Community Resilience to Foreign Interference

National Cyber Security Centre

# آنلاین کې خوندیتوب

## ولې زما لپاره سایبري امنیت مهم دی؟

انټرنټ او ټولنیزې رسنۍ حیرانونکې پلیټ فارمونه دي چې له موږ سره د مالوماتو شریکولو او د ملګرو او کورنۍ سره په اړیکه کې په پاتې کېدلو 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 ویرولو لپاره کاروي.

دوی کولی شي د نړۍ له هر ځای څخه یې وکاروي، په ډېرو ژبو په روانه ډول سره خبرې کولی 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 ښايي 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 درپېژني، ا هڅه به وکړي چې تاسو کوم کار وکړي.**
  ډیر وخت دا شخص یو ډول ګواښ کوي.
- **یو څوک ستاسو یو یا ډیرو آنلاینې 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 توګه ورته معرفي کړئ.

- **ستاسو د کرېډېټ کارت مشخصات غلا شوي، یا ستاسو پیسي 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 ومومي چې ستاسو مشخصات آنلاین افشا شوي وي.

دلته نورې سناریوګانې هم شته: [Get help now – Own Your Online](Get help now – Own Your Online)

## زه څرنګه آنلاین خوندي پاتې شم؟

### اوږده او ځانګړي 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 پاسورډونه 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 پاسورډونه په یاد ولرئ او نوي پاسورډونه جوړ کړئ.
- [ښه پاسورډونه جوړ کړئ - خپل آنلاین مالکیت ولرئ](ښه پاسورډونه جوړ کړئ - خپل آنلاین مالکیت ولرئ)

### دوه فکتوره تصدیقول یا د کارونې اجازه فعال کړئ.

- دا د مالوماتو یوه اضافي توټه 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.
- موږ 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](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 تل وسیلو ته د ننوتلو لپاره لارې لټوي او دا تازه کول دا خلاوې او درځونه ډکوي.
- خپل وسایل په منظم ډول بیا ریستارټ (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 ښارنه کوئ.
- که کوم څه غلط ښکاري، له هغه چا سره اړیکه مه نیسئ چې تاسو سره یې اړیکه نیولې ده. په ځانګړې توګه محتاط اوسئ که دوی د پیسو غوښتنه کوي، حتی که دوی دوستانه هم ښکاري.
- د نامالومو لینکونو او بریښنالیکونو پټې وکورئ (د مثال په توګه: ستاسو بانک به تاسو ته د Gmail حساب څخه بریښنالیک ونه لیږي).
- هیڅکله په لیکنۍ پیغامونو کې په لینکونو کلیک مه کوئ.
- یوازې له رسمي اپ پلورنځیو څخه خپلو وسیلو ته اپونه ډاونلوډ کړئ.
- که شک لرئ، 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 بېلګې په توګه، د فټنس اپ ستاسو اړیکو ته، لاسرسی ته اړتیا نلري.

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

ډیر ځایونه شتون لري چې تاسو کولی شئ مرسته ترې وغواړې. دا سازمانونه به ستاسو مشخصات له بل چا سره شریک نه کړي، پرته لدې چې تاسو خپله رضایت ورکړئ.

تاسو کولی شئ د سایبري پیښو راپور د CERT NZ پورټل له لارې NCSC ته ورکړئ او مور کولی شو مرسته وکړو یا تاسو سره له بلې اداري سره په اړیکه کې کړو: [د پیښې راپور ورکړئ | CERT NZ]

که ستاسو پیسې ورکې شوې وي، نو تاسو باید سمدلاسه له خپل بانک سره اړیکه ونیسئ.

د درغلۍ لیکنې پیغامونه وړیا 7726 ته لیږل کیدی شي، چې د کورنیو چارو وزارت لخوا سمبالیږي.