د درغليو څخه ډډه کول

درغلي يوه بې ايمانه هڅه ده چې يو څوک په داسې طريقه سره وغولوئ چې د غولول کيدونکی کس په لګښت سره، چال چلونکي سړي ته مالي ګټه رسوي. دا مهمه ده چې د درغلي ځينې عام ډولونه وپيژنئ او يوه شئ چې دوی څنګه په نښه کړئ.

عمومي درغلياني

لاندې د عمومي درغليانو څلور بيلګې دي. دلته سلګونه نور هم دي. په عموم کې، د زنګونو، بريښناليکونو، يا پيغامونو څخه محتاط اوسئ چې داسې وړانديزونه چمتو کوي چې د ريښتيا کيدو لپاره ډير ښه وي، ګواښونه يا تورونه رامنځته کوي، د هجو او ګرامري غلطيو څخه ډک وي، يا د شخصي پيژندلو وړ معلوماتو (PII) غوښتنه وکړي.

غير متوقع ګټې

پدې درغليو کې، د درغلي کيدونکی کس سره اړيکه نيول کيږي او داسې ويل کيږي چې دوی په سيالۍ کې پيسې، توکي يا خدمات ګټلي چې دوی ورته ندي ننوتلي. له دوی څخه د پيسو يا د PII ليږلو غوښتنه کوي ترڅو د خپلې ګټې ادعا وکړي. دغه ګټې هيڅکله نه راځي. ستاسو د PII سره، څوک چې چال چلوي ستاسو بانکي حساب ته لاسرسی کولی شي او ستاسو سپمونې د دوی شخصي حساب ته انتقال کړي.

جعلي خيراتونه

پدې درغليو کې، د درغلي کيدونکی کس سره اړيکه د يو داسې چا لخوا اړيکه نيول کيږي چې د خيرات استازي مکاري کوي، څوک چې بيا د پيسو غوښتنه کوي. تل خيريه موسسې آنلاين ګورئ ترڅو د دوی اعتبار تاييد کړي او يوازې د پيسو بسپنه کولو لپاره خوندي بسپنې پورټلونو څخه استفاده وکړئ.

د ځنډيدلی پور ماليات

پدې درغليو کې، درغلي کيدونکی کس ته د هغه چا لخوا زنګ وهل کيږي چې د داخلي عوايدو خدماتو (IRS) يا کومې بلې دولتي څانګې نمايندګي ادعا کوي، تر هغه وخته پورې د نيول کيدو يا شړلو ګواښ کوي ترڅو فيس ور نه کړل شي. IRS به هيڅکله د PII غوښتنه کولو لپاره زنګ ونه کړي، نو خپل مه چمتو کوئ! که چيرې تاسو دا ډول زنګ ترلاسه کړئ، نو په خپل ويب لټون براوزر کې د تليفون شميره وګورئ. دا به تاسو سره پدې زده کړه کې مرسته وکړي که چيرې شميره له وړاندې څخه د درغليو په توګه راپور شوې وي. که چيرې تاسو بې زړه ياست، نو پيښه خپل د قضيې مدير ته راپور کړئ.

