جوړول** (پښتو)- د قوی پسورد جوړولو پړاونو په اړه مالومات.

٥. **د بروزر خوندیتوب** (پښتو)- بروزرونه څنګه ناپیژندلی حالت ته بدل کړو او د VPN څخه د ګټې اخیستنې په اړه نوری لازمی سپارښتنې.

٦. **د خطرونو پیژندنه** (پښتو)- څنګه کولای شی چې په مجازي فضا کې د خپل ځان [دیتا] ساتنه وکړی.

٧. **د بیومتریک د مالوماتو څخه د ناوړه ګټې اخیستنی** (دری - پښتو)- د بیومتریک وخت کی څه وکړو او د څه نه ډډه وکړو.

٨. **د ډیجیتلي خوندیتوب دپاره لارې چارې** (دری)- د یو فایل د ځای د پټولو، د دیتا او مالوماتو خوندیتوب، د بدو سافت ویرونو په وړاندې ساتنه او د فایلونو آنلاین ساتنې په اړه مالومات.

٩. **ډیجیتل تاریخچه یا مخینه پاکول** (پښتو)- د ایمیل او ټولنیزو رسنیو د اکونټونو پاکول او ساتنه.

١٠. **د انټرنت بندیدل او بندښت** (پښتو)- د VPN دکارولو او د انټرنت د بندیدو په حال کی خوندي اړیکه.

١١. **د مدني ټولنې فعالانو دپاره لارښود** (دري او انګریزی)- د خطرونو ډک چاپیریال کی د مدافعې په اړه مالومات.

١٢. **د لومړی کرښې مدافعین** (دری، عربي او انګلیسي) – د بشر حقونو د مدافعینو لپاره د ډیجیټل او نورو امنیتي خطرونو په اړه معلومات او مرسته.

١٣. **امنیت په یو بکس کې** (دری، عربي او انګلیسي) – د بشر حقونو د مدافعینو لپاره د ډیجیټل او نورو امنیتي خطرونو په اړه معلومات او مرسته.

١٤. **ځارونکې د ځان دفاع** (پښتو، عربي او انګلیسي) – د خوندي آنلاین اړیکو لپاره لارښوونې، وسایل او طریقې، د الکترونیک فرنټییر فاونډېشن له خوا.

١٥. **د دیجیتلی امنیت پیښو په وخت کی د اړیکو شمیرې** (انګریزی)- د دیجیتلی امنیت پیښې په وخت کې چټک ځواب ورکول.

X. بیړنۍ غبرګون (Emergency Assistance):

د مهربانۍ له مخې د بیړنۍ غبرګون په اړه لاندې آدرسونو ته مراجعه وکړی.

۱. د لومړۍ کرښې مدافعین: (انګریزی) Emergency Contact | Front Line Defenders

۲. بی پولې خبریالان: (دری) تماس با ما | RSF

۳. د افغان خبریالانو د خوندیتوب کمیټه: (پښتو) Pashto | Afghan Journalists Safety Committee (safety-committee.org)

۴. د ښځو د سولې او بشردوستانه فنډ (WPHF) د بشري حقونو ښځینه مدافعینو (WHRDs) لپاره تمویل کړکۍ: (پښتو) د ښځو د سولې او بشردوستانه وجهي صندوق (WPHF) د بشري حقونو د ښځینه مدافعینو (WHRDs) لپاره تمویل دریځه - Women's Peace and Humanitarian Fund (wphfund.org)

۵. د کړکیچ د غبرګون فنډ، مدني ټولنې فعالینو سره سمدستي مرسته: (انګریزی) Crisis Response Fund (civicus.org)

۶. د اروپایی اتحادیې د بشري حقونو د مدافعانو میکانیزم: (انګریزي) ProtectDefenders.eu - You have the right to defend rights

XI. د سایبري امنیت د اصطلاحاتو لړ

مګر دا چې په بل ډول یې یادونه شوې وي، لاندې تعریفونه بنایي د ملګرو ملتونو د ټرمینالوژۍ په ډیټابیس (UNTERM) کې هم موندل شي، چې دلته د لاسرسي وړ دی.

- **اډویر (Adware):** د سافټویر اپلیکېشن یو ډول دی چې کله روان وي نو یو څه اعلانات ښکاره کوي. ځینې وختونه د سافټویر مالکان د خپل سافټویر وړیا نسخه په دې شرط وړاندیز کوي چې تاسو به اعلانات ګورئ، دوی ته پر اعلان باندې د کلیک کوونکو خلکو د شمېر پر بنسټ پیسې ورکول کېږي. ډېری وختونه د ورته سافټویر تادیه شوې نسخه هم موجوده وي چې له اعلانونه نلري.

