# آنلاين کي خوندیتوب

## ولي زما لپاره سایبري امنیت مهم دی؟

انټرنټ او ټولنیزې رسنۍ حیرانونکي پلیټ فارمونه دي چې له موږ سره د مالوماتو شریکولو او د ملګرو او کورنۍ سره په اړیکه کې په پاتې کیدلو کې مرسته کوي.

په همدې ډول، مجرمین او نور غیرقانوني سازمانونه یې هم ستاسو د پیسو، ستاسو د مالوماتو د ترلاسه کولو یا ستاسو د ویروسونو لپاره کاروي.

دوی کولی شي د نړۍ له هر ځای څخه یې وکاروي، په ډیرو ژبو په روانه ډول سره خبرې کولې شي او د قناعت وړ جعلي ویب پاڼې جوړوي. دوی به تاسو سره د بریښنالیک، ټولنیزو رسنیو او متني پیغام له لارې اړیکه ونیسي او دوی به هڅه وکړي چې تاسو د ویرې یا اندیښنې احساس وکړي، نو پدې حالت کې به تاسو په روښانه ډول فکر نه کوئ.

دا ټول پدې مانا دي چې تاسو اړتیا لرئ چې چمتو اوسئ او تل د هغو چلونو څخه خبر واوسئ چې دوی یې کاروي.

## هغه کومې عامې ستونزې دي چې زه ښایي آنلاین ورسره مخ شم؟

دا ځینې خورا عام حالتونه دي چې موږ یې ګورو.

- تاسو یو شکمن بریښنالیک یا لیکلي پیغام ترلاسه کوئ چې له تاسو څخه غوښتنه کوي چې په لینک کلیک وکړئ.
  - دا لینکونه داسې ډیزاین شوي چې ډیر وخت جعلي ویب پاڼو ته لاره هواروي تر څو ستاسو حساب یا مالي مالومات غلا کړي.
- تاسو ته یو شکمن زنګ راځي چې د شخصي مالوماتو غوښتنه کوي.
  - پورته ذکر شوی زنګ وهونکی به ځان ستاسو د بانک کارکوونکي معرفي کړي او مالومات به وغواړي.
- یو شخص له تاسو سره اړیکه نیسي او ځان یو چارواکي شخص درپیژني، ا هڅه به وکړي چې تاسو کوم کار وکړي.
  - ډیر وخت دا شخص یو ډول ګواښ کوي.
- یو څوک ستاسو یو یا ډیرو آنلایني حسابونو ته ننوځي (د بیلګې په توګه: بریښنالیک یا ټولنیزې رسنۍ).
  - که څوک ستاسو آنلاین حساب ته ننوځي دوی کولی شي مالومات غلا کړي، د پیسو د لیږلو او مصرفولو لاره بدله کړي، او په بالقوه توګه ستاسو ملګري یا کورنۍ په نښه کړي چې ځان ستاسو په ټوګه ورته معرفي کړئ.
- ستاسو د کریډیټ کارت مشخصات غلا شوي، یا ستاسو پیسې په جعلي پلور یا پانګونه کې غلا شوي دي.
  - درغلګر هیله لري چې تاسو به یوه ښه معامله وګورئ او پرته له فکر کولو څخه به پیسې ورکړئ. یا کیداي شي د یوې ریښتینې ویب پاڼې داتا ته لاسرسي وموميې چې ستاسو مشخصات آنلاین افشا شوي وي.

دلته نورې سناریوګانې هم شته:
Get help now – Own Your Online

## زه څرنګه آنلاین خوندي پاتې شم؟

- **اوږده او خانګړي پاسوردونه.**
  - هر څومره چې پاسورډ اوږد وي، هغومره قوي وي.
  - د څلورو غیرمعمولي کلمو په یوځای کولو سره د 16 حروفو څخه ډیر د یادولو وړ پاسورډ جوړ کړئ (د بیلګې په توګه: TriangleRhinoOperationShoes) او که اړتیا وي نو شمیرې، لوی توري او سمبولونه اضافه کړئ (د بیلګې په توګه: Triangle&"Rhino"Operation2Shoes).
  - مهمه دا ده چې خپل پاسوردونه مه تکراروئ. که یو مجرم ستاسو یو پاسورډ ترلاسه کړي نو دوی به یې په نورو حسابونو کې هم د کارولو هڅه وکړي.
  - د پاسورډ مدیر سیستم وکاروئ ترڅو ستاسو پاسوردونه په یاد ولرئ او نوي پاسوردونه جوړ کړئ.
  - ښه پاسوردونه جوړ کړئ - خپل آنلاین مالکیت ولرئ