د نه ليدل شوي دندې وړانديزونه

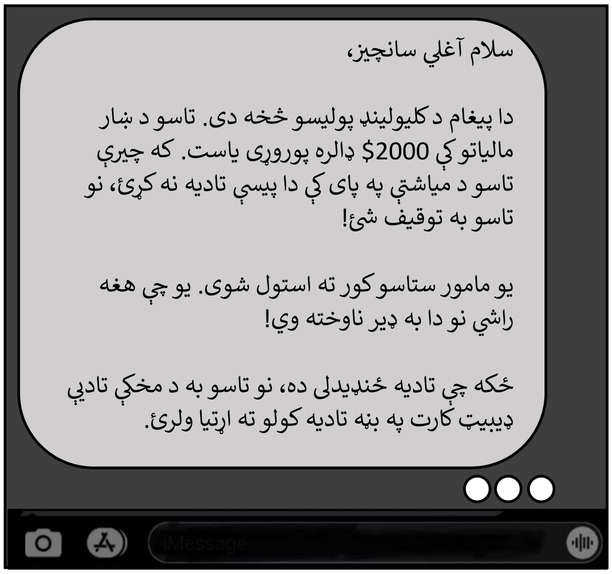
پدې درغليو کې، د درغلي کيدونکی کس سره د جعلي شرکت لخوا اړيکه نيول کيږي چې دوی په شخصي توګه مرکه درلوده يا په رسمي ډول غوښتنه کيدو څخه مخکې دوی ته د دندې وړانديز کوي. هيڅکله احتمالي کارګمارونکي ته لومړی د دوی مشروعيت تائيد کولو پرته PII مه ورکوئ.

ايا د شخصي پيژندلو وړ معلومات څه شی دی؟

د شخصي پيژندلو وړ معلومات (PII) هغه معلومات دي کوم چې يو کس په ځانګړي ډول پيژندلې شي. پدې کې لاندې شامل دي، خو لاندې ته محدود ندي:

- د ټولنيز امنيت شميرې
- بشپړ نومونه
- د زيږون نيټه
- ادرسونه
- د بانکي حساب شميرې

ايا نښې نښانې څه دي چې دا پيغام يوه درغلی ده؟



- غير رسمي لهجه
- له مخکې تادې کارټ لپاره غوښتنه وکړئ

آيا نور څه؟

HIAS

د ماشومانو څارنه

په ډیجیټل دور کې د والدینو په توګه، ستاسو د ماشومانو آنلاین فعالیت څارنه ستونزمن کیدی شي. د انټرنیټ ته د ماشومانو افشا کول مهم دي، کوم چې به د دوی د ټولنیز، تعلیمي او مسلکي ژوند یوه برخه وي. په ورته وخت کې، **دا مهمه ده چې د انټرنیټ زیان رسونکو اړخونو، پشمول د سایبر ځورونې، د نامناسب منځپانګې، مالي استحصال، او د آنلاین لوټمارانو څخه د ماشومانو ساتنه وشي**. د والدینو کنټرول او د څارنې وسیلې ستاسو د ماشومانو په ساتنه کې لازمي دي.

کلیدي اصلاحات

د نوي Android او iOS (Apple) ساوترې کې ذاتی جوړ شوي د والدینو کنټرولونه شامل دي. د والدینو د کنټرول اضافي کاریالونه وریا، یا د پیرود لپاره د کاریال په نصب کولو پلیټ فارمونو کې شتون لري (*د ایپ پلورنځي په اړه د نورو معلوماتو لپاره، 1.1 بیاکتنه وګړئ*).

سایبر ځورونې

سایبر ځورونه د متن پیغام رسونې، کاریالونو، ټولنیزو رسنیو، فورمونو، یا لوبو کې د چا په اړه د منفي، زیان رسونکي، یا غلط منځپانګې لیږل، خپور کول یا شریکول دي چیرې چې خلک کولی شي منځپانګې وګوري، ګډون وکړي، یا له نورو سره یې شریک کړي.

آنلاین لوټماران

آنلاین لوټماران بالغ آنلاین کاروونکي دي چې د کوچنیانو د موندلو او په نښه کولو لپاره د ډیجیټل ټیکنالوژۍ څخه استفادې سره د ماشومانو استحصال په لټون کې وي.

د منځپانګې فلټرونه

دا وسیلې د عمر نامناسب منځپانګې ته د ماشومانو لاسرسی محدودوي. د منځپانګې فلټرونه په ډیرو کاریالونو، آلاتو، او لټونکرو کې شتون لري.

د استفادې کنټرولونه

دا کنټرولونه وخت محدودوي چې ماشومان یې ځانګړي کاریالونو ته لاسرسی ولري، د هغه ساعتونو په جریان کې چې دوی ځانګړي کاریالونو څخه استفاده کوي، او ایا دوی په ټوله کې کاریالونو ته لاسرسی کولی یا نشي.

