د کډوالو میرمنو ډیجیټلي ځواکمنتیا او ارتباط پروژه

د 3 ورکشاپ د بدرګي لارښود

دا لارښود د یوې ملاتړکوونکې وسیلې په توګه د هغو میرمنو لپاره تدوین شوی چې د کډوالو میرمنو ډیجیټلي ځواکمنتیا او ارتباط پروژې په ورکشاپونو کې برخه اخلي. دا د هغو میرمنو لپاره دی چې د کډوالی، بشردوستانه خوندیتوب یا د کډوالي کورنی بیا یوځای کیدلو حیثیت لري او په انګلستان کې ژوند کوي. نوموړې پروژه د کورنیو چارو وزارت د بیا میشتېدنې پناه غوښتنې د ملاتړ او ادغام (Home Office Resettlement Asylum Support and Integration Fund) ریاست لخوا تمویلیږي.

مورِ غواړو د VOICEs شبکې له غړو او د Voices له استازوڅخه منه وکړو چې د دې پانګه ایزواسنادو د تدوینولو ملاتړ یې کړي. مواد په انګلیسي، امهاري (Amharic)، عربي، فارسي، کردي (سوراني) صومالي، تیګرینیایي (Tigrinya) او اردو کې چمتو شوي. تمه کیږي چې هغه کډوالي میرمني چې په ورکشاپونو کې برخه نشي اخیستلای، ښایی لاهم دا د ستونزو هوارولو لپار ګټور وموميِ او په دې کې شته معلومات د خپلې خوښې سره سم وڅېړي.

منځپانګې

سریزه 3
کلیدي اصطلاحات 3
ډیجیټلي خوندیتوب څه شی دی؟ 3
د ډیجیټلي خوندیتوب اړیني سپارښتنې 4
د قوي پاسورډونو درلودل 4
د پاسورډ یو سمبالونکی (password manager) وکاروئ 4
دوه فاکتوریزه منظوري (Two-factor authentication) تنظیم کړئ 4
له ویروسونو څخه د خپلو وسایلو خوندي ساتل 5
خپله ډېټا بېک اپ (Back up) کړئ 5
په لنډو ټکو 6
که کوم څه ناسم وي نو څه باید وشي 6
د آنلاین ګواښ عام ډولونه 6
دوکه او درغلی 6
فیشینګ (Phishing) 7
خوندي او ناخوندي ویب پاڼې 9
که تاسو د یوه درغلګر لخوا په نښه شئ څه باید وکړي 9
آنلاین اړیکې 10
د عاشقۍ دوکه 10
سایبري لنډغري 10
ګرومبنګ 11
سیکسټینګ او د پورن غچ اخیستنه 11
سایبري تعقیبوونه او ځارنه 12
کورنی ناوړه ګټه اخیستنه، ځورونه او ځارنه 13
لنډیز 14

سریزه

دا وسیله د خدمتونو په آنلاین بڼه ترلاسه کولو په اړه د بشپړو سپارښتنو د څېړلو توان نلري او د یوې ابتدایي پیژندنې په توګه ګټل کیږي چې هیله لري ستاسو پام ځینو کلیدي ټکو ته او چیرې چې تاسو نور معلومات ترلاسه کولای شئ، وروړوي.

مونږ دا منو چې پر ناوړه ګټې اخیستنې او جنایي جرمونو پورې اړوندو موضوعاتو بحث کول کېدای شي حساس او ډیرې وختونه منع وي. زمونږ بشردوستانه ماموریت او د زیان نه رسولو اصل پدې معنی دی چې مونږ د هغو کړنو ترسره کولو ته هڅاند یو چې د جندر پر بنسټ تاوتریخوالي مخنیوي لپاره زمونږ په واک کې دي، پشمول د هغو معلوماتو چمتو کولو چې د خلکو ملاتړ کوي ترڅو داسې غوراوی وکړي چې دوي ځواکمن کړي او هغه پریکړې وکړي چې دوي خوندي وساتي.

د دې لارښود په اوږدو کې به تاسو په متن کې ځای په ځای شوي داسې لینکونه (links) ومومئ چې، که کلیک (Click) ورباندې وکړئ، نو نومورې ویب پاڼې ته به مو ورسوئ. د ببلګې په توګه، که تاسو په دلته کلیک وکړئ نو د برتانیا سره صلیب ویب پاڼې ته به ورسیږئ. مونږ تر شوني بریده هڅه کړې چې د ژباړل شویو سرچینو لینکونه پکې شامل کړو، خو پدې لارښود کې ډېرې لینکونه د معلوماتو لپاره دي چې په انګلیسي کې دي. پداسې حال کې چې مونږ د اتوماتیک ژباړې په محدودیتونو اعتراف کوو، خو په دویم لارښود کې مو د نومورې فعالیت (function) کارولو د څرنګوالي په اړه معلومات ورکړل.
ستاسو د وسیلو خوندي کولو څرنګوالي او د آنلاین ګواښونو څخه د ځان او نورو د خوندي کولو پراوونو پشمول د ډیجیټلي خوندیتوب په اړه هراړخیزه سپارښتنې په www.getsafeonline.org.uk، او د سایبر ملي امنیتي مرکز www.ncsc.gov.uk کې د لاسرسي وړ دي. د آنلاین ناوړه ګټې اخیستنې قربانیانو لپاره لا ډېر معلومات او ملاتړ په آنلاین ناوړه ګټه اخیستنه بنده کړئ (Stop Online Abuse) کې د لاسرسي وړ دي – www.stoponlineabuse.org.uk. د جنسیت پر بنسټ د هر ډول تاوتریخوالي، کورني ناوړه ګټې اخیستنې یا ځوروني سره د مبارزې یا یې د راپور ورکولو د ملاتړ یا معلوماتو لپاره د کډوالۍ یا د کورني ناوړه ګټې اخیستنې ملي کومکي لیکې
(Refuge or the National Domestic Abuse Helpline) سره www.refuge.org.uk /
0808 2000 247 www.nationaldvhelpline.org.uk اړیکه ونیسئ.

که تاسو ته سمدلاسي اندیښنې پېښې شي یا د یو جرم راپور ورکول وغواړئ، نو د پولیسو سره اړیکه ونیسئ – 999 (بیرنۍ حالت) – 101 (نابیرنۍ حالت)

کلیدي اصطلاحات

ډیجیټلي خوندیتوب - د انټرنیټ کارولو پرمهال د ځان، نورو او د خپلو شخصي معلوماتو خوندي ساتلو لپاره تمرینونه او عادتونه
خپلمنځي - د خلکو ترمنځ تعامل سره د تړاو په معنی
آنلاین ګواښ – یو خطر یا ستونزه چې د انټرنیټ له لارې د ناګلې پېښې یا عمل لامل کیږي
پاسورډ - د ټکو یوه پټه لړۍ چې یوه کمپیوټري سیسټم یا خدمت ته د لاسرسي اجازه ورکوي
خوندي - خوندي او بې خطره پاتې کېدل، د خطر یا زیان سره نه مخ کېدونکي.

ډیجیټلي خوندیتوب څه شی دی؟

ډیجیټلي خوندیتوب د آنلاین خطرونو څخه د ځان (او خپلې ډیټا) خوندي کولو څرنګوالي په اړه د خبریدو او پوهیدو په معنی دئ. ډیجیټلي خوندیتوب ډیرې وختونه یواځې د یو څو داسې بڼه عادتونو درلودلو په معنی دی چې تاسو د انټرنیټي جرمونو (cyber-crime)، دوکو یا ګواښونو پر وړاندې لږ زیانمنونکي کوي. دا د ځینو هغو چلونو پوهېدل رانغاړي چې مجرمین یې په کارولو کولای شي له خلکو معلومات یا پیسې ترلاسه کړي یا یې په شخصي ژوند یرغل وکړي.

د آنلاین ګواښونو خورا عام ډولونه له لاندې مواردو څخه دي

- وايروسونه او مالویر (Viruses and malware) چې هڅه کوي ستاسو شخصي معلومات یا د حساب تفصیلات هیک یا "hack" کړي، یا داسې پروګرامونه نصب (install) کړي چې کولای شي ستاسو جاسوسي وکړي
- آنلاین دوکه کوم کې چې مجرمین هڅه کوي تاسو قانع کړي چې معلومات ورته وسپاري
- لنډغران، تعقیبوونکي او ناوړه ګټه اخیستونکي چې ستاسو د ځورولو، ناوړه ګټې اخیستنې یا کنټرولولو لپاره د آنلاین نا معلومه هویت څخه ګټه پورته کوي.