- **پټه ذخیره (Cache):** د ذخیرې لپاره مؤقته ساحه ده چې د چټک لاسرسي لپاره په کې ډېری وختونه کارول کیدونکې ډیټا ذخیره کېږي.

- **مات شوی سافټویر (Cracked software):** یو «مات شوی» یا «patch» شوی پروګرام دی چې د دې لپاره طرحه شوی وي چې د یو اختصاصي پروګرام ازماینښتي دوره فعاله، ثبت یا تمدید کړي چې په معمول ډول د غلا او غیرمجازي کارونې د مخنیوي لپاره یوې مسلسلې شمېرې ته اړتیا لري. د «مات شوي» یا «patch» شوي سافټویر کارول تل غیرقانوني کار دی.[۵]

۵ وګورئ Software cracking - Wikipedia.

- **د انکرپشن ټکنالوژي (Encryption technology):** کاروونکی جوګه کوي چې پر یو ایس بي ډرایو، موبایل، فلش دیسک، پین ډرایو، سي ډي یا هارډ ډیسک باندې ثبت شوې ډېټا خوندي وساتي. انکرپټ شوی سند د پردیو ترلاسه کوونکو له خوا نه شي لوستل کېدلی یا لیدل کېدلی، که څه هم سند یې په ملکیت کې وي.

- **له یو اړخ تر بل اړخ انکرپشن (End-to-end encryption):** د اړیکو د وسایلو او خدمتونو د انکرپشن اپلیکېشن، په داسې ډول چې یوازې د وسایلو یا خدمتونو کاروونکي ساده متني پیغامونو ته لاسرسی لري. د انکرپشن زیات ډولونه د خدمتونو د وړاندې کوونکو له خوا کارول کېږي چې اړیکې په داسې ډول سره خوندي کړي چې د دربهمګړي لوري د غیرمجاز لاسرسي مخنیوی وکړي، خو د خدمتونو وړاندې کوونکي چې دا پلي کوي لا هم د کاروونکو اړوندې ډېټا ته لاسرسی لري.

- **فایروال (Firewall):** فایروال یو سیستم دی چې د دې لپاره طرحه شوی دی چې یوې خصوصي شبکې ته له غیرمجاز لاسرسي څخه مخنیوی وکړي. فایروال هم په هارډویر او هم په سافټویر، یا د دواړو په ترکیب کې کارېدلی شي.

- **آی پي ادرس (IP address):** یوه ځانګړې شمېره ده چې د معلوماتي ټکنالوژۍ وسیلې یې د دې لپاره کاروي چې د کمپیوټر پر شبکه یو بل وپېژني چې د انټرنېټ پروټوکول (IP) له معیارونو کار اخلي. د هرې ګډون کوونکې شبکې وسیله – لکه روټر، کمپیوټر، پرنټر، د انټرنېټ فاکس ماشین – باید خپل ځانګړي ادرسونه ولري. دا د یو کمپیوټر یا پر انټرنېټ باندې د بلې شبکې د وسیلې لپاره د کوڅې د پتې یا د تیلیفون شمارې معادل ګڼل کېږي. لکه څنګه چې د هرې کوڅې ادرس یا د ټیلیفون شمېره په ځانګړې توګه یوه وداني یا ټیلیفون مشخصوي، دا ډول د آی پي ادرس په ځانګړې توګه یو مشخص کمپیوټر یا پر یوه شبکه باندې د بلې شبکې وسیله مشخصوي.

- **کي‌لاګر (Keylogger):** یوه وسیله ده چې د کاروونکي فعالیت ثبتوي، لکه د تڼیو کېکاږل، او دا معلومات یو بریدکوونکي ته لېږي چې برېښنالیک یا نور میتودونه کاروي.

- **مخرب سافټویر (Malicious Software) یا «ملویر»:** دا سافټویر د دې لپاره طرحه شوی چې د یو مالک له صریح رضایت پرته د یو کمپیوټر سیستم ته نفوذ وکړي یا یې تخریب کړي. دې سافټویر ته د ایجادوونکي د تصور شوې ارادې پر بنسټ ملویر وایي، نه د کومو مشخصو ځانګړنو پر بنسټ. په دې کې د کمپیوټر وایروسونه، چینجي، ټروجن هارس، سپای‌ویر، کاذب اډویر او نور زیان‌رسوونکي او غیرمطلوب سافټویرونه شامل دي. دا د «malicious» او «software» د کلمو ترکیب دی.