د ماشومانو څارنه کول

دا وسیلې والدینو ته اجازه ورکوي چې د آلاتو موقعیت تعقیب کړي، وګورئ چې ماشومان د دوی د آلاتو سره څه کوي، او د دوی د کارونې د نورو اړخونو په اړه زده کړه وکړئ.

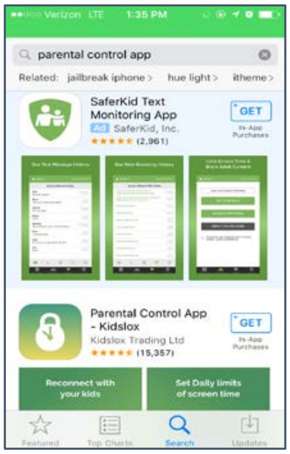
څه باید وګورئ

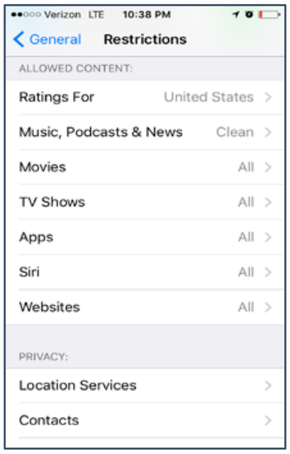
دلته ډیری لارې شتون لري چې د ماشومان، او ځوان لویانو څخه په انټرنیټ کې ناوړه ګټه اخیستل کیدی شي. د والدینو په توګه، د سایبر ځورونې او آنلاین لوټمارانو پېژندل ستاسو سره د دې په مخنیوی کې مرسته کولی شي.

ډیر کاریالونه او لوبې په کاریال کې د پیرودلو ځانګړتیا لري. دا ماشومانو ته د ریښتیني مالي پیرودونو اجازه ورکوي. د امکان په صورت کې، د والدینو کنټرول ترتیباتو تازه کولو سره په کاریال کې د پیرودونو څخه مخنیوی وکړئ او خپل بانک معلومات د کاریال پلورنځي سره د لینک کولو څخه ډډه وکړئ.

تاوتریخوالی، جنسي یا په بل ډول نامناسبه منځپانګې په انټرنیټ کې په پراخه کچه د لاسرسي وړ دي. خپلو ماشومانو ته د استفادې اجازه ورکولو څخه مخکې د ویب پاڼو، لوبو او کاریالونو په بیاکتلو سره د خپل ماشوم افشا کول محدود کړئ.

دا ممکنه ده چې خپل ماشوم ته زیان رسونکي منځپانګې محدوده کړئ، خو بشپړ مخنیوي لپاره نشئ. **ډاډمن کړئ چې په مستقیم ډول د ماشومانو سره د انټرنیټ خوندیتوب په اړه مباحثه وکړئ**. له دې مهارتونو څخه ډیر به د دوی د ژوند په نورو برخو کې ګټور وي.





HIAS

ستاسو د ډیجیټل پښې نخش اداره کول

ستاسو د ډیجیټل پښې نخښ د هرڅه بریښنایي ریکارډ دی چې تاسو یې په انټرنیټ کې ترسره کوئ. **هر متن پیغام، بریښنالیک، د ټولنیزو رسنیو پوسټ، عکس، پیرود، او د انټرنیټ لټون د تل لپاره خوندي کیږي.** دې ډیجیټل پښو نخش ته دوه پرتونه شتون لري. لومړی پرت هغه معلومات دي چې د هر انټرنیټ کارونکي لخوا لاسرسی کیدی شي. دوهم، هغه معلومات دي چې ستاسو د انټرنیټ خدمت چمتو کونکو، شرکتونو، دولتونو، او سایبر جنایتکارانو لخوا لاسرسی کیدی شي. دا پوهیدل مهم دي چې دا معلومات څنګه راټول شوي، له دې سره څه کیدی شي، او دا څنګه اداره کړو.