آنلاین ګوابنونه دا وړتیا لري چې مالي، عاطفي او شخصي هوساینه اغیزمنه کړي. د دې توازن په پام کې نیولو سره، او ترټولو مهمه، د ډیجیټلي خوندیتوب پوهه له خلکو سره مرسته کوي چې خپل آنلاین اطمینان غښتلی کړي.

د ډیجیټلي خوندیتوب اړیني سپارښتنې

د قوي پاسورډونو درلودل

بریښنالیک او نور ټول آنلاین حسابونه په یوه پاسورډ (یوې کونجې) قفل کړي، ترڅو ستاسو حساب ته د نورو د لاسرسي مخه ونیسي. ددې لپاره چې خپلو شخصي معلوماتو ته د بل کس د ننوتلو مخه ونیسي، نو د پاسورډ پیچلي کول یا "قوي" کول یې غوره لاره چاره ده.

د بریښنالیک لپاره د قوي پاسورډ ټاکل اړین دي. که یو هیکر (hacker) ستاسو بریښنالیک ته ننوځي، نو هغه کولای شي د 'forgot password' ځانګړنې په کارولو سره ستاسو د نورو ټولو حسابونو پاسورډونه بیا له سره تنظیم کړي او ستاسو په ټولو حسابونو کې حساسو شخصي معلوماتو ته لاسرسی وکړي.

هیکران پوهیږي چې زمونږ څخه ډیرې د 123456، زمونږ په ژوند کې د یوې مهمې نیټې یا د ماشوم نوم په څیر پاسورډونه غوره کوو– د هر هغه څه کارولو ته مه لیوالـه کیږئ چې په اسانۍ سره اټکل کیدای شي. اسانه پاسورډونه په چټکۍ سره ماتیږي، خو یو ښه پاسورډ د مجرمینو مخه نیسي. د داسې یوه پاسورډ رامنځته کول، د وخت په لګولو ارزي.

د نوي قوي پاسورډ جوړولو لپاره لاندې مرحلې تعقیب کړئ:

1. دري تصادفي ټکي سره یوځای کړئ: د بیلګې په توګه، غالۍ (rug)، اور (fire)، پنجه (fork) د (rugfirefork) جوړولو لپاره.
2. لوی حروف اضافه کړئ، د بیلګې په توګه، RugFireForK
3. شمیرې اضافه کړئ، د بیلګې په توګه، 19RugFireForK90، او
4. د پاسورډ ډیر پیچلي کولو لپاره سمبولونه اضافه کړئ: !19RugFireForK90!

هیکران د ملیونونو په خطر کې پاسورډونو لستونه شریکوي خو دري تصادفي ټکي د نویو پاسورډونو رامینځته کولو یوه اسانه لاره چاره ده چې ددې احتمال یې ډیر دی چې تاسو ته ځانګړی وي او ددې احتمال یې کم دي چې اټکل شي. ددې په کلکه سپارښتنه کوو چې تاسو وخت په وخت خپل پاسورډونه بدل کړئ او د خپلو ټولو حسابونو (accounts) لپاره ورته پاسورډ مه کاروئ. که تاسو د نویو پاسورډونو جوړولو په لټه کې یاست، نو د پاسورډ جنریټر (password generator) یې هم یو ښه غوراوی دی.

د پاسورډ یو سمبالونکی (password manager) وکاروئ

که تاسو اندیښمن یاست چې تاسو به 'قوي' پاسورډونه په یاد ونلرئ، نو کولای شئ د پاسورډ سمبالونکی وکاروئ. د پاسورډ سمبالونکی به په پدې معنی وي چې په ویب لټونګر کې ستاسو پاسورډ خوندي کړي (لکه Google Chrome یا Microsoft Edge)، ترڅو لټونګر ستاسو لپاره پاسورډ په یاد وساتي. دا د ناوړه یا کمزورو پاسورډونو کارولو په پرتله خوندي دي خو په یاد ولرئ چې ستاسو د وسیلې د ورکیدلو په صورت کې یې باید خوندي کړئ. ځینې کمپنۍ چې په انټي ویروس او آنلاین خوندیتوب کې تخصص لري (که تاسو د دوي انټي ویروس وسیلې واخلئ، نو د معیار په توګه به درته د پاسورډ یو سمبالونکی چمتو کړي؛ خو نورې کمپنۍ به پخپله د پاسورډ سمبالونکي وړاندیزوي.

دوه فاکتوریزه منظوري (Two-factor authentication) تنظیم کړئ

دوه فاکتوریزه منظوري ستاسو د پاسورډ سربیره د یوې بلې برخې معلوماتو په غوښتنې سره ستاسو حساب ته د خوندیتوب یو بل پوښ وراضافه کوي. دا ستاسو حسابونو ته د نورو د ننوتلو په مخنیوي کې مرسته کوي، حتی که هغوي ستاسو پاسورډ هم

ولري. د مشهور بريښنالیک او ټولنیزې رسنۍ لپاره د دوه فاکتوریزه منظورۍ فعالولو څرنګوالي په اړه لارښود به دلته د سایبر ملي امنیتي مرکز په ویب پا ډه کې وموندل شي.

له ویروسونو څخه د خپلو وسایلو خوندي ساتل

ویروسونه هغه پټ پروګرامونه دي چې د ویب پاڼو، بریښنالیکي لینکونو، ضمیمو یا د لرې کېدونکي میډیا (لکه د USB سټیکونو) له لارې لیږدول کیږي. دا د ډیرې ګډوډۍ لامل کېدای شي او کولای شي تاسو له خپل کمپیوټر یا حسابونو څخه بند کړي، شخصي معلومات یا ډیټا مو د خرڅولو یا کارولو لپاره غلا کړي، ستاسې پیسې ترلاسه کړي، یا حتی تاسو په خپل کور کې وګوري. د اندیښنې وړده، چې هرڅوک نه پوهیږي چې د دې ګواښونو څخه د خپلو وسایلو د ساتنې لپاره کوم اقدامات ترسره کړي. ONS راپور ورکړی چې په 2020 کې، د هغو لویانو څخه چې ځیرک تلیفون لري، 17٪ یې په خپل ځیرک تلیفون کې خوندیتوب (security) نه درلود او 32٪ نه پوهیدل چې دوي خوندیتوب درلود که نه.

انټي ویروس، د امنیتي ساتونکي په څیریوه وسیله ده چې په لپ ټاپ، ټابلیټ یا تلیفون کې ددې لپاره نصبیږي چې د هغو ستونزو رامینځته کوونکو پروګرامونو مخنیوی وکړي چې ستاسو وسایل منتن کوي. د انټي ویروس خوندیتوب د کمپیوټر، لپ ټاپ، ټابلیټ یا ځیرک تلیفون ته لکه د لاندې معمول ګواښونو په مخنیوي کې د مرستې رسولو لپاره اړین دی:

- **Trojans یا تروجانس** کوم چې د داسې یوه پروګرام په څېر ښکاري چې تاسو یې ډاونلوډول غواړئ (لکه د انټي ویروس پروګرام، یو عکس یا وړیا فلم) خو یو ناوړه سافټویر (مالویر) دی یا یې لري، کوم چې فعالیږي کله چې یې په خپل کمپیوټر یا تلیفون کې نصب کړئ.
- **Spyware یا سپای وېر** کوم چې معلومات تعقیبوي او هغه څه چې تاسو یې په کمپیوټر کې ترسره کوئ، د جرمي موخو لپاره ګوري،
- **Adware یا ادویر** کوم چې پاپ اپ (pop-up) کړکۍ پرانیځي کومه چې هڅه کوي په تاسو شیان وپلوري.
- **Ransomware یا رینسموېر** کوم چې تاسو له خپلې وسیلې څخه بندوي او د تادیې غوښتنه کوي.
- Spam یا سپم د چینجیو (worms) په نوم پروګرامونه تولیدوي، کوم چې ستاسو سیسټم ته د پرانستو انټرنټي اړیکو له لارې ننوځي، او ستاسو اړیکو ته د لیږلو لپاره ډیر ناغوښتل شوی "spam" بریښنالیکونه بیا کاپي کوي. ناغوښتل شوي بریښنالیکي مکاتیب ته **سپم (spam)** یا **جنک (junk) بریښنالیک** ویل کیږي. سپم بریښنالیک که څه هم په ساده توګه یو تکلیف بلل کیدای شي، خو د خلکو دوکه کولو او ناسمو معلوماتو خپرولو لپاره هم کارول کیدای شي.

