



HEDDLU  
DE CYMRU  
SOUTH WALES  
POLICE



Comisiynydd  
yr Heddlu a  
Throseddu  
De Cymru

South Wales  
Police  
and Crime  
Commissioner

# Canllawiau Seiberstelcio ac Aflonyddu

---

Heddlu De Cymru

---

2025

Mae'r ddogfen hon hefyd ar gael yn Seisneg

This document is also available in English.



Defnydd mynych a bwriadol o'r rhyngwyd a dulliau cyfathrebu electronig eraill i gyfathrebu mewn modd parhaus a dieisiau gyda'r bwriad o ddychryn rhywun, ei fygwth neu aflonyddu arno yw seiberstelcio.

Mae'r canllawiau a roddir yn y llyfryn hwn yn cynnwys gwybodaeth gyfredol o fis Ionawr 2025. Dylai'r llyfryn hwn gael ei adolygu a'i ddiweddarau y flwyddyn ganlynol ym mis Ionawr 2026. Os bydd unrhyw wybodaeth yn dyddio, gweler y ganolfan gymorth ar gyfer y pwnc dan sylw, y gellir chwilio amdani ar-lein.

Hefyd, mae'r llyfryn hwn yn cynnwys y dulliau a allai gael eu defnyddio gan troseddwr stelcio ac aflonyddu digidol. Nid yw hyn yn golygu y bydd yr holl ddulliau y sonnir amdanynt yn berthnasol i'ch amgylchiadau chi, ond byddant yn eich helpu i atal y posibilrwydd y bydd y troseddwr yn defnyddio'r dulliau hyn yn y dyfodol.

Dylech hefyd fod yn ymwybodol y bydd cael gwared ar y dulliau stelcio technolegol y gall y troseddwr eu defnyddio yn cynyddu'r risg y bydd yn cyflawni ei weithredoedd wyneb yn wyneb yn lle hynny.

## Rhoi Gwybod am Ddigwyddiad

Pan fyddwch yn darllen y ddogfen hon, mae'n bosibl y byddwch chi neu rywun rydych yn ei adnabod yn wynebu seiberstelcio ac aflonyddu. Mae'n bwysig rhoi gwybod i'r gwasanaethau cywir er mwyn eich diogelu eich hun ac eraill.

### Help a chefnogaeth

### Os nad yw'n argyfwng

Os nad yw'n argyfwng, gallwch roi gwybod:

- ar-lein
- drwy ffonio 101
- drwy fynd i orsaf heddlu

### A yw'n argyfwng?

A yw'n teimlo fel y gallai'r sefyllfa fynd yn danbaid neu'n dreisgar yn fuan iawn? A oes rhywun mewn perygl uniongyrchol? A oes angen cymorth arnoch ar unwaith? Os felly, ffoniwch 999 nawr.

Os oes gennych amhariad ar eich clyw neu'ch lleferydd, defnyddiwch ein gwasanaeth ffôn testun ar 18000 neu anfonwch neges destun atom ar 999 os ydych wedi cofrestru â gwasanaeth SMS brys.



<b>Rhagair</b>	<b>6</b>
<b>Cyflwyniad</b>	<b>7</b>
Y Darlun Cenedlaethol	8
Trais yn Erbyn Menywod a Merched – y Gofyniad Plismona Strategol a'r Fframwaith Cenedlaethol ar Gyfer Cyflawni	9
<b>Rhan Un: Canllawiau ar gyfer Cyfrifon Cyfryngau Cymdeithasol</b>	<b>11</b>
Facebook & Instagram (both owned by Meta)	12
X (formerly known as Twitter)	16
WhatsApp	18
TikTok	20
Snapchat	22
Ffugenwau	24
Docsio	25
Cyfrifon dynwared/ffug	26
<b>Rhan Dau: Canllawiau ar gyfer Ffonau Symudol (Apple ac Android)</b>	<b>29</b>
Negeseuon e-bost	30
Rhif ffôn symudol a negeseuon llais	31
Cyfrifon Apple ID ac iCloud	32
Cyfrifon Android	33
Sut i greu cyfrineiriau cryf a rhoi prawf dilysu dau gam ar waith	34
'Find My' a nodweddion eraill sy'n dangos lleoliad (Apple)	36
Google Location (Android)	38
Cyfrifon plant ar Android ac Apple	40
Ysbiwedd	42
Ffurfweddu gwasanaethau brys	44
<b>Dyfeisiau cysylltiedig</b>	<b>46</b>
AirPods/Clustffonau	47
Watshys clyfar	48
AirTags a Chipolo	50