کلیدي اصلاحات

هدف شوي اعلانونه

ډیری ویب پاڼې ستاسو مخکې لیدل شوي ویب پاڼو څخه د محصولات اعلانولو لپاره ستاسو د ډیجیټل پښو نخش څخه استفاده کړي.

اوڅاریز شخصي شبکه (VPN)

یو VPN تاسو ته د عامه انټرنیټ اتصال څخه د یو شخصي شبکې رامینځته کولو له لارې آنلاین محرمیت درکوي. VPN د سایبر جنایتکارانو د هغه ډاټا مداخله کولو څخه مخنیوی کې مرسته کوي چې تاسو یې له خپل آلې څخه لیږئ او ترلاسه کوئ. ډیر انټرنیټ روټرونه ذاتي جوړ شوي VPN لري. د یو VPN تنظیم کول ممکن یو لږ میاشتني فیس مصرف کړي (*د راوټرونو په اړه د نورو معلوماتو لپاره، د 1.2 بیاکتنه وکړئ*).

د شخصي لټون (نا پېژندویه اکر)

کله چې تاسو یو انټرنیټ لټونګر څخه استفاده کوئ، دا ممکن هغه څه ثبت کړي چې تاسو یې ترسره کوئ، شفرونه او مالي معلومات خوندي کړئ، او له مخکې لیدل شوي ویب پاڼو څخه کوکیز ډاونلوډ کوي. شخصي لټون له دې څخه یو څه مخه نیولو کې مرسته کوي، او په ځانګړې توګه د استفادې لپاره مهم دي کله چې په عامه کمپیوټر کې یاست.

کوکیز

کوکیز د انټرنیټ لټونګر څخه لیږل شوي ډاټا ته اشاره کوي او ستاسو په کمپیوټر کې خوندي شوي. دا ویب پاڼو ته ستاسو د شفرونو او د لټون کولو مخینه په یاد ساتلو او ثبت کولو لپاره اجازه ورکوئ. که چیرې یوه ویب پاڼه تاسو ته خبرداری درکړي چې دا د کوکیز څخه استفاده کوي، د هغه ویب پاڼې په استفادې سره چې تاسو د دې لپاره اجازه ورکوي چې ستاسو مجموعي ډیجیټل پښو نخش ته لاسرسی وموئ، کوم چې ممکن د هدف شوي اعلاناتو پایله وي.

ستاسو لومړنی ډیجیټل ګام

کارګمارونکي او د ځمکې مالکان ممکن د احتمالي کارمند یا کرایه کونکي ټولنیز رسنی حساب له لارې لټون وکړي ترڅو د دوی په اړه نور معلومات زده کړي.

که چیرې یو کارونکی ستاسو Twitter، Facebook یا Instagram حساب وموئ، نو دوی به څه فکر وکړي؟

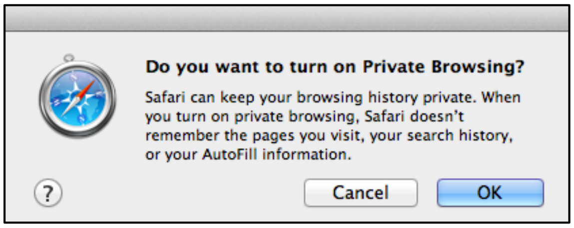
د خپل لومړني ډیجیټل ګام اداره کولو لپاره، تاسو دوه شیان ترسره کولی شي. لومړی، په ټولو ټولنیزو رسنیو حسابونو کې د خپلې خوښې محرمیت ترتیبات تنظیم کړئ. دوهم، **یوازې هغه څه خپور کړئ که چیرې تاسو یې د هرچا لیده بد نه ګڼئ**. دلته تل یوز موقع شتون لري دوی ممکن وي!