ډیرې سیسټمونه به له مخکې نصب شوي بعضې د خوندیتوب **انټي ویروس یا سپایویر** ولري، د بیلګې په توګه د مایکروسافټ ویندوز 10 (Microsoft Windows 10) لرونکي لپټاپونه به دمخه نصب کړی ویندوز ډیفنډر (Windows Defender) ولري.

تاسو کولای شئ د انټي ویروس اضافي خوندیتوب ترلاسه کړئ: ځینې وختونه دا وړیا وي، خو داسې کمپنۍ هم شته چې د پلورلو په موخه پروګرامونه چمتو کوي.

پخواني سافټویر ښایي خالیګاوې (holes) ولري چې ویروسونه له هغې لارې په پټه ټیریدلای شي. **Updates** نومورې خالیګاوې پیوندوي. تاسو کولای شئ پروګرامونه او سافټویر داسې تنظیم کړئ چې په اوتومات ډول اپډېټ (update) شي ترڅو ستاسو په خوندیتوب کې کومه شته خالیګاه پیوند کړي. د دې معنی دا ده چې تاسو د دې ترسره کولو په یاد ساتلو ته اړ نه یاست. ځینې وختونه تاسو ښایي خپله وسیله په غیر اتوماتیک ډول اپډېټ کړئ او که همداسې پېښه وي نو معمولاً به یوه یادونه (reminder) ترلاسه کړئ. هغه له پامه مه غورځوئ!

خپله ډیټا بیک اپ (Back up) کړئ

ویروس کولای شي ستاسو ډیټا او معلومات ړنګ (delete) یا غلا کړي. د خپلو شخصي عکسونو، فایلونو او معلوماتو خوندي کولو لپاره تاسو باید د خپلې وسیلې اپډېټ کولو دمخه ډیټا بیک اپ کړئ. د بیک اپ معنی دا ده چې یوه کاپي جوړه کړئ، کومه به چې د لېږدېدونکي هارډ ډرایو (portable hard drive) په کارولو سره په فزیکي بڼه وي، خو ډیره معمول بڼه یې بلې وسیلې ته لېږد یا "cloud" (آنلاین) ذخیره کې ساتل دي. دا ځکه چې اپډېټ ترسره کول ځینې وختونه فایلونه بدلوي، خو که تاسو د خپلې ډیټا داسې بیک اپ ولرئ چې ژر تر ژره یې بیرته ترلاسه کړای شئ نو د رینسموېر بریدونو له لارې به نه بلک

مبل (blackmailed) کېږئ. تاسو کولای شئ اتوماتیک بیک اپ چالان کړئ پدې معنی چې تاسو اړتیا نلرئ د خپلې ډیټا بیک اپ کول په یاد وساتئ.

ستاسو د ډیټا بیک اپ کولو په اړه نوري لارښوونې دلته موندل کیدای شي
www.getsafeonline.org/protecting-your-computer/Backups

په لنډو ټکو

- خامخا یواځې د خپل بریښنالیک لپاره یو جلا پاسورډ وساتئ
- د خپل بریښنالیک پاسورډ او د خپلو نورو حسابونو پاسورډونه چک (check) کړئ چې قوي وي
- چک کړئ چې تاسو پوهیږئ چې څنګه خپل پاسورډ بدل او دا کار په منظم ډول ترسره کړای شئ
- د متعددو حسابونو لپاره ورته پاسورډ مه کاروئ اوکه تاسو د پاسورډونوهیرولو په اړه اندیښمن یاست نو د پاسورډ سمبالونکي کارول په پام کې ونیسئ.
- دوه فاکتوریزه منظوري وکاروئ
- ځان مطمئین کړئ چې تاسو انټي ویروس لرئ او هغه فعال دی (که تاسو ډاډه نه یاست نو یو ترلاسه کړئ
- خپل انټي ویروس وکاروئ او اپډېټ یې کړئ – په منظم ډول د سیسټم بشپړ سکین وکړئ او خپل انټي ویروس اپډېټ کړئ ترڅو د نویو رامینځته شویو ویروسونو یا بګونو (bugs) پروړاندې مو ساتنه وکړئ.
- د هغه څه په اړه چې تاسو یې ډاونلوډوئ محتاط اوسئ – د اعلانونو یا سپای ویر پروګرامونه ستاسو کمپیوټر ته د هغو شیانو سره د ځان نښلولو له کبله داخلیږي چې تاسو یې ډاونلوډوئ، نو هغه ځایونه چک کړئ چې تاسو خپل فایلونه ورځخه ترلاسه کوئ.

که کوم څه ناسم وي نو څه باید وشي

که په خپل لپ ټاپ کې مو لینک خلاص کړی وي یا مو د یو څه نصبولو لارښوونې تعقیب کړې وي خو وربانديې شک لرئ، نو د انټي ویروس سافټویر خلاص کړئ او بشپړ سکین ترسره کړئ. انټي ویروس ته اجازه ورکړئ چې انتان کشف او له منځه یوسي او د هغه د سپارښتنو په تعقیبولو سره خپله وسیله بیرته ورغوئ. که نه سمبدلو نو باید د یوه مجرب کس مرسته ترلاسه کړئ.

نړیدي ملګری مو در سره اړیکه نیسي او ډیر خفه ښکاري. هغه په بریښنالیک کې یو فایل خلاص کړ چې فکر یې کاوه عکس دئ. دا په حقیقت کې یو ټروجان آس (trojan horse) و چې د رینسمویر یې مخفي کړی وو او اوس یې هغه د خپل کمپیوټر څخه بند کړي دي. تاسو به څه وکړئ، او هغه ته به د څه کولو سپارښتنه وکړئ؟

که تاسو په رینسمویر اخته شوي یاست، نو خبر اوسئ چې که د یرغمل بیې ورکول مو غوره کړې وي نو دا به جرمي فعالیت تمویل کړي او هیڅ تضمین نشته چې تاسو به خپلې وسیلې ته لاسرسی وموندئ؛ بې له دې چې تاسو ته کومه ګټه ورسوي، ښایي دا کار مو داسې انګیرنه ورکړي چې تاسو په راتلونکي کې بیا تادیه کولو ته لیواله یاست او راتلونکو بریدونه رابلئ.

د آنلاین ګوابښ عام ډولونه

دوکه او درغلي

درغلګرې کول د تېرایستلو یوه لاره چاره ده ترڅو د یو چا څخه پیسې ترلاسه شي یا یې شخصي معلومات یوه مجرم ته چمتو کوي ترڅو د هغوي د حساب څخه غلا وکړي یا یې هویت غلا کړي. پدې کې د دوي له کمپیوټر یا آنلاین حساب څخه د معلوماتو غلا کولو لپاره د ویروسونو کارول یا د یو کس، د تېر ایستلو یا لارورکي کولو له لارې، په دې قانع کول شاملېدای شي چې په خپله خوښه پیسې وسپاري.

یوه درغلي ډیرې وختونه د جعلي بریښنالیکونو (**فیشینګ یا phishing**)، د متني پیغام (**سمیشینګ یا smishing**) یا تلیفوني زنګ (**ویشینګ یا vishing**) د کارولو له لارې ترسره کیږي. بریښنالیکونه یا متنونه ښایي جعلي ویب پاڼې ته لینک ولري چې تاسو هڅوي تر څو شخصي معلومات ورکړئ یا د یوه دهلیز په توګه عمل کوي او ویروسونه ستاسو کمپیوټر ته انتقالوي. یا ښایي بریښنالیک داسې یوه ضمیمه ولري چې ویروس پکې وي او د بانکداری تفصیلات، شخصي معلومات یا عکسونه غلا کوي.

درغلی تاسو اړباسي چې فکر وکړئ چې ګواکې د یوې اداري لخوا درسره اړیکه نیول شوې چې تاسو یې پیژنئ یا ځینې وختونه د داسې چا لخوا چې مرستې ته اړتیا لري. دا داسې ډیزاین شوې ترڅو د یوځه "ترسره کولو" لپاره تاسو، ډیرې ځله د چټک عمل کولو تر فشار لاندې راشئ، لکه – یو لینک خلاص کړئ، توضیحات ورکړئ، په ضمیمه کلیک وکړئ. باور ورباندې مه کوئ!