- **اونین روټینګ (Onion routing):** د Tor شبکې ټیکنالوژیکي بنسټ دی. دا نوم یې د پیاز ته ورته انکرپشن جوړښت له امله ورکړی دی چې دوی یې کاروي، چې په ګڼو پردو کې څو ځلې خوندي شوی دی. د اونین روټینګ هدف د امکان تر حده محرمیت سره د انټرنېټ کارول دي، چې د ګڼو سرورونو او په هر ګام کې د دوی د انکرپټ کولو له لارې ترافیک رهنمایي کوي.[٦]

- **د پرانیستې سرچینې سافټویر (Open source software):** دا د سافټویر (اپلیکېشن او سیستم سافټویر) لپاره یوه عامه اصطلاح ده چې په کې د سرچینې کوډ د هر کاروونکي لپاره د لاسرسي وړ وي؛ یو پروګرام چې کارول کېدلی، کاپي کېدلی، څېړل کېدلی، تعدیل کېدلی او له محدودیت پرته بېرته توزیع کېدلی شي.

- **پي جي پي (PGP):** پي جي پي د «ډېر ښه محرمیت» لنډیز دی، دا د نا متقارن عامه کیلي (asymmetric public key) انکرپشن سافټویر دی چې د برېښنایي اړیکو د محرمیت او اصلیت د تامینولو وړتیا لري.

---

٦ د نورو معلوماتو لپاره د Tor پروژه وګورئ https://www.torproject.org.

- **فیشینګ (Phishing):** د آنلاین فریب او د هویت د غلا ترسره کولو لپاره یو تکتیک دی. د بېلګې په توګه یو «فیشر» یو برېښنالیک لېږي چې یوه قانوني سوداګریزه غوښتنه په کې شوې وي – لکه له یو بانک څخه چې له خپل پېرودونکي څخه غواړي چې خپل مالي معلومات تائید کړي. په دې برېښنالیک کې یو لینک ورکړل شوی وي چې داسې تمثیل کوي چې تاسو د بانک قانوني ویب سایټ ته بوځي. خو، دا سایټ جعلي وي او کله چې قرباني په کې د خپل حساب شمېرې، پاسورډ یا نور حساس معلومات ټایپ کوي، ډېټا یې اخیستل کېږي او وروسته د غله (phisher) له خوا د فریب ترسره کولو لپاره کارول کېږي.
- **رینسم‌ویر (Ransomware):** یو ډول مخرب سافټویر دی، د دې لپاره طرحه شوی دی چې یو کمپیوټر سیستم ته لاسرسی تر هغه پورې بند کړي چې یو معلوم مقدار ورته تادیه شوی نه وي. د رینسم‌ویر ځینې بڼې د سیستم پر هارډویر فایلونه انکرپټ کوي (لکه cryptoviral extortion)، په داسې حال کې چې ځینې یې ښايي په ساده توګه سیستم قفل کړي او داسې پیغامونه وښیي چې موخه یې د تادیې لپاره د کاروونکي مجبورول وي.
- **سپای‌ویر (Spyware):** د کمپیوټر سافټویر چې د کاروونکو په اړه د دوی له خرګند رضایت پرته شخصي معلومات راغونډوي. شخصي معلومات په پټه سره د یو لړ تکنیکونو له لارې ثبتېږي چې په کې د تېیو د کېکاړلو ثبتول، د انټرنیټ د ویب لټولو تاریخچه ثبتول او د کمپیوټر پر هارډ ډیسک باندې د اسنادو سکن کول شامل دي.
- **ټروجن یا ټروجن هارس (Trojan or Trojan Horse):** یو پروګرام دی چې قانوني ښکاري خو کله چې نصب کړل شي غیرقانوني فعالیتونه ترسره کوي. دا پروګرام ښايي د پاسورډونو د معلوماتو ترلاسه کولو یا د راتلونکې دخولي لپاره سیستم زیانمنونکی کولو یا په ساده توګه د کاروونکي د ذخیره شوي سافټویر او ډېټا د تخریبولو لپاره وکارول شي. ټروجن هم وایروس ته ورته دی، مګر دا چې خپل ځان نه غبرګوي.
- **وي پي این (VPN):** «مجازي خصوصي شبکه» یوه شبکه ده چې د انټرنیټ له لارې یوه کنترول شوې لاره وړاندیز کوي چې یوازې مجاز کاروونکي ورته لاسرسی لري او یوازې مجازه ډېټا پرې لیږدول کیدای شي.
- **چینجي (Worms):** یوه کمپیوټري اصطلاح ده چې د ککړو پرازیتي پروګرامونو لپاره کارول کېږي، چې وایروسونو ته ورته دي، خپل ځانونه غبرګوي او پر شبکو ګرځي چې زیانمنونکي ماشینونه په اخته کړي. د وایروسونو بر خلاف، چینجي د کمپیوټر د پروګرام نور فایلونه نه ککړوي. چینجي په ورته کمپیوټر باندې کاپي ایجادوي، یا د شبکې له لارې نورو کمپیوټرونو ته کاپي ګانې لېږي.

UN Women Afghanistan Country Office
www.unwomen.org
www.unama.unmissions.org

UNAMA