ستاسو مجموعي ډیجیټل ګام

دا نه یوازې هغه څه دي چې تاسو یې د عامه کولو اراده لرئ کوم چې ستاسو ډیجیټل ګام ته شکل ورکوي. شرکتونه، د قانون اجرا کوونکی، دولتونه، او سایبر جنایتکاران د انټرنیټ کاروونکو څخه معلومات راټولوي. **ستاسو معلومات د هدف شوي اعلاناتو رامینځته کولو څخه ستاسو د هویت غلا کولو پورې په ډیرو لارو کارول کیدی شي.**

ایا په کومو مواردو کې بنایي یو شرکت د قانون اجرا کوونکو ته ستاسو ډیجیټل ګام په اړه معلومات چمتو کړي؟ ایا دا قانونی ده؟

پداسې حال کې چې دا د شرکتونو لپاره قانوني دی چې ستاسو ډیجیټل ګام شریک کړي، نو ځینې شرکتونه د دې پر خلاف تکلاري لري. تاسو د خپل آنلاین شتون پټولو لپاره د یو VPN خدمت څخه استفادې سره، د کوکیز مخه نیولو لپاره د خصوصي لټون کولو اکر باندې تګ کولو سره، او په احتیاط سره چې تاسو آنلاین څه ترسره کوئ لخوا خپل ډیجیټل ګام خوندي کولی شي!



مالویر، ویروسونه، د ویروس محافظت او د پرچالونه

دلته ډیرې لارې شتون لري چې درغلي کوونکي او سایبر جنایتکاران کولی شي ستاسو معلوماتو ته لاسرسی ومومي. یوځل چې دوی ستاسو آلې ته لاسرسی ولري، یا ستاسو شخصي پیژندلو وړ معلومات تعقیب کړي، دوی ستاسو په نوم کریډیټ کرښې خلاصولې شي، ستاسو د چکونو حساب ته پیرودونه چارج کړي، او ستاسو د سپما حساب څخه پیسې غلا کړي. ویروسونه او مالویر لومړني وسیلې دي چې پدې هڅو کې جنایتکارانو ته د مرستې لپاره کارول کیږي. **خپلې آلې، او خپل ځان د باور لرونکي ویروس ضد ساوترې او پرچالونو سره خوندي کړئ!**

کلیدي اصلاحات

مالویر

مالویر د زیانمن ساوترۍ هر هغه شکل دي چې یوې بریښنایي آلې ته د لاسرسي یا زیان رسولو لپاره ډیزاین شوی. دا زیاتره د پیسو غلا لپاره ډیزاین شوي. د کمپیوټر ویروسونه د مالویر یوه شکل دی کوم چې سایبر جنایتکارانو ته ستاسو بانکي معلوماتو ته لاسرسی او ستاسو کریډیټ خرابولو لپاره اجازه وکوي (*د کریډیټ په اړه د نورو معلوماتو لپاره، د 4.1 بیاکتنه وکړئ*).

د کمپیوټر ویروس

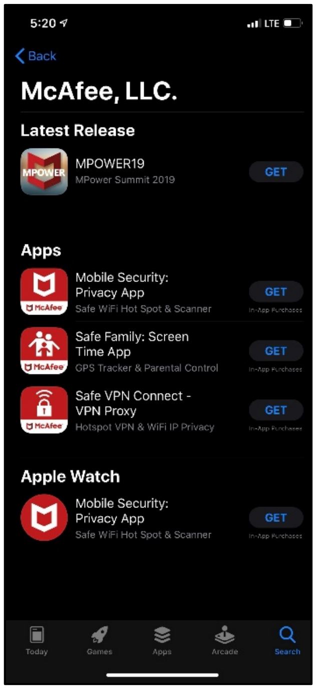
د کمپیوټر ویروس یو زیانمن ساوترۍ، یا کوډ دي چې د یوې آلې عملیاتو لارې بدلولو لپاره اراده شوي. د کمپیوټر ویروس یو زیانمن ساوترۍ، یا کوډ دي چې د یوې آلې عملیاتو لارې بدلولو لپاره اراده شوي. ویروس د وصل شوي آلاتو تر مینځ خپور کیدی، شفرونه غلا کولی، د کیلي ضربان ثبتوي، دوتني ککړوي، د بریښنالیک اړیکي سپام کوي، او حتی اله ترلاسه کوي. دوی د بریښنالیک ضمیمې، ډاونلوډ شوي دوتنو او کاریالونو، او د شریک شوي ټولنیزو رسنیو مینځپانګې له لارې خپروي.