<b>Rhan Tri: Canllawiau ar gyfer Apiau Ar-lein</b>	<b>53</b>
Bancio ar-lein	54
Apiau siopa a chludfwyd	56
Apiau caru	57
Apiau cludiant	58
Apiau rhedeg (Strava)	60
Apiau sy'n cysylltu â cheir	62
<b>Rhan Pedwar: Canllawiau ar gyfer Adloniant Ar-lein</b>	<b>64</b>
Chwarae gemau	65
Cyfrifon ffrydio (Netflix, Disney+, Amazon Prime ac ati)	66
<b>Rhan Pump: Canllawiau ar gyfer Llwybryddion Wi-Fi</b>	<b>69</b>
Rhwydweithiau preifat rhithwir (VPNs)	71
<b>Rhan Chwech: Canllawiau ar gyfer Gliniaduron/Cyfrifiaduron</b>	<b>73</b>
Dyfeisiau Mac	74
Dyfeisiau Windows	78
<b>Rhan Saith: Canllawiau ar wneud Copïau wrth gefn o'ch Data</b>	<b>83</b>
<b>Rhan Wyth: Canllawiau ar gyfer Dyfeisiau Clyfar/Y Rhyngwyd Pethau</b>	<b>86</b>
Gwylidwriaeth cloch drws	87
Dyfeisiau Alexa a/neu ddyfeisiau â nodweddion tebyg	88
Setiau teledu clyfar	90
Camerâu gwarchod/gwe-gamerâu	91
Systemau hyb cartref	92
Dyfeisiau a gafodd eu rhoi'n rhodd gan y troseddwr	93
<b>Rhan Naw: Canllawiau ar gyfer Tracio Ceir</b>	<b>95</b>
Tracwyr ceir ffisegol	96
Camerâu dashfwrdd	97
<b>Rhan Deg: Canllawiau ar gyfer Trydydd Partion</b>	<b>98</b>
<b>Rhan Un ar Ddeg: Deddf Camddefnyddio Cyfrifiaduron 1990 a Deddf Troseddau Rhywiol 2003</b>	<b>100</b>
<b>Rhan Deuddeg: Deallusrwydd Artiffisial (AI)</b>	<b>104</b>
<b>Cyfeiriadau</b>	<b>106</b>



## Rhagair

Chloe Williams, Myfyrwraig Raddedig  
mewn Seiberddiogelwch

Yn ystod fy nghyfnod yn y brifysgol, fy mhrif bwnc oedd Seiberddiogelwch. Roedd angen i mi gwblhau traethawd hir, a phenderfynais ganolbwyntio ar effaith peirianeg gymdeithasol ar ein cymdeithas. O edrych yn ôl, rwy'n sylweddoli na wnes i weld y cysylltiad rhwng peirianeg gymdeithasol a stelcio ac aflonyddu. Fodd bynnag, drwy weithio ar Brosiect Athena, bu modd i mi edrych drwy lens wahanol. Erbyn hyn, rwy'n gweld y gall peirianeg gymdeithasol gael ei defnyddio fel un o lawer o ddulliau at ddibenion llawer mwy anghyfreithlon.

Cefais fy annog i ymgymryd â'r prosiect hwn gan y Ditectif Arolygydd Andrew Westlake, a bwysleisiodd effaith trais yn erbyn menywod a merched ar ein cymdeithas, ac ar ein heddluoedd hefyd. Ar ôl siarad â Chydgysylltydd Stelcio ein heddlu, roedd yn amlwg bod datblygiadau technolegol yn arwain at ddatblygiad anffodus yn y ffordd y gall troseddwr ddefnyddio dulliau digidol i stelcio eu goroeswyr ac aflonyddu arnynt. Gwnaeth fy rheolwr llinell annog y prosiect hwn ymhellach a chynnig canolbwyntio ar ganllawiau y gellir eu rhoi i swyddogion, staff a goroeswyr ynglŷn â stelcio ac aflonyddu digidol.