مورِ دومره وخت نلرو چې دلته هر ډول دوکه او درغلي لست کړو. د درغلیو د ډولونو په اړه چې مجرمین یې کاروي، نور معلومات، او سربیره پر دې د دوکو او سایبر جرمونو راپور ورکولو د ځرنګوالي په اړه سپارښتنې دلته موندل کیدای شي:
www.actionfraud.police.uk

فیشینګ (Phishing)

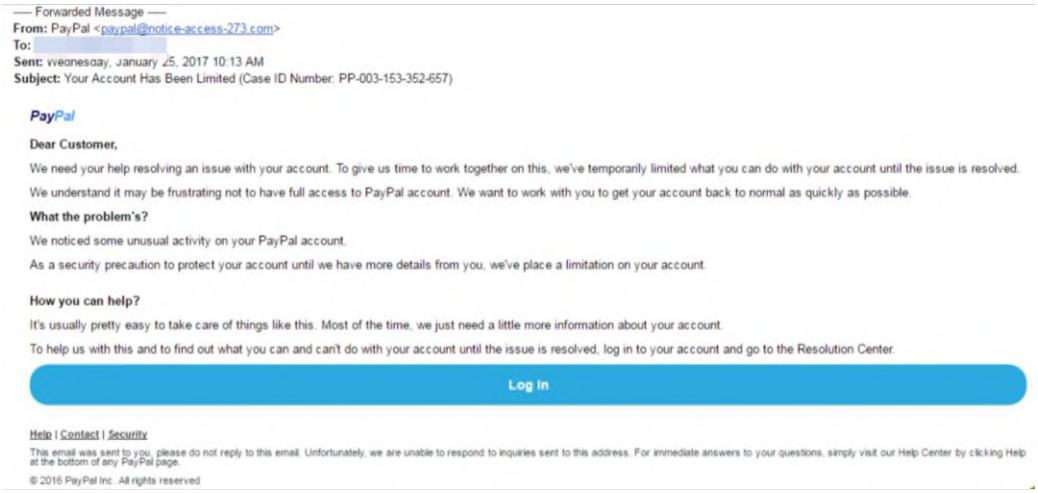
فیشینګ یو ډول درغلي ده، چې پکې یو سایبري مجرم د شخصي معلوماتو، بانکداری یا دبانکي کارت تفصیلاتو، یا د حساب تفصیلاتو او پاسوردونو په چمتو کولو کې د خلکو د تیرایستلو لپاره یو "هوک یا hook" کاروي. دوي بیا دا معلومات ستاسو حسابونو ته د لاسرسي لپاره کاروي او له تاسو څخه پیسې یا د بریښنالیک اړیکې غلا کوي یا ستاسو هویت غلا کوي. مجرمین ښایي زرګونو خلکو ته د فیشینګ بریښنالیک واستوي پدې هیله چې ښایي دوي به وکړای شي چې د پیسو یا معلوماتو ترلاسه کولو کې یواځې یو څو یې تیرباسي.

هیکران او درغلګران به د داسې یو کس یا یوې اداري په توګه د ځان ښودلو عالي دنده ترسره کړي چې تاسو پرې باور کوئ، او دوي ښایی ستاسو نوم او نور شخصي معلومات هم وکاروي ترڅو تاسو و ازمایي او قانع کړي. دوي به هڅه وکړي چې په وړاندیزونو سره مو تیرباسي یا مو د ګواښ له لارې په دام کې واچوي. د بیلګې په توګه، ښایی د حکومت په توګه ځان وښایي مثلاً د مالیې دفتر تاسو سره د پیسو بېرته سپارلو وړاندیزولو لپاره تماس نیسي، خو له تاسو غواړي چې د پیسو ترلاسه کولو لپاره باید خپل بانکي تفصیلات چمتو کړئ. دوي کولای شي ځان ستاسو سیمه ایزه شورا وښیي، او درته ووایی چې تاسو د تادیه کولو لپاره جریمه لرئ یا تاسو به محکمې ته ولاړ شئ، یا خپل بانک یا د بانکداری د منځګړی په توګه د پی پال (PayPal) په توګه ځان وښایي او دا چې تاسو د خپل بانکي حساب له کارولو څخه منع شوي یاست.

د فیشینګ په هکله د میټروپولیټین (Metropolitan) پولیسو دا ویډیو وګورئ.

د چک کولو ګړندۍ لار چې چا واقعاً بریښنالیک لیږلی او ایا دا د فیشینګ درغلي ده که نه، هغه د لیږونکي د بریښنالیک د پتې پلټلنه ده، نه یواځې هغه څه چې په "From" کې څرګندیږي. یو ریښتینی پیغام به اکثراً د پیژندل کېدونکي سازماني پتې څخه راځي (د بېلګې په توګه noreply@yourbank.com) خو درغلګر او مجرمین نشي کولای ستاسو د بانک یا سازمان اصلي ډومین نوم وکاروي، نو ډیرې ځله به د بریښنالیک پته له تصادفي حروفو او شمیرو ډک وي (د بیلګې په توګه noreply@1234bank12.com). که دا د یوې شخصي پتې څخه وي (د بیلګې په توګه person@gmail.com) نو بیا دا شوني نده چې د رسمي سازمان څخه دي وي – حتی ګوګل د سازماني بریښنالیکونو لیږلو لپاره د ګوګل میل (@gmail) ډومین (domain) نه کاروي.

دې بیلګې ته په کتو تاسو لیدلای شئ چې که څه هم دا د PayPal څخه د ریښتیني بریښنالیک په څیر ښکاري، خو دا د دې پرځای د **بل کوم ډومین له نوم** څخه دی: Paypal@**notice-accessxxx.com**


— Forwarded Message —
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

دا د دې ارزښت لري چې د هغو بريښنالیکونو په اړه محتاط اوسئ چې په ریښتیا هم خورا ښه ښکاري، یا دا چې پر تاسو د ګړندیو پریکړو کولو لپاره فشار راوړي، حتی که هغه سمه لوګو هم کاروي او مشروع ښکاري. ارام اوسئ او څه مو چې ترلاسه کړي دي په اړه یې پوښتنه وکړئ. ځواب مه ورکوئ او په کوم لینک هم کلیک مه کوئ. کله چې تاسو د لینک ویروس خلاص کړئ نو ښایی ستاسو په کمپیوټر کې د معلوماتو غلا کولو لپاره نصب شي، یا ښایي تاسو داسې ناوړه یا جعلي ویب پاڼې ته واستول شئ چې د حساب یا بانکي توضیحاتو دننه کولو غوښتنه وکړئ کوم به چې بیا له تاسو څخه غلا شي.

د فیشینګ او درغلګرو بریښنالیکونو پیژندل

- ایا تاسو رالیږونکی پیژنئ؟ ایا دوي تاسې د یوه عمومي ښه راغلاست په بڼه مخاطبوي؟
- ایا املایي غلطی شته یا په ناسم ډول لیکل شوي؟
- ایا هغه غواړي چې تاسو یو څه وکړي یا د بېړي کولو احساس درکوي یا مو ګواښوي؟
- د هغه بریښنالیک پته پرانیځئ چې پیغام ورڅخه رالیږل شوی. ایا د هغې د ډومین (domain) نوم سم دی؟
- ایا هغه ناڅاپي دی یا د داسې کومې کمپنۍ څخه دی چې تاسو ورسره سوداګري نلرئ؟
- که هغه تاسو یوې ویب پاڼې ته برابروي نو ایا په هغې ویب پا ڼه کې د پیډلاک (padlock) نښه نشته او د ویب پتې په پیل کې https:// نشته؟

د فیشینګ بریښنالیکونو پیژندلو په اړه نور مطالب دلته موندل کیدای شي: www.ncsc.gov.uk

زهرا یو بریښنالیک ترلاسه کوي چې هغه فکر کوي؛ د هغې د بانک څخه دی – هغه دا د دې لپاره خلاصوي چې پوه شی چې دوي وایي دوي په لنډمهاله توګه د هغې حساب ځنډولی دی. زهرا په ډیره ویره کې، وموندله چې د هغې بانک د هغې په بانکي حساب کې غیر معمولي فعالیت موندلی او د هغې د خوندیتوب لپاره یې د ترلو پریکړه کړی. دا وایي چې هغه نشي کولای تر هغوچې بانکي حساب ته دننه نشي او بیا یې فعال نه کړي، وکاروي او له هغې یې وغوښتل چې په یوه لینک کلیک وکړي. زهرا پوهیږي چې هغه سبا ته کرایه تادیه کوي، او خپل حساب ته باید سمدستي لاسرسی ومومي، خو هغه شکمنه ده.