- **دوه فکتوره تصدیقول یا د کارونې اجازه فعال کړئ.**
  - دا د مالوماتو یوه اضافي ټوټه ده – معمولا ستاسو په تلیفون کې یو کوډ – چې تاسو ویب پاڼې ته د ننوتلو پرمهال ورته اړتیا لرئ.
  - دا تخنیک خورا پیاوړی دی او کولی شي ستاسو حسابونو ته د ننوتلو ډیری هڅې ودروي.
  - مور د 'تصدیق کوونکي اپ' کارولو وړاندیز کوو، چیرې چې د دې ملاتړ کیږي.
  - دوه فکتوره تصدیق کوونکي ((two-factor authentication (2FA)) تنظیم کړئ – خپل آنلاین مالکیت ولرئ
- **آنلاین شخصي پاتې شئ.**
  - په ټولنیزو رسنیو کې د خوندي پاتې کیدلو لپاره تر ټولو غوره انتخاب دا دی چې، ستاسو د محرمیت ترتیبات فعال کړئ.
  - دا به د تصادفي خلکو او د هغه سایبري مجرمینو مخه ونیسي، چې ستاسو د پوسټونو د لیدلو یا تاسو ته د پیغامونو لیږلو توان ولري.
  - بیا هم د ځان، خپلې کورنۍ یا خپلو ملګرو په اړه د شخصي مالوماتو په پوسټ کولو کې محتاط اوسئ.
  - ډاډ ترلاسه کړئ چې په اړیکه کې هغه شخص چې د ځان ادعا کوي هماغه شخص وي.
  - د جعلي ملګرو غوښتنو څخه باخبره اوسئ. د هغو خلکو په اړه محتاط اوسئ چې ادعا کوي ژورنالیستان دي یا نور څه چې تاسو یې ښه نه پیژنئ.
  - خپل محرمیت آنلاین خوندي کړئ – خپل آنلاین مالکیت وکړئ
- **هر څه نوي وساتئ.**
  - کله چې تاسو خپل تلیفون، کمپیوټر یا سافټویر تازه کوئ، دا په امنیت کې هر ډول درځونه هم بندوي.
  - مجرمین ټل وسیلو ته د ننوتلو لپاره لاري لټوي او دا تازه کول دا خلاوي او درځونه ډکوي.
  - خپل وسایل په منظم ډول بیا ریستارت (بیا چالان) کړئ.
  - نوي کولو ته دوام ورکړئ – خپل آنلاین مالکیت ولرئ
- **له درغلیو څخه باخبره واوسئ.**
  - غوره مشوره دا ده چې له دې درغلیو څخه خبر واوسئ او د هغوی څارنه کوئ.
  - که کوم څه غلط ښکاري، له هغه چا سره اړیکه مه نیسئ چې تاسو سره یې اړیکه نیولې ده. په ځانګړي توګه محتاط اوسئ که دوی د پیسو غوښتنه کوي، حتی که دوی دوستانه هم ښکاري.
  - د نامالومو لینکونو او بریښنالیکونو پټې وګورئ (د مثال په توګه: ستاسو بانک به تاسو ته د Gmail حساب څخه بریښنالیک ونه لیږي).
  - *هیڅکله* په لیکنی پیغامونو کې په لینکونو کلیک مه کوئ.
  - یوازې له رسمي اپ پلورنځیو څخه خپلو وسیلو ته اپونه ډاونلوډ کړئ.
  - که شک لري، له هغه اداري سره اړیکه ونیسئ چې تاسو سره مستقیم اړیکه نیسي او هغه لینکونه یا تلیفون شمیرې مه تعقیبوئ چې تاسو ته لیږل کیږي.
  - هڅه وکړئ چې د ځان، خپلې ټولنې او هر هغه ګروپ لپاره چې تاسو ورسره تړاو لرئ د آنلاین امنیتي خطرونو څخه باخبره واوسئ.
- **خپل مالومات خوندي کړئ.**
  - د کوډ شوي پیغام رسولو اپونو څخه کار واخلئ، لکه سیګنال (Signal). دا به د هر چا څخه ستاسو د پیغامونو د لوستلو مخه ونیسي.
  - یوازې له هغه ویب پاڼې سره مالومات شریک کړئ که چیرې پته یې د HTTPS سره پیل شي. S د "خوندیتوب" لپاره دی او پدې مانا چې ستاسو او ویب پاڼې ترمنځ لیږل شوي هر ډول مالومات کوډ شوي دي.
  - د مجازی خصوصي شبکې ((virtual private network (VPN) کارولو په اړه فکر وکړئ کوم چې کولی شي ستاسو مالومات خوندي وساتي او ستاسو موقعیت پټ کړي.
  - وګورئ چې ستاسو اپونه کومو مالوماتو او اجازې ته لاسرسی لري. د بیلګې په توګه، د فټنس اپ ستاسو اړیکو ته، لاسرسی ته اړتیا نلري.

## که زه د درغلي يا له دې هم د بدتر څه ښکار شم نو څه وکړم؟

ډير ځايونه شتون لري چې تاسو کولی شئ مرسته تري وغواړي. دا سازمانونه به ستاسو مشخصات له بل چا سره شريک نه کړي، پرته لدې چې تاسو خپله رضايت ورکړئ.

- تاسو کولی شئ د سايبري پيښو راپور د CERT NZ پورټل له لارې NCSC ته ورکړئ او مورِ کولی شو مرسته وکړو يا تاسو سره له بلې اداري سره په اړيکه کې کړو:
  د پيښې راپور ورکړئ | CERT NZ
- که ستاسو پيسې ورکې شوې وي، نو تاسو بايد سمدلاسه له خپل بانک سره اړيکه ونيسئ.
- د درغلۍ ليکنې پيغامونه وړيا 7726 ته ليږل کيدی شي، چې د کورنيو چارو وزارت لخوا سمبالېږي.