له وایرس څخه خوندیتوب

ډیر شرکتونه، لکه نورټون، ویروس خوندیتوب ساوترۍ تولیدوي. دا د داونلوډ وړ ساوترۍ بندلونه میاشتنۍ فیس لګښت اخلي، خو د مالویر او ویروس پر خلاف قوي محافظت وړاندې کوي.

پرچال

یو پرچال ستاسو د انټرنیټ اتصال لپاره د یو ویروس ضد ساوترۍ ته ورته دی. دا د راتلونکي او بهرنی تلونکي شبکې ترافیک څارنه او کنټرولونه کوي. دا د باوري داخلي شبکو او بې باورۍ بهرنی شبکو ترمینځ خندونه هم رامینځته کوي.



ستاسو د ویروس لرلو نښې نښانې

- ډیر پیښې بریوکیزه کړکې
- ستاسو کور پاڼې ته بدلونونه
- ستاسو له حساب څخه لیږل شوي بریښنالیکونه چې تاسو لیکلې نه وي
- ډیر پیښې کمپیوټر یا برنامې ټکرونه
- د اوسط فعالیت څخه ډیر ورو
- ستاسو په آله کې نامعلوم برنامه
- غیر معمولي فعالیت

څنګه د ویروسونو او مالویر مخنیوي وکړئ

- په بریوکیزه اعلاناتو باندې مه کلیک کوئ
- د خوندي شبکې ارتباطاتو څخه استفاده وکړئ، او د هغه کمپیوټرنو سره پردي شریکول یا اتصال مه کوئ کوم چې د ویروس محافظت نه لري
- د دوتنو ډاونلوډ کولو څخه مخکې تل یې سکین کړئ
- د یو باوري ویروس محافظت ساوترۍ څخه استفاده وکړئ

HIAS

غلط معلومات

انټرنیټ معلوماتو په آسانۍ سره د لاسرسي وړ ګرځولي. دا د معلوماتو ګړندي خپرولو ته هم اجازه ورکوي. نن ورځ، تاسو د غونډېو په اړه معلومات په اسانۍ سره په آنلاین توګه موندلې شي، خو **هر هغه څه چې تاسو یې په انټرنیټ کې لولئ ریښتیا نه وي**. که تاسو په ټولنیزو رسنیو یا د یوې خبري سرچینې څخه خپل معلومات ترلاسه کړئ، تاسو باید تل هغه څه چې آنلاین لوستئ حقایق چیک کړئ ترڅو دا تائید کړئ چې ایا دا ریښتیا ده

جعلي خبرونه

جعلي خبرونه یو عصري عبارت دی چې د ټولنیزو رسنیو پلېټ فارمونو کې غلط معلومات تشریح کوي، لکه Facebook او Twitter. دا عبارت اوس مهال د افرادو او رسنیو لخوا کارول کیږي. په ساده ډول، جعلي خبرونه پدې معنا دي چې معلومات غلط دي او هیڅ د تایید وړ حقایق، سرچینې، یا اقتباسونه نه لري. جعلي خبرونه ممکن غلطۍ ته راجع کړي. د بېلګې په توګه، که چیرې د خبري سرچینه داسې معلومات شریک کړي چې حقایق یې نه وي کتل شوی، کوم چې دوی وروسته زده کوي چې غلط دي. جعلي خبرونه غلط معلومات هم کیدی شي چې په قصدي ډول شریک شوي دي. خلک ممکن حتی یو څه ته جعلي خبرونه ووایی کله چې دا په حقیقت کې ریښتیا وي.