زهرا تاسو ته د مشورې لپاره زنګ وهي: تاسو هغې ته څه وایاست او تاسو به څنګه مشوره ورکړئ؟

لینک ښایي خطرناک وي. دا پدې معنی کیدای شي چې هیکران به هڅه وکړي چې د هغې په کمپیوټر کې د جرمي موخو، لکه معلومات غلا کولو یا د هغې بریښنالیک، بانک یا ټولنیزو رسنیو حسابونو د هیک کولو لپاره یو څه نصب کړي. یا نومورې لینک کولای شي هغه بلې ویب پاڼې (د بانک جعلي نسخې) ته بوځي چې له هغې څخه د هغې د ID او پاسورډ یا نورو بانکي توضیحاتو غوښتنه کوي. کله چې هغه ویب پاڼې ته دا معلومات ورکړي، نو هغه به درغلګرانو ته خپل بانکي حساب او پیسې وسپاري.

ستاسو بانک به د شخصي توضیحاتو د غوښتنې لپاره له تاسو سره د بریښنالیک، تلیفون یا متني پیغام له لارې اړیکه ټینګه نکړی. که هرکله هم تاسو ډاډه نه یاست چې دا به واقعاً ستاسو بانک وي چې تاسو ته زنګ وهي، نه د ویشینګ درغلګر، نو تلیفون پای ته ورسوئ او د هغوي د مشتریانو خدمتونو شمیره په آنلاین بڼه وپلټئ. د بیا تلیفون کولو دمخه د 5 دقیقو لپاره انتظار وکړئ یا یو بل تلیفون وکاروئ ځکه چې درغلګر کولای شي د تلیفون لیکې (lines) هم غلا کړي.

له تاسو سره له خبرو وروسته:

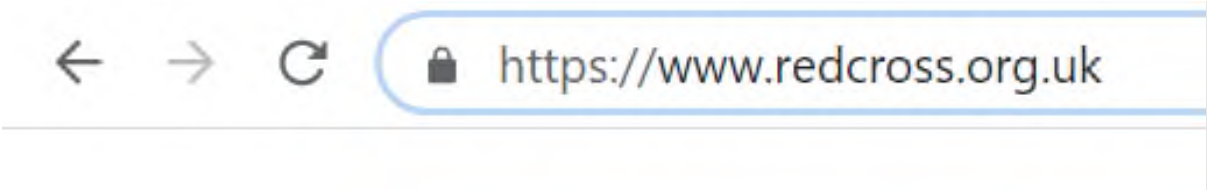
زهرا د خپل بانک د مشریانو خدماتو تلیفون شمیره په آنلاین بڼه پلټي. بانک تاییدوي چې هغه یو جعلي بریښنالیک دی او د هغې حساب په سمه توګه کار کوي. دوي هغې ته وویل چې په بریښنالیک کې لینک داسې یوې ویب پاڼې ته تللی ؤ چې د بانک د ویب پاڼې په توګه یې ځان ښودلی ؤ. که بانک وښیي چې محتاط ندي نو ځینې وختونه به د دې ډول دوکو د قربانیانو لپاره ستونزمنه وي چې خپلې پیسې بیرته ترلاسه کړي.

د فیشینګ او درغلیو په اړه نور معلومات د سایبر ملي امنیتي مرکز کې موندل کیدای شي.
www.ncsc.gov.uk/guidance/phishing

خوندي او ناخوندي ويب پاڼې

دا مهمه ده چې وړتيا ولرئ ترڅو چک کړئ چې هغه ويب پاڼې چې تاسو يې ګورئ خوندي دي که نه. هره ويب پاڼه چې تاسو يې ګورئ ښايي ناخوندي ثابته شي، يا هيکران تاسو ته داسې جعلي بريښنالیکونه ولیږي چې ښايي تاسو داسې جعلي ويب پاڼې ته هدايت کړي کومه چې ښايی خورا ريښتيني وبرينې.

د پيډ لاک دا لوګو يا دا حروف https:// ر بار (browser bar) کې وپلټئ، کوم چې پدې معنی دي چې ويب پاڼه خوندي ده.



ځينې وختونه به تاسو **پيډلاک** او **https** دواړه، يا يواځې د پيډلاک سمبول وګورئ، چې توپير يې د کمپيوټر يا لټونګر دول پورې اړه لري. هغه ويب پاڼه چې يواځې **http** لري ښايي خوندي نه وي، ځکه چې '**s**' خوندیتوب په ګوته کوي.

که له تاسو څخه وغوښتل شي چې حساب ته ننوځئ، د تادیې توضیحات یا نور معلومات چمتو کړئ، نو ډاډ ترلاسه کړئ چې هغه ويب پاڼه چې تاسو به يې کاروئ په لټونګر بار کې د پټې په پيل کې "https" ولري. يواځې هغه وخت د ننوتلو جزيات ورکړئ چې تاسو ډاډه شئ چې دا د ويب پاڼې سمه پته ده او خوندي ده.

تل د خپلې ويب پاڼې ليدو لپاره بشپړه ويب پته دننه کړئ، په ځانګړې ډول که تاسو آنلاين بانکداري ته ننوځئ. هيڅکله د خپل بانک ويب پا ڼې ته د رسيدو لپاره د لټون انجن مه کاروئ، ځکه چې دا مرحله د هيکرانو لخوا کارول کيدای شي چې له امنيت سره جوړجاړی وکړي او ستاسو توضيحات غلا کړي.

د فيشينګ او درغلۍ کوونکو ويب پا ڼو پروړاندې اقدام وکړئ

د خپل ځان د خوندیتوب د هڅې کولو لپاره لاندې ټکي په ياد ولرئ:

- د خپل لټونګر سافټويرز، انټي ويروس او سپای وير اپډېټ (up to date) وساتئ
- له هغو خطرناکو ويب پا ڼو څخه ډډه وکړئ چې خوندي نه وي يا پيډ لاک نلري
- هيڅکله په بريښنالیک کې په هغه لينک باندې چې د نامعلومې يا مشکوکې سرچينې څخه وي، کليک مه کوئ
- هيڅکله خپل شخصي توضيحات، پاسورډونه يا د خوندیتوب کوډونه په بريښنالیک يا تليفون باندې چاته مه ورکوئ

که تاسو د يوه درغلګر لخوا په نښه شئ څه بايد وکړي

بريښنالیک، د تليفون زنګ، پيغام يا ويب پاڼه خامخا رپوټ کړئ.

که تاسو بريښنالیک ترلاسه کړی وي او پدې اړه ډاډه نه ياست، نو کولای شئ هغه **د شکمن بريښنالیک رپوټ کولو خدمت (SERS)** ته په report@phishing.gov.uk ور واستوئ. که هغه د فيشينګ بريښنالیک وي يا ښکاري نو مشوره به درکړي.

که تاسو مشکوک متن ترلاسه کړئ، نو کولای شئ هغه 7726 وړيا شمیرې ته واستوئ. که هغه کومه درغلي وي نو دا ستاسو د تليفون چمتو کونکي ته اجازه ورکوي چې متن وڅيړي او اقدام وکړي.

خپل توضيحات مه شريکوئ خو د دې پرځای يې چک کړئ. هيڅکله په بريښنالیک کې شمیرې ته زنګ مه وهئ او لينکونو باندې کليک مه کوئ ځکه چې هغه ښايی تاسو يوه بل جعلي حساب ته هدايت کړي. آنلاين لاړشئ او په پراخه کچه د اعلان شمیره وموميئ او پرځای يې زنګ ووهئ.

لينکونه پرته له دې پوښتنې چې دوي تاسو چيرته وړي، مه تعقيبوئ. د دې چک کولو لپاره چې ايا ويب پا نه ريښتيني ده که نه، خپل ويب لټونګر خلاص کړئ او سمدستي په URL بار کې د نوم له ټايپ کولو سره ننوځئ.

