Community Resilience to Foreign Interference

National Cyber Security Centre

# ستاسو د سازمان آنلاین خوندي ساتل

## ولې د ټولنې د ډلو او سازمانونو لپاره سایبري امنیت اړین دی؟

دا پاڼه مشورې او ځینې ګامونه لري چې تاسو یې کولی شئ د خپلې ټولنې ډلې یا سازمان د سایبري امنیت د ګواښونو څخه خوندي کړئ. د افرادو لپاره جلا لارښود هم شتون لري.

دا مشوره د خورا عامو او جدي ګواښونو پراساس ده.

### نوي کول (اپډیت)

په خپلو وسیلو کې سافټویر نوي وساتئ ترڅو په امنیتي لحاظ خوندي وي.

- د خپلې ټولنې ډلې یا سازمان وسایل تازه وساتئ. پدې کې تلیفونونه، کمپیوټرونه، وای فای روټرونه، او هر هغه څه شامل دي چې انټرنیټ سره وصل دي – په شمول د سمارټ وسیلو.
- که شوني وي اتوماتیک نوي کول وکاروئ.

### دوه فکتوره تصدیقول (Two-factor authentication (2FA))

ستاسو حسابونو ته د پاسورډ او یو بل ګام په اړتیا سره اضافي خوندیتوب اضافه کوي، لکه یو کوډ ستاسو په تلیفون کې د یوه ځانګړي اپ له لارې د اجازې غوښتنه.

- یادونه: دې ته څو فکتوري تصدیق یا د کارونې اجازه (multi-factor authentication (MFA))، دوه مرحلې تصدیق یا د کارونې اجازه (two-step verification (2SV)) او ډېر نور نومونه ویل کیږي.
- د خپلو ټولو ټولنیزو ګروپونو یا سازمانونو په حسابونو کې دوه فکتوري تصدیق یا کارولو دوه ځلې اجازه غوښتل FA2 و کاروئ.
- که شوني وي، د 2FA داسې یوه بڼه وکاروئ چې د فشینګ په وړاندې مقاومت ولري، پدې مانا چې تاسو په اسانۍ دوکه نشئ. دا ممکن د امنیت فزیکي ډول کلي یا د ګوتو نښې یا د مخ څیره وي.

### خپل آنلاین حسابونه څارئ

ډاډ ترلاسه کړئ چې پخواني غړي د ټولنې ګروپ یا سازمان له پریښودلو وروسته خپلو حسابونو ته لاسرسی ونلري.

- که تاسو له یو څخه ډیر کسان لرئ چې ورته حساب ته لاسرسی لري، ډاډ ترلاسه کړئ چې دوی ټول مختلف لاګونه یا اکونټونه لري، او ټولو 2FA فعال کړي دي.
- د ټولو کاروونکو حسابونو لست وساتئ او هر هغه غیر فعال کړئ چې اړتیا ورته نه وي، لکه کله چې کارکوونکي ډنده پریږدي.
- د هر هغه وسیلو راجستر وساتئ چې تاسو خپلو غړو ته ورکړې وي او په یاد ولرئ چې کله هغه شخص له سازمان څخه ووځي نو هغه بیرته ترلاسه کړئ او کمپنې سره یې بیا تنظیم کړئ که چیرې هغه شخص له سازمان څخه ووځي (کار پریږدي). تاسو شايي ودانۍ ته د لاسرسي یا ننوتلو لپاره د فزیکي کوډونو بدلولو ته هم اړتیا ولرئ.

## وګورئ چې څوک ستاسو آنلاین حسابونو ته لاسرسی لري

ستاسو د ټولنې ګروپ یا سازمان کې خلک باید یوازې هغه شیانو ته لاسرسی ولري چې دوی ورته اړتیا لري.

- که د یو کس حساب 'هک' شي، دا کامونه هغه زیان محدودوي چې بریدګر یې کولی شي.
- په منظم ډول غیر ضروري اجازې وګورئ او لرې یې کړئ.
- که تاسو یو واحد "اډمین" حساب لرئ چې ډیر خلک یې کاروي، د غیر معمولي فعالیت لپاره یې وڅارئ. هڅه وکړئ چې د دې ډول حسابونو درلودل محدود کړئ، په ځانګړې توګه د ورځني کارونو لپاره.
- دا قواعد وسیلو ته د مدیر پر لاسرسي باندې هم پلي کیږي، لکه روټرونه.

## د خدماتو چمتو کونکو سره د خپلو قراردادونو بیاکتنه وکړئ

که تاسو د مالوماتي ټیکنالوژۍ خدمتونو د چلولو لپاره څوک ګمارلي وي.

- ډاډ ترلاسه کړئ چې دوی ستاسو د ټولنې ډلې یا سازمان له اړتیاوو سره سم د سایبر امنیتي خوندیتوب لري.

## پوه شئ چې ستاسو ټول حسابونه او سیستمونه څنګه یوځای کار کوي

د اړیکو پوهیدل له تاسو سره مرسته کوي چې پوه شئ چې بریدګر چیرته ننوتلی شي.

- ستاسو د سیستمونو ترمنځ په اړیکو بیاکتنه وکړئ، د بیلګې په توګه، بریښنالیک، د کلاوډ زیرمه، او د محاسبې پلیټ فارمونه.
- د اضافي آنلاین خوندیتوب لپاره د مجازی خصوصي شبکې (Virtual Private Network (VPN)) کارولو په اړه فکر وکړئ. د VPN کارول ستاسو آنلاین فعالیت د هر هغه چا څخه پټوي چې ممکن ستاسو د تعقیب هڅه وکړي. دا په ځانګړي توګه ښه ده که ستاسو د ټولنې ډلې یا سازمان کوم غړی له لرې سره وصل شي.

## خپل خلک 'سایبر ځیرک' وساتئ

ستاسو د ټولنې ډلې یا سازمان غړي ښايي ستاسو د سیستمونو په پرتله ډیر احتمال لري چې په نښه شي.

- ټولو کارکوونکیو ته به سایبري امنیت کې په اساسي ټوکه روزنه ورکړئ. خپل آنلاین ویب پاڼه خپل کړئ Own Your Online | NCSC د مشورې او لارښوونو پراخه لړۍ لري ترڅو څان آنلاین خوندي وساتئ او د درغلۍ موندلو څرنګوالی باندې پوه شئ.
- دوی ته یادونه وکړئ چې دا د دوی د شخصي حسابونو لپاره هم اړین دی او همدارنګه هغه چې دوی یې ستاسو د سازمان لپاره کاروي.
- مورږ د اشخاصو لپاره هم لارښود لرو Keeping safe online

### د پېښې لپاره پلان

د غبرګون پلان درلودل مهم دي ترڅو خلک د پیښې پر وخت له ویرې څخه وساتي.

- د پیښې د غبرګون پلان دا په ګوته کوي چې څوک د پیښې پرمهال څه کوي. ټیمپلیټونه دلته شتون لري د پیښې مدیریت | NCSC
- د هغه څه لپاره یو پلان شامل کړئ چې که تلیفونونه، کمپیوټرونه، یا نور سیستمونه کار ونکړي نو څه وکړي. دا پلان تازه وساتئ.
- د هرچا د اړیکو توضیحات او د بک اپ مشخصات خوندي وساتئ که چیرې د دوی سره د اړیکې اصلي لاره کار ونکړي (لکه بریښنالیک).
- پلان د خپل سیستم څخه بهر په کوم ځای کې وساتئ، که چیرې تاسو نشئ کولی ورته لاسرسي ولرئ.