Daeth rhwydwaith dadansoddwyr CSAE (2024) i'r casgliad mai stelcio ac aflonyddu yw 85% o'r

holl droseddau ar-lein a throseddau a alluogir gan dechnoleg. Mae hyn yn destun pryder enfawr nid yn unig i'n cymdeithas, ond hefyd i'r holl heddluoedd ledled y wlad, ac mae'n un y mae Heddlu De Cymru wir yn ei gymryd o ddifrif.

Pan oeddwn yn gweithio ar Brosiect Athena, cefais gyfle i siarad â goroeswraig trais yn erbyn menywod a merched. Drwy fod yn ddigon dewr i siarad am y profiadau personol y mae wedi'u hwynebu, ac mae'n dal i'w hwynebu, daeth â'r pwnc hwn yn fyw i mi i raddau helaeth iawn. Gwnaeth clywed am y ffordd y bydd yr oroeswraig hon yn byw ei bywyd bob dydd, oherwydd gweithredoedd y troseddwr, wir fy nhristâu. Ei phrofiad hi oedd un o ffactorau allweddol fy nghymhelliant, ac rwy'n gobeithio y bydd y prosiect hwn yn gymorth, ni waeth pa mor fach, i oroeswyr stelcio ac aflonyddu digidol groesawu normalrwydd yn ôl i'w bywydau.

Drwy gwblhau Prosiect Athena, rwy'n gobeithio codi ymwybyddiaeth o'r dulliau a gaiff eu defnyddio gan droseddwr stelcio ac aflonyddu digidol. Hefyd, rwy'n gobeithio y bydd yn rhoi gwybodaeth i swyddogion, staff a goroeswyr am ffyrdd o sicrhau diogelwch dyfeisiau ac atal y troseddau hyn rhag digwydd.



## Cyflwyniad

Cyrhaeddodd trais yn erbyn menywod a merched anterth o ran ymwybyddiaeth y cyhoedd yn dilyn cyfres o ymosodiadau gan ddynion dieithr ar fenywod a arweiniodd at y canlyniadau mwyaf dinistriol.

Yn nodedig yn eu plith roedd Bibaa Henry a Nicole Smallman, a lofruddiwyd ym mis Mehefin 2020 ar ôl cynnal picnic pen-blwydd mewn parc yn Llundain, Sarah Everard, a gafodd ei herwgipio, ei threisio a'i lofruddio gan swyddog heddlu a oedd yn gwasanaethu ar y pryd ym mis Mawrth 2021, a Sabina Nessa a lofruddiwyd ym mis Medi yr un flwyddyn yn ne Llundain tra oedd, fel Sarah, yn cerdded adref.

Y rhain yw'r achosion mwyaf ffiائد ac, yn anffodus, mae trais yn erbyn menywod a merched yn ymledu i lawer o droseddau eraill, gan gynnwys cam-drin domestig, stelcio, aflonyddu, ymddygiad rheolaethol a gorfodaethol, ymosod a chamfanteisio, i enwi ond rhai.

Effeithir yn anghymesur ar fenywod a merched, ac mae'r troseddau hyn yn peri pryder i'r graddau bod y DU wedi mynd ati i roi'r un statws i drais yn erbyn menywod a merched â therfysgaeth, gan ei wneud yn fygythiad cenedlaethol fel rhan o'r Gofyniad Plismona Strategol.



**“Mae troseddau trais yn erbyn menywod a merched yn cyfeirio at droseddau gaiff eu cyflawni gan ddynion yn erbyn menywod yn bennaf, ond nid yn unig. Mae hyn yn cynnwys digwyddiadau sy'n gysylltiedig â cham-drin domestig, gan gynnwys ymddygiad rheolaethol neu orfodaethol, treisio a throseddau rhywiol eraill, stelcio, aflonyddu, cam-drin seiliedig ar ‘anrhydedd’ fel y'i gelwir, priodas dan orfod, anffurfio organau cenhedlu benywod, cam-drin plant yn rhywiol, caethwasiaeth fodern a masnachu pobl gyda ffocws ar gamfanteisio rhywiol, puteindra, pornograffi ac anlladrwydd”**

(Gwasanaeth Erlyn y Goron, 2019)



## Y Darlun Cenedlaethol

O Ddatganiad Plismona Cenedlaethol 2024 ar gyfer trais yn erbyn menywod a merched, gwyddom y canlynol;