هیڅکله خپل پاسورډ یا د شخصي هویت شمیره (pin) مه شریکوئ. دا مهمه نده که تاسو فکر کوئ هغه څوک چې پوښتنه کوي ستاسو مور یا غوره ملګری دی – خپل پاسورډ مه ورکوئ.

که تاسو د خپلو بانکي توضیحاتو په چمتو کولو کې تېروتي یاست نو خپل بانک ته یې سمدلاسه ووایاست.

که تاسو پیسې له لاسه ورکړي وي، خپل بانک ته وواياست او Action Fraud ته (د انګلینډ، ویلز او شمالي آیرلینډ لپاره) یا Police Scotland ته (د سکاټلینډ لپاره) د جرم په توګه رپوټ کړئ؛ د دې کار ترسره سره به تاسو د نورو قرباني کیدو په مخنیوي کې هم مرسته وکړئ.

Action Fraud www.actionfraud.police.uk

آنلاین اړیکي

پدې برخه کې به مونږ په شخصي اړیکو کې د انټرنیټ د اغیزو په اړه وغږیږو. هغه څه چې مونږ یې آنلاین کوو، مستقیماً زمونږ په شخصي ژوند اغیزه کولای شي. له همدې امله، دا مهمه ده چې د هغو معلوماتو سره خورا محتاط اوسئ چې تاسو یې آنلاین له نورو خلکو سره شریک کوئ .

مونږ ټول غواړو له خلکو سره ارتباط ونیسو، او دا د انټرنیټ په اړه یو له غوره شیانو څخه دی چې مونږ کولای شو په اسانۍ سره د ملګرو، کورنۍ او خلکو سره په ټوله نړۍ کې د ګډو لېوالتیاوو لرلو سره اړیکه ونیسو. په ورته وخت کې، دا مهمه ده چې پوه شئ چې آنلاین ارتباطات باید په غور سره اداره شي کټ مټ لکه څنګه چې په سړک کې د یو چا سره لیدنه کیږي او دا چې نور ښایي وغواړي په بد نیت له خلکو سره ارتباطات رامینځته کړي چې ښایي د ناوړه ګټې اخیستنې لامل شي.

آنلاین ناوړه ګټه اخیستنه د بیخي پردیو یا د هغو خلکو څخه کیدای شي چې دمخه مو پیژندل، او مونږ به لاندې د خپلمنځي (inter-personal) ناوړه ګټې اخیستنې ځینو بېلګو ته وګورو.

د عاشقۍ دوکه

د عاشقۍ دوکه هغه وخت پېښیږي کله چې یو څوک د آنلاین ډېټینګ (online dating) ویب پاڼه یا ایپ (app) کاروي، د باور ترلاسه کولو لپاره خپلمنځي اړیکي رامینځته کوي او بیا د پیسو یا شخصي معلوماتو غوښتنه کوي. هغوي کېدای شي د اړیکي رامینځته کولو لپاره داسې جعلي پروفایل وکاروي، چې ریښتیني او غمخور ښکاره شي. ډیرې وختونه به نوموړی کس ډیري شخصي پوښتنې وکړي، خو ځان په اړه به ډېر څه نه ښیي یا نه وایي. دوي به تر هغه وخته پورې انتظار وباسي چې مطمین شي چې باور یې رامینځته کړی او د مرستې، معمولاً پیسو، غوښتلو لپاره عاطفي اړیکي کاروي، همدارنګه کیدای شي د یوه پارسل تسلیمېدلو یا یوې پټې وړاندې کولو لپاره هم ترسره شي. دوي ښایي د ځان جعلي ځېرې یا عکسونه واستوي، کوم چې ډیرې وختونه په انټرنیټ کې له بل ځای څخه اخیستل کیږي.

هیڅکله پیسې مه لیږئ یا مه ترلاسه کوئ یا خپل بانکي تفصیلات هغه چا ته مه ورکوئ چې تاسو آنلاین ورسره لیدنه کړې وي، مهمه نده چې تاسو په دوي څومره باور لرئ یا د دوي په کیسه باور وکړئ.

دا په ښځتیا هم خوابدي کوونکي یا شرموونکي کیدای شي کله چې فکر کوئ چې ګواکې په آنلاین بڼه مو ځانګړي ملګرتیا یا اړیکي جوړولو کې ټېر ایستل شوي یاست، خو کولای شئ چې د اکشن فراډ (Action Fraud) ته یې رپوټ کړئ یا 0300 123 2040 ته زنګ ووهئ.

د عکس د سرچینې چک کولو لپاره تاسو کولای شئ د *معکوس عکس لټون وکړئ (reverse image search)* لکه څنګه چې له نوم نه یې ښکاري، تاسو ته اجازه درکوي چې د انټرنیټ په عکسونو کې لټون وکړئ ترڅو د دوي په ځېر نور وموميئ. تاسو کولای شئ د معکوس عکس لټهدلته **ترسره کړئ**

سایبري لنډغري

سایبري لنډغري د آنلاین یا د ټیکنالوژۍ کارولو له لارې د لنډغرۍ او ځوروني لپاره یوه عمومي اصطلاح ده. دا د آنلاین ناوړه ګټې اخیستنې هر ډول رانغاړي چې موخه یې بل چا ته د ضرر، خوابدۍ یا شخصي زیان رسول وي. ډیرې وختونه لنډغران د ټولنیزو رسنیو د شبکو سایټونه لکه فیسبوک یا ټویټر او تعاملي یا د پیغام رسونې فورمونه کاروي. سایبري لنډغري په څرګند ډول خوابدي کوونکي کیدای شي ځکه چې دا یواځې په ځانګړي حالت لکه ښوونځي یا کار کې نه، بلکه د انټرنیټ او ګرځنده تلیفونونو له لارې هر وخت خلکو ته رسېدای شي.

که چا په انټرنیټ یا ټولنیزو رسنیو کې ستاسو په اړه غلط یا ناوړه شیان خپاره کړي وي، دا د ځوروني په توګه پیژندل کیدای شي کوم چې جرم دی. په همدې ډول، که تاسو داسې تلیفونونه ترلاسه کړئ چې تاسو ته ګواښ کوي یا مو ډاروي نو هغه څوک چې دا کوي ښایي جنایي جرم ترسره کړي.

لنډغري هرڅوک اغیزمنولای شي، د ماشومانو او لویانو پشمول، خو که تاسو مور/پلار یا د ماشومانو ساتونکی یاست نو دا په ځانګړي ډول مهمه ده چې په اړه یې خبر اوسئ. که تاسو یا ستاسو ماشوم یا هغه څوک چې تاسو یې پیژنئ ځوروړل شوی وي، د آنلاین ځوروني پشمول، نو د مشورې لپاره د لنډغرۍ ملي کومکي لیکې (national bullying helpline) ته په 0300 323 0169 شمیره زنګ وهلای شئ.

ګرومینګ

ګرومینګ (Grooming) هغه وخت پیښیږي چې یو څوک د یو چا سره د اړیکې باور او ارتباط رامینځته کړي ترڅو له هغه څخه ګټه پورته او هغه کنټرول کړای شي. د ماشومانو او ځوانانو آنلاین ګرومینګ یوه ځانګړي اندیښنه ده، چیرې چې یو کوچنی د جنسي ناوړه ګټې اخیستنې (آنلاین یا حضوري)، د مخدره توکو قاچاق یا د استثمار د نورو موخو لپاره چمتو کیدای شي.

ګرومینګ په لنډ یا اوږده وخت کې ترسره کیدای شي او ګرومران ښایي د ماشوم له کورنۍ سره هم اړیکه رامینځته کړي ترڅو دوي د باور وړ، معتبر او مرستندوي ښکاره شي. د ماشوم د نژاد، جندر یا عمر سره د کومې اړیکې په پام کې نیولو پرته، هرڅوک ګرومر کېدای شي.

ګرومینګ آنلاین ترسره کیدای شي چیرې چې یو ګرومر ښایي خپل ځان یو ماشوم ته د همزولي په توګه وروپیژني او د نورو خلکو داسې عکسونه یا ویډیوګاني وروانستوي چې د دې کار ملاتړ کوي. هغه ښایي ګپمونه وکړي، مشوره درکړي، تفاهم وښیي او د ځوان کس لپاره ډالۍ وپیري ترڅو د یو باوري ملګري په توګه خپل دریځ پیاوړی کړي، یا هڅه وکړي چې ماشوم له کورنۍ یا ملګرو څخه جلا کړي، د بلک میل (blackmail) په کارولو ماشوم په فعالیت او عدم فعالیت سره و ازمایي او شرمنده کړئ، یا د ماشوم د کنټرول لپاره د "رازونو" مفکوره معرفي کړئ.

د ناوړه ګټې اخیستنې او آنلاین ګواښونو په اړه د ماشومانو سره د خبرو کولو د څرنګوالي په اړه د نورو سرچینو سره یوځای، د ګرومینګ په اړه لا ډېر معلومات د NSPCC په ویب پاڼې کې د لاسرسي وړ دي. www.nspcc.org.uk

که تاسو شک لرئ چې ماشوم په خطر کې دی نو پولیسو ته د خبر ورکولو څخه ډډه مکوئ. تاسو کولای شئ د آنلاین ناوړه ګټې اخیستنې راپور ورکولو په اړه د مشورې او ملاتړ لپاره له NSPCC سره هم اړیکه ونیسئ.

سیکسټینګ او د پورن غچ اخیستنه

سیکسټینګ (Sexting) هغه وخت پیښیږي کله چې یو جنسي پیغام، عکس یا ویډیو بل کس ته لیږل کیږي. یو څوک ښایي د ځان یا بل چا عکس ولیږي. یوسیکسټ ښایي یوه ملګري، انډیوال یا بل چا ته آنلاین ترسره شي، او لږه یا بشپړه لوڅېدنه، په جنسي ډول څرګندتیا یا د جنسي عملونو په اړه خبرې کول پکې شاملېدای شي.

پداسې حال کې چې جنسي پیغام د دوه رضایت لرونکو اړخونو ترمینځ لیږل کیدای شي، خو عکسونه د زیانمن له رضایت پرته په انټرنیټ کې په چټکۍ سره شریکیدای شي. کله چې یو بل څوک عکس یا ویډیو آنلاین شریکه کړي، دوي کولای شي هغه هرچا ته واستوي.

د پورن غچ اخیستنه هغه وخت پیښیږي کله چې یو څوک د یو چا **شخصي جنسي** عکس یا فلم پرته د زیانمن له رضایت او **دوي د خوابدی لامل کیدو په نیت** بل کس یا نورو خلکو ته خپروي.

یو چا ته ګواښ کول؛ چې د هغه شخصي معلومات او عکسونه به افشا کړي هم بلک میل کول او جنایي جرم دی. د پورن غچ اخیستنې په اړه نور معلومات دلته شته

د پورن غچ اخیستنې کومکي لیکه 0845 6000 459 – (Revenge Porn Helpline)
/www.revengepornhelpline.org.uk

دا هیڅکله سمه نده چې یو څوک په بل چا د لوڅو عکسونو استولو فشار راوړي.

دا په یاد ساتل مهم دي چې لیږل شوي عکسونه، حتی د سنیپ چیټ (Snapchat) په څیر خدماتو په کارولو سره، لاهم سکرین شاټ کیدای او خوندي کیدای شي. که تاسو یو لوڅ یا سکسی عکس لیږلی وي او تاسو د هغه څه په اړه اندیښمن یاست چې څه به وشي، نو کولای شئ د لاندې لارښوونو له لارې عمل وکړئ:

- د پیغام د ړنګولو غوښتنه وکړئ.
- ګوابنونو ته ځواب مه ورکوئ.
- له یو چا سره خبرې وکړئ او د ملاتړ غوښتنه وکړئ. تاسو کولای شئ د پورن غچ اخیستنې کومکي لیکې سره اړیکه ونیسئ .
- **راپور ورکړئ چې څه پیښ شوي**. تاسو کولای شئ د ناوړه مینځپانګې راپورهغې ویب پاڼې ته ورکړئ چې عکسونه پکې خپاره شوي. د ټولنیزو رسنیو ډیرې پلیټ فارمونه (ټګلاري) د مینځپانګې راپور ورکولو لپاره وسیله لري. تاسو باید پولیسو ته د دې ډول ځوروني راپور هم ورکړئ: 101 ته زنګ ووهئ که هغه بیړنئ حالت نه وي.

دا مهمه ده چې خبر اوسئ چې **د 18 کالو څخه کم عمر لرونکي کس** د لوڅ عکس شریکول د ماشومانو ناوړه ګټه اخیستنه او د 2003 کال د جنسي جرمونو د قانون له مخې جنایي جرم دی. یو عمل لکه د 18 کالو څخه کم عمر لرونکي کس ته "سیکستټ" ورکول ښایي د پولیسو د تحقیق لامل شي.

که تاسو د ماشومانو د عکسونو شریکولو په اړه اندیښمن یاست یا د ماشومانو د آنلاین خوندیتوب په اړه نورې اندیښنې لرئ، نو کولای شئ دا د ماشومانو د استثمار او آنلاین خوندیتوب (Child Exploitation and Online Protection) ساتنې مرکز ته رپوټ کړئ. www.ceop.police.uk

سایبري تعقیبوونه او ځارنه

تعقیبوونه د بل چا د چلند یوه بڼلګه ده چې تاسو په ویره کې اچوي چې ګواکې ستاسو پر وړاندې به تاوتریخوالی وکارول شي یا ستاسو د وارخطایي یا خوابدۍ لامل کیږي او ستاسو په ورځنیو معمول چارو باندې جدي اغیزه لري. کله چې هغه په آنلاین بڼه ترسره کیږي نو دی ته سایبري تعقیبوونه (cyberstalking) ویل کیږي. دا کېدای شي ستاسو په اړه معلومات راټولول، ستاسو تقلید (نقش لوبول)، د ناغوښتل شوو یا ګوابنونکو پیغامونو لیږل، ستاسو لیدل یا ستاسو آنلاین حساب ته لاسرسی موندل او ستاسو په اړه د ناسمو معلوماتو خپرول وي. یو تعقیبوونکی هغه څوک کیدای شي چې تاسو ته اشنا وي یا نا اشنا وي. سایبري تعقیبوونه کولای شي د هغه په قرباني باندې جدي اغیزه ولري او یو جنایي جرم دی.

د تعقیبوونې ملي کومکي لیکه– 0808 802 0300

/www.stalkinghelpline.org/faq/about-the-law

که تاسو اندیښنه لرئ چې تاسو تعقیبیږئ یا د ناوړه ګټې اخیستونکي لخوا لیدل کیږئ:

- د تعقیبوونکي سره له ښکېلېدو ډډه وکړئ، کوم چې ډیرې وختونه غواړي له تاسو سره خبرې وکړي او اړیکې پیدا کړي. هیڅکله د هغوي سره لیدو ته مه راضي کیږئ او مه ورسره مخ کیږئ.
- دا جدي ونیسئ اود نومورې فعالیت راپور پولیسو ته ورکړئ. تاسو کولای شئ 101 ته زنګ ووهئ چې له پولیسو سره راساً خبرې وکړئ خو که فکر کوئ چې یو سمدلاسه ګواښ شته نو 999 ډایل کړئ.
- د محرمیت تنظیمات (privacy settings) مو چک کړئ، ډاډ ترلاسه کړئ چې ستاسو په اړه لږترلږه آنلاین معلومات شته، او په خپله وسیله کې د موقعیت ټګینګ (location tagging) بند کړئ.
- خپلو شاوخوا خلکو ته خبرداری ورکړئ. دوي ښایي دې ته اړتیا ولري چې وپلټي چې ستاسو په اړه څه شریکوي او ښایي اړتیا ولري چې خپل د محرمیت تنظیمات هم وپلټي.
- د هغه څه چې پیښیږي ریکارډ وساتئ – تاسو ښایي د زنګونو، پیغامونو یا ټولنیزو رسنیو پوستونو سکرین شاټ وغواړئ، پدې معنی چې تاسو د شواهدو کاپي لرئ حتی که مجرم د دوي پیغامونه او پوستونه بیا وروسته ړنګ هم کړي.

یو ناوړه ګټه اخیستونکی کولای شي په احتمالي توګه د انټرنیټ د فعالو شویو وسیلو له ځانګړتیاوو څخه ناوړه ګټه پورته کړي ترڅو قرباني وګوري، چک کړي او کنټرول کړي. پدې کې د نورو خلکو سره ستاسو د اړیکي ځارل، ستاسو د وسیلې له لارې ستاسو موقعیت تعقیبول، یا ستاسو د مالي لګښتونو چک کول شامل دي. کله چې نوموړي چلندونه د ژوند یوه شریکوال، د ژوند پخواني شریکوال، د کورنۍ غړي یا پالونکي لخوا ترسره شي نو دا ټول د انګلستان د قانون له مخې د کورني ناوړه ګټې اخیستنې ډولونه ګڼل کیږي.

که تاسو اندیښمن یاست چې کوم څوک به ښایي ستاسو ګرځنده تلیفون یا کومه بله وسیله ځاري نو د کورني ناوړه ګټې اخیستنې ملي کومکي لیکه یو واک ترو وسیله (walk-through tool) لري چې له تاسو سره د وسیلې خوندي کولو لپاره د تنظیماتو په بدلولو کې مرسته کوي.

د کورني ناوړه ګټې اخیستنې ملي کومکي لیکه (24 ساعته) 0808 220 0247

www.nationaldomesticviolencehelpline.org.uk

ایا تاسو د لاندې ځرګندونو سره موافق یاست؟

آنلاین ګواښونه واقعاً مهم ندي ځکه چې دا ریښتینی نړۍ نده

نه. آنلاین ناوړه ګټه اخیستنه جدي ده، د خلکو په ژوند جدي اغیزه لري او ټل باید د چارواکو لخوا جدي چلند ورسره وشي. تعقیبوونه، ځارنه، او ځوروونه ټول د لوړ خطر چلندونه دي چې ستاسو تیروتنه نده. تاسو حق لرئ د دې راپور ورکړئ، مشوره وغواړئ او د حل لپاره یې ملاتړ ترلاسه کړئ.

د ځورونې جرم پدې معنی دی چې په ریښتیني ژوند کې له تاوتریخوالي سره ګواښل کیږي.

قانون وایی چې ځورول هغه وخت پیښیږي کله چې یو څوک په داسې طریقه چلند کوي چې موخه یې ستاسو خوابدي کول یا ستاسو وارخطا کول وي او دا چلند له یو ځل څخه زیات پیښ شي. دا په جلا وختونو یا جلا حالاتو کې د چلند مختلف ډولونه کیدای شي. د بیلګې په توګه، یو پیغام چې موخه یې ستاسو خوابدي کول وي، ځورونکی ندی. دوه پیغامونه ښایي ځورونکي وي، یا د تلیفون له زنګ څخه وروسته د ګواښونکي بریښنالیک ځورونکی کیدای شي. نور فعالیتونه چې د ځورونې په توګه ګڼل کیدای شي دا دي؛ که تاسو تعقیب شوي یاست، ستاسو کور یا کار لیدل شوی وي، ستاسو ملکیت زیانمن شوی وي، یا که تاسو په ناوړه او غلط ډول پولیسو ته راپور ورکړئ کله چې تاسو هیڅ غلط کار ندی کړی.

زهرا د تره لور لري چې هغې ته خورا نږدې ده. د هغې د تره لورپه دې وروستیو کې نا آشنا چارې کولې، هغه خفه او تند خویه ښکاري او کله چې سره یوځای وي نو په وسواس سره خپل تلیفون هر وخت چک کوي. بالاخره، د زهرا د تره لور ورته وایي چې هغې سم خوب نه دی کړی او هغه د خپل پخواني میړه د ګواښونو له امله ډیره خوابدي ده له کوم څخه چې هغه جلا کېدونکي ده. هغه هغې ته په منظم ډول پیغامونه لیږي او بریښنالیکونه استوي ترڅو ورته ووایی چې هغه یوه وحشتناکه میرمن او مور ده، او د دوي دواړو کورنیو ته یې شرم راوړی، او دا چې هغه باید بیرته ورشي او د هغه سره ژوند وکړي. د زهرا د تره لورد دې پیښې په یادولو سره خورا خوابدي ده.

هغه زیاتوي چې د هغې پخوانی میړه د هغې یو لوڅ عکس لري، کوم چې دوي یوځای اخیستی ؤ کله چې د دوي اړیکي سالمې وې. هغه ګواښ کړی دی که چیرې هغې ته بیرته ستنه نه شي نو د هغې کورنۍ ته به یې لوڅ عکس ولیږي.

ایا د زهرا د تره لور د جرم قرباني ده؟

هو. د زهرا د تره لور د **ځورونې او جبري کنټرول** قرباني ده. دا ګواښونه د زهرا د تره د لور په وړاندې شوي ترڅو د هغې د کنټرولولو هڅه وکړي. قانون وایی چې دا سرغړونه هغه وخت کیږي کله چې یو څوک په داسې طریقه چلند کوي چې موخه یې ستاسو د خوابدۍ یا وارخطایي لامل کېدل وي. نوموړی چلند باید له یو څخه ډیر ځله پیښ شي.

لکه څنګه چې دا چلند د هغې د پخواني میړه لخوا ترسره کیږي، دا ځورونه د **جبري کنټرول** یوه بڼه ده (د **کورني ناوړه چلند** یو ډول). دا یو جنایي جرم دی. هغه باید پولیسو ته د هغه راپور ورکړي.

دا د پورن غچ اخیستنې یو ګواښ هم دی، کوم چې د خوابدۍ یا سپکاوي لامل کېدو په موخه د هغې شخصي لوڅ عکسونه پرته له اجازې شریکول. ګواښ پخپله جرم نه دی، په هرصورت که د زهرا پخوانی میړه دا عکس آنلاین، د بریښنالیک یا ټولنیزو رسنیو له لارې شریک کړي، پشمول د WhatsApp یا نورو پیغام رسولو خدماتو، نو هغه به یو جرم شي.

د زهرا میړه د کورنۍ دعزت او د دوي د جلا کیدو په اړه هم خبرې کوي چې کورنۍ ته 'شرم' راوړي. تش په نوم تاوتریخوالی د ناوړه ګټې اخیستنې یوه بیلګه ده او زهرا ښایي وغواړي د یوه سازمان ملاتړ ترلاسه کړي چې د ناموس پر اساس د ناوړه ګټې اخیستنې او ګواښونو قربانیانو سره په کار کولو کې تخصص لري. **کارما نروانا (Karma Nirvana)** د دوشنبې څخه تر جمعې پورې د تلیفون کومکي لیکه چلوي 0800 5999 247 www.karmanirvana.org.uk

لنډیز

- د پوسټ کولو دمخه فکر وکړئ. شیان مه اپلوډ کوئ یا مه شریکوئ؛ پرته لدې چې تاسو په پام کې ولرئ چې که دا غلطو لاسونو ته ورسیږي تاسو به څه احساس کړئ. یوځل چې تاسو یو څه پوسټ کړئ تاسو د هغه کنټرول له لاسه ورکوئ، په ځانګړي توګه که بل څوک یې سکرین شاټ واخلي.
- **خپل هویت خوندي کړئ او هرڅه په ټولنیزو رسنیو مه شریکوئ. ټولنیزې رسنۍ په زړه پورې دي چې ملګرو او کورنۍ ته اجازه ورکوي چې په تماس کې پاتې شي خو پدې اړه فکر وکړئ چې تاسو ښایي نړۍ ته ستاسو د خپل ژوند په اړه له هغه څه څخه ډیر څه وواياست چې اراده یې لرئ.**
- په دقت سره په پام کې ونیسئ چې څوک کولای شي هغه څه وګوري چې تاسو یې آنلاین شریکوئ، چک کړئ چې ستاسو د محرمیت تنظیمات لوړې کچې ته تنظیم شوي او د دې په اړه فکر وکړئ چې تاسو له چا سره خبرې کوئ.
- **د درغلیو له نښو او د سکیم بریښنالیکونو او ویب پاڼو د لیدلو له ځرنګوالی څخه خبر اوسئ**
- هیڅکله ډیر شخصي معلومات آنلاین مه را اخلئ لکه ستاسو پته، د تلیفون شمیره، بشپړ نوم، او د زیږون نیټه.
- هیڅکله خپل لاګ په توضیحاتو او پاسورډونو کې مه ورکوئ.
- هیڅکله نامعلوم بریښنالیکونه، فایلونه یا ضمیمې مه پرانیځئ او د فیشینګ او درغلیو څخه خبر اوسئ