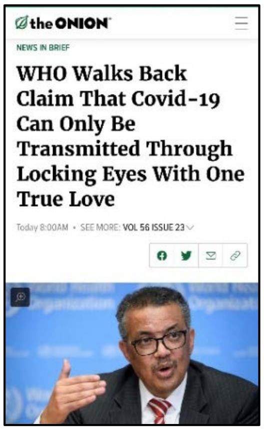
د انټرنیټ سره نا اشنا خلکو ته، ډیر طنزونه یا ملنډې، رسنۍ سرچینې ریښتینې ښکاري. د طنزي پلېټ فارمونو باندې معلومات ریښتونی نه دي. یو عام پېژندل شوی طنزي پلېټ فارم پیاز دی – تاسو دا سرچینه پدې theonion.com لوستلۍ شي.

غلط معلومات تل پیژندل اسانه نه وي. **تل د خپل خبري سرچینې په توګه باوري او یې پرې رسنۍ وتن ځای څخه استفاده وکړئ.** تاسو ممکن د خپلو خبرونو لپاره لاندې باوري ویب کاریالونو څخه د یو لیدنه غوره کړئ: د نیویارک ټایمز، وال سټریټ ژورنال، واشنګټن پوسټ، ملي عامه راډیو (NPR)، اقتصاد پوه، نیویارکر، رویټرز، اتلانټیک یا پولیټیکو.

په نهایي کې، ستاسو د خوښې رسنۍ سرچینه ستاسو پریکړه ده. تل د مختلف لړ لیدونو لوستلو هڅه کوئ. د بېلګې په توګه، ښایي ستاسو د خوښې رسنۍ سرچینه پورته لیست شوي وي. که چیرې داسې وي، نو د یو نړیوال خبري سرچینې لوستل هم په پام کې ونیسئ، لکه BBC. دا به په خبرونو کې د متحده ایالاتو او نړیوال لړ لید دواړه وړاندې کړي، او په غوره توګه به تاسو ته اجازه درکړي چې د سیاست، دولت او نورو اوسنیو غونډېو په اړه خپل نظرونه رامینځته کړئ.

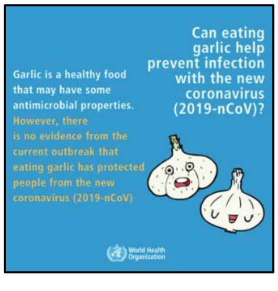
د غلط معلوماتو پیژندل

د غلط معلوماتو د پیژندلو لپاره کومه اسانه لار نشته دې، خو تاسو د لاندې ګامونو په اخستلو سره پیل کولی شي:



- وپوښتئ څه چې تاسو ولولئ
- وپوهیږئ چې کوم پلېټ فارمونه عموماً غلط معلومات وړاندې کوي
- حقایق وپلټئ

تاسو کاریالونه هم کارولې شي، لکه د Reuters حقایق کتنه، ترڅو غلط معلوماتو وپیژنئ: www.reuters.com/fact-check.

انفوډیمک:

په مارچ 2020 کې، د روغتیا نړیواله سازمان (WHO) د کورونا ویروس وبا په اړه په انټرنیټ کې موندل شوي غلط معلومات د یو انفوډیمک په توګه وبلل. په ټولنیزو رسنیو کې موندل شوي غلط معلوماتو سره د مبارزې لپاره، WHO د کورونا ویروس په اړه په پراخه کچه خپاره شوي افواګانو د افشا کولو لپاره یو کمپاین پیل کړ. د بېلګې په توګه، د هوږې خوړل ثابته ندې چې خلک به د کورونا ویروس څخه خوندي وساتي.