- Bydd o leiaf un o bob 12 o fenywod yn goroesi trais yn erbyn menywod a merched bob blwyddyn (dwy filiwn o oroeswyr) – er y disgwylir i'r ffigur gwirioneddol fod yn uwch am na roddir gwybod am droseddau'n ddigonol
- Rhwng mis Ebrill 2022 a mis Mawrth 2023, roedd troseddau trais yn erbyn menywod a merched yn cyfrif am ychydig o dan 20% o'r holl droseddau a gofnodir gan yr heddlu
- Mae pum bygythiad allweddol sy'n achosi niwed mawr wedi cael eu nodi, sef; trais rhywiol, cam-drin domestig, stelcio, cam-drin a chamfanteisio'n rhywiol ar blant, a thrais yn erbyn menywod a merched ar-lein ac a alluogir gan dechnoleg
- Yn y flwyddyn a ddaeth i ben ym mis Mawrth 2023, cofnododd yr heddlu: 103,135 o droseddau treisio a throseddau rhywiol difrifol, 400,213 o droseddau cysylltiedig â cham-drin domestig, 436,196 o droseddau stelcio ac aflonyddu a, rhwng mis Awst 2022 a mis Gorffennaf 2023, cafodd 41,540 o achosion o

gam-drin a chamfanteisio'n rhywiol ar blant eu cyflawni yn erbyn merched rhwng 10 a 17 oed.

- Rhwng mis Awst 2022 a mis Gorffennaf 2023, cyflawnwyd o leiaf 123,515 o droseddau trais yn erbyn menywod a merched a oedd yn cynnwys elfen ar-lein, sy'n dangos y ffordd y mae bygythiad troseddau trais yn erbyn menywod a merched ar-lein ac a alluogir gan dechnoleg yn datblygu.
- Stelcio ac aflonyddu oedd 85% o'r holl droseddau ar-lein a throseddau a alluogir gan dechnoleg.

Daeth Policing UK yn fwy ymwybodol o droseddau a alluogir ac a hwylusir gan dechnoleg yn 2023, yn dilyn euogfarn cyn-swyddog heddlu a oedd wedi hwyluso camdriniaeth rywiol a blacmel cannoedd o fenywod ifanc ar-lein, gan arwain at ddedfryd ddigynsail o garchar am oes.

Yn sgil datblygiad technoleg glyfar, gwyddom fod modd tracio cartrefi, cerbydau a dyfeisiau, ac y gellir cyflawni gwyliadwriaeth o bell, a hynny'n aml heb yn wybod i bobl eraill, os na chaiff mesurau rheoli mynediad cadarn eu rhoi ar waith.

## Trais yn Erbyn Menywod a Merched – Y Gofyniad Plismona Strategol a'r Fframwaith Cenedlaethol ar gyfer Cyflawni

Strategol, ac mae iddo gynllun sy'n seiliedig ar bedwar sbardun allweddol ('4P' yn Saesneg) sef Ymlid, Paratoi, Amddiffyn ac Atal, ac sy'n gweithredu ochr yn ochr â'r Fframwaith Cenedlaethol ar gyfer Cyflawni.

Mae gan Heddlu De Cymru ei gynllun gweithredu ei hun sy'n cyd-fynd â'r un blaenoriaethau sef, yn gryno;

### Ymlid:

Rydym yn gyfrifol am ymlid troseddwyr trais yn erbyn menywod a merched am eu bod yn achosi niwed sylweddol ac yn aml yn troseddu'n fynych.

Rhaid i ni dargedu ein hadnoddau er mwyn ymlid y troseddwyr sy'n achosi'r niwed mwyaf ac sy'n troseddu'n fynych – mae hyn yn gysylltiedig â'n pum bygythiad allweddol.

### Amddiffyn:

Mae dyletswydd statudol arnom i amddiffyn a diogelu goroeswyr trais yn erbyn menywod a merched.

Rhaid i ni wella'r ffordd yr awn ati i amddiffyn goroeswyr trais yn erbyn menywod a merched, gan gydnabod y cydbwysedd sy'n ofynnol rhwng camau gorfodi amserol a diwallu anghenion ehangach goroeswyr.

### Paratoi:

Un o ofynion sylfaenol ymlid troseddwyr trais yn erbyn menywod a merched yn effeithiol yw sicrhau bod gennym y galluoegrwydd, y capasiti a'r diwylliant cywir.

Rhaid i ni flaenoriaethu proffesiynoldeb ac arbenigedd ein gweithlu, gan ddefnyddio adnoddau'n effeithiol heb danseilio ein gofynion gweithredol.

Rydym yn ymrwymedig i wella ein hymateb i drais yn erbyn menywod a merched ar-lein ac a alluogir gan dechnoleg, drwy wneud y canlynol;

- darparu ymateb wedi'i deilwra i niwed ar-lein er mwyn amddiffyn goroeswyr o bob oedran
- adnabod bygythiad deallusrwydd artifisial cynhyrchiol (ei fygythiad i bobl ifanc), ei deall a bod yn barod i ymateb iddo
- digon o adnoddau penodedig a hyfforddiant a recriwtio arbenigol
- annog y llywodraeth i atgyfnerthu trefniadau rheoleiddio er mwyn atal trais yn erbyn menywod a merched rhag ymledu'n barhaus ar-lein.

### Atal:

Rydym yn glir ynghylch ein rôl o fewn dull system gyfan o atal trais yn erbyn menywod a merched

Rhaid i ni allu ymateb mewn partneriaeth ac mewn modd cydgysylltiedig i drais yn erbyn menywod a merched, gyda ffocws ar atal yn gynnar, gan gyflawni ein rôl ni o fewn hynny.

Mae Heddlu De Cymru a Chomisynydd yr Heddlu a Throseddu wedi datgan eu hymrwymiad parhaus i drechu trais yn erbyn menywod a merched.



## Rhan Un: Canllawiau ar gyfer Cyfrifon Cyfryngau Cymdeithasol

Rhyngweithio ymhlith pobl lle y byddant yn creu, yn rhannu a/neu'n cyfnewid gwybodaeth mewn cymunedau a rhwydweithiau rhithwir.



## Facebook a Instagram (sydd ill dau'n eiddo i Meta)

**Instagram** - ap rhannu ffotograffau a fideos sy'n eich galluogi i anfon negeseuon at ffrindiau.

**Facebook** - ap sy'n eich galluogi i anfon negeseuon a phostio diweddariadau statws er mwyn cadw mewn cysylltiad â theulu a ffrindiau.

### Bydd y troseddwr yn defnyddio Facebook ac Instagram i wneud y canlynol:

**Cael gwybodaeth o'ch proffil** - er enghraifft, gallai edrych ar eich postiau er mwyn gweld â phwy y byddwch yn treulio amser (ffotograffau ohonoch chi gyda theulu neu ffrindiau).

**Gwneud sylwadau ar bopeth y byddwch yn ei bostio** - gallai'r sylwadau hyn fod yn ddifriol/yn fygythiol.

**Defnyddio'r nodweddion negeseua** - er enghraifft, eich peledu'n barhaus â negeseuon drwy gydol y dydd.

**Eich tagio neu sôn amdanoch mewn postiau** - gallai eich tagio neu sôn amdanoch mewn postiad amhriodol y bydd eich holl ddilynwyr yn gallu ei weld.

**Mewngofnodi i'ch cyfrif** - os bydd gan y troseddwr fynediad i'ch cyfrif, gallai bostio cynnwys amhriodol ar eich proffil. Gallai hefyd ddarllen eich negeseuon a/ neu anfon negeseuon at eich teulu a'ch ffrindiau yn esgus mai chi ydyw.

**Ceisio gweld ble ydych chi** - os byddwch wedi symud i ffwrdd oddi wrth y troseddwr, gall edrych ar eich proffil i weld a yw'r cynnwys yn dangos ble ydych chi (er enghraifft, ym mha dref).

Bydd llawer o bobl yn defnyddio Facebook, Instagram neu'r ddau. Mae'r canllawiau isod yn berthnasol i'r ddau lwyfan.

### Blocio pobl

Blociwch y troseddwr ac unrhyw gyfrifon eraill a all fod ganddo. Dylech hefyd edrych drwy eich rhestr 'dilynwyr'/'ffrindiau', a chael gwared ar unrhyw bobl sy'n eich dilyn chi ac sy'n gysylltiedig â'r troseddwr.

**Ewch i broffil y person yr hoffech ei flocio > cliciwch y tri dot (...) > tapiwch 'Block'.**



### Gosodiadau Preifatrwydd

Edrychwch ar eich gosodiadau preifatrwydd a ffurfweddwch eich cyfrif i fod yn breifat; bydd gwneud eich cyfrif yn breifat yn eich galluogi i benderfynu pwy fydd yn gallu eich dilyn/bod yn ffrindiau â chi.

#### Crëwch gyfrif preifat

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf eich proffil > tapiwch 'Account privacy' > tapiwch y togl wrth ymyl 'Private account'.

**Facebook** - tapiwch 'Menu' gyda'ch llun proffil yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > sgroliwch i lawr i 'Audience and visibility' a thapiwch 'Followers and public content' > wrth ymyl 'Who can follow me' dewiswch 'friends'.

#### Diffoddwch eich statws gweithgarwch

Bydd hyn yn atal cyfrifon sy'n eich dilyn rhag gweld pryd roeddech ar-lein ddiwethaf:

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf eich proffil > sgroliwch i lawr i 'How others can interact with you' a thapiwch 'Messages and story replies' > tapiwch 'Show activity status' > sicrhewch fod y togl wedi'i ddiffodd.

**Facebook** - tapiwch 'Menu' gyda'ch llun proffil yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > sgroliwch i lawr i 'Audience and visibility' a thapiwch 'Active status' > sicrhewch fod y togl wedi'i ddiffodd.



## Mesurau rheoli negeseuon

Penderfynwch a fydd ceisiadau negeseuon yn mynd i'ch rhestr sgysiau, neu i'ch ffolder "Message requests", neu a fyddwch yn eu cael o gwbl:

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf eich proffil > sgrolwch i lawr i 'How others can Interact with you' a thapiwch 'Messages and story replies' > tapiwch 'Message controls' > tapiwch 'Others on Instagram' > sicrhewch fod 'Don't receive requests' wedi'i farcio.

**Facebook** - ewch i ap Messenger > tapiwch 'Privacy & Safety' > o dan 'who can reach you' tapiwch 'Message delivery' > tapiwch 'Others on Messenger or Facebook' > sicrhewch fod tic wrth ymyl 'Don't receive requests'.

## Tagio a Sôn

Dewiswch pwy sy'n gallu eich tagio yn eu ffotograffau a'u riliau, a phwy sy'n gallu sôn amdanoch gan ddefnyddio '@' er mwyn cysylltu eich cyfrif â'u straeon, postadau ac ati. .

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf eich proffil > sgrolwch i lawr i 'How others can Interact with you' a thapiwch 'Tags and Mentions' > o dan 'who can tag you' tapiwch 'don't allow tags' neu toglwch 'Manually approve tags' a thoglwch 'Don't allow mentions.'

**Facebook** - tapiwch 'Menu' gyda'ch llun proffil yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > sgrolwch i lawr i

'Audience and visibility' a thapiwch 'Profile and tagging' > ar gyfer 'who can see what others post on your profile?' dewiswch 'only me' o'r gwymplen. Ar gyfer yr adran 'Tagging', dylai 'Only me' fod wedi'i ddewis ar gyfer y naill a'r llall. Hefyd, dylai'r ddau dogl fod wedi'u galluogi yn yr adran 'Reviewing'.

**Noder** - Bydd hyn yn sicrhau y gallwch fwrw golwg dros unrhyw ffotograffau a gaiff eu tagio cyn iddynt gael eu postio. Diben hyn yw cadw eich lleoliad yn gyfrinachol gan y bydd llawer o bobl yn tagio'r lle ar eu postadau, neu am y bydd cefndir y ffotograff yn ei gwneud hi'n hawdd gwybod ble ydych chi o bosibl.

## Gwybodaeth bersonol

Tynnwch unrhyw wybodaeth bersonol oddi ar eich cyfrifon cyfryngau cymdeithasol.

## Rhwystrwch beiriannau chwilio rhag cysylltu â'ch proffil

**Instagram** - er mwyn atal peiriannau chwilio rhag cysylltu â'ch proffil Instagram, bydd yn rhaid i chi wneud cais drwy eu tudalennau gwe 'Help/Support'.

**Facebook** - tapiwch 'Menu' gyda'ch llun proffil yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > sgrolwch i lawr i 'Audience and visibility' a thapiwch 'How people can find and contact you' > sicrhewch fod y togll 'Do you want search engines outside Facebook to link to your profile' wedi'i analluogi.

## Os byddwch yn credu bod y troseddwr wedi/yn gallu cael mynediad i'ch cyfrif Instagram/ Facebook

Newidiwch eich cyfrineiriau a rhowch brawf dilysu dau gam ar waith.

### Newidiwch eich cyfrineiriau

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf tudalen eich proffil > sgrolwch i lawr i 'privacy centre' a thapiwch arno (bydd hyn yn mynd â chi i ganolfan Meta, lle y dylai eich cyfrif Facebook a'ch cyfrif Instagram fod) > tapiwch yr eicon 'More' sydd yn y gornel dde uchaf > tapiwch 'Manage your accounts' > o dan 'Account settings' tapiwch 'Password and security' > tapiwch 'Change password' > dewiswch y cyfrif yr hoffech newid ei gyfrinair.

**Facebook** - cliciwch y tab 'Menu' yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > tapiwch 'Meta accounts centre' a fydd i'w weld ar y brig > tapiwch 'Password and security' > 'Change password'

### I roi prawf dilysu dau gam ar waith

Yn hytrach na thapio 'change password' wrth ddilyn y camau uchod, fe welwch 'Two-factor authentication' oddi tano i'w dapio yn lle hynny.

**Noder** - gallwch hefyd gael rhybuddion mewngofnodi drwy dapio 'Login alerts' sydd o dan 'Where you're logged in'.

Dylech wneud yn siŵr mai eich manylion chi eich hun yw'r manylion adfer – gellir gwneud hyn drwy gymryd yr un camau ag y sonnir amdanynt uchod ond, yn hytrach na thapio 'Password and security', tapiwch 'Personal details'. Bydd hyn yn dweud wrthyhych pa gyfeiriadau e-bost a rhifau ffôn sy'n gysylltiedig â'ch cyfrif. Gallwch ddileu cyfeiriad e-bost neu rif ffôn drwy eu tapio ac yna 'delete email' neu 'delete number'.

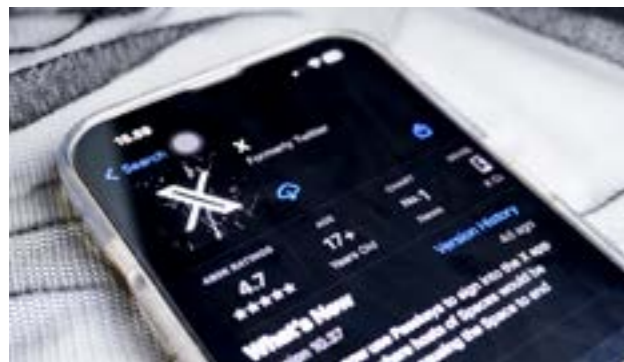
## Edrychwch dros eich dyfeisiau cysylltiedig a'ch hanes mewngofnodi

Os gwelir tystiolaeth bod rhywun arall wedi bod yn defnyddio eich cyfrif, dylid tynnu sgrinlun:

**Instagram** - cliciwch yr eicon 'More' yng nghornel dde uchaf tudalen eich proffil > sgrolwch i lawr i 'privacy centre' a thapiwch arno (bydd hyn yn mynd â chi i ganolfan Meta, lle y dylai eich cyfrif Facebook a'ch cyfrif Instagram fod) > tapiwch yr eicon 'More' sydd yn y gornel dde uchaf > tapiwch 'Manage your accounts' > o dan 'Account settings' tapiwch 'Password and security' > tapiwch 'Where you're logged in' > edrychwch dros eich cyfrifon Instagram a Facebook drwy dapio arnynt.

Os gwelwch ddyfais nad ydych yn ei hadnabod > tapiwch 'Select device to log out'.

**Facebook** - cliciwch y tab 'Menu' yn y gornel dde isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > tapiwch 'Meta accounts centre' a fydd i'w weld ar y brig > tapiwch 'Password and security' > o'r cam hwn, bydd y camau nesaf yr un fath â'r rhai uchod.



## X (Twitter gynt)

Safle rhwydweithio cymdeithasol lle y bydd pobl yn cyfathrebu drwy negeseuon byr.

### Bydd y troseddwr yn defnyddio X i wneud y canlynol:

#### Defnyddio'r nodweddion negeseua

- er enghraifft, eich peledu'n barhaus â negeseuon difriol drwy gydol y dydd.

#### Eich tagio neu sôn amdanoch mewn postiau

- gallai eich tagio neu sôn amdanoch mewn postiad amhriodol y bydd eich holl ddilynwyr yn gallu ei weld.

**Gwneud sylwadau ar bopeth y byddwch yn ei bostio** - gallai'r sylwadau hyn fod yn ddifriol/yn fygythiol.

**Mewngofnodi i'ch cyfrif** - os bydd gan y troseddwr fynediad i'ch cyfrif, gallai bostio cynnwys amhriodol ar eich proffil. Gallai hefyd ddarllen eich negeseuon a/ neu anfon negeseuon at eich teulu a'ch ffrindiau yn esgus mai chi ydyw.

## Tewi a blocio

Ewch ar ap 'X' > chwiliwch am y person yr hoffech ei flocio neu ei dewi a thapiwch ei broffil > tapiwch y tri dot yng nghornel dde uchaf ei broffil > tapiwch naill ai 'Mute @[enwproffil]' neu 'Block @[enwproffil].

**Noder** - i gael y canlyniad gorau, fe'ch cynghorir yn gryf i flocio'r troseddwr.

## Cynulleidfa a thagio

### Amddiffyn eich postiau

Bydd hyn yn sicrhau mai dim ond pobl sy'n eich dilyn chi fydd yn gweld eich postiau. Bydd angen i chi gymeradwyo pob dilynwr newydd:

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > tapiwch 'Privacy and safety' > tapiwch 'Audience and tagging' > sicrhewch fod y togll 'Protect your posts' wedi'i alluogi.

### Tagio ffotograffau

Pan fydd tagio ffotograffau wedi'i ddiffodd, ni fydd pobl yn gallu eich tagio mewn ffotograffau:

Bydd y camau ar gyfer hyn yr un fath â'r rhai ar gyfer 'protect your posts', gydag un cam ychwanegol. Wrth dapio 'Audience and tagging' tapiwch 'photo tagging' > sicrhewch fod y togll wedi'i ddiffodd.

## Negeseua uniongyrchol

Gallwch benderfynu pwy fydd yn gallu anfon negeseuon atoch drwy fynd i'r gosodiadau ar gyfer negeseua uniongyrchol. Os byddwch wedi blocio'r troseddwr, ni fyddwch yn cael dim negeseuon ganddo. Os bydd rhywun yn eich dilyn chi, bydd bob amser yn gallu anfon negeseuon atoch:

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > tapiwch 'Privacy and safety' > tapiwch 'Direct messages' > o dan 'Allow message requests from:' dewiswch 'No one'. Bydd hyn yn golygu na fyddwch yn cael yr un neges gan y troseddwr, hyn yn oed os bydd yn anfon un atoch gan ddefnyddio cyfrif gwahanol/heb ei flocio.

Gallwch hefyd reoli/adolygu pa ddyfeisiau sydd â mynediad at eich negeseuon uniongyrchol –

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > tapiwch 'Privacy and safety' > tapiwch 'Direct messages' > tapiwch 'Manage encrypted devices' > os gwelwch unrhyw ddyfais nad ydych yn ei hadnabod, tapiwch yr eicon 'X' wrth ymyl y ddyfais i'w dileu.

## Darganfyddadwyedd a chysylltiadau

Gallwch reoli eich darganfyddadwyedd a rheoli cysylltiadau drwy ddilyn y camau canlynol:

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > 'Privacy and safety' > tapiwch

'Discoverability and contacts' > sicrhewch fod y togllau yn y gosodiadau hyn i gyd wedi'u hanalluogi.

## Newidiwch eich cyfrinair a rhowch brawf dilysu dau gam ar waith

Mae canllawiau ar sut i greu cyfrineiriau cryf a rhoi prawf dilysu dau gam ar waith i'w gweld ar dudalen 34.

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > 'Your account' > tapiwch 'Change your password'.

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > 'security and account access' > 'Security' > tapiwch 'Two-factor authentication'.

**Noder** - yn 'Your account' gallwch hefyd weld y cyfeiriad e-bost sy'n gysylltiedig â'ch cyfrif drwy dapio 'Account information'.

## Apiau a sesiynau

gallwch weld gwybodaeth ynglŷn â phryd y gwnaethoch fewngofnodi i'ch cyfrif drwy ddilyn y camau canlynol:

Tapiwch eich llun proffil yng nghornel chwith uchaf y dudalen hafan > tapiwch 'settings and privacy' > 'security and account access' > 'Apps and sessions' > yma fe welwch chi 'sessions', 'Account access history' a 'logged-in devices and apps'.



## WhatsApp

Ap negeseua gwib a galwadau fideo.

### Bydd y troseddwr yn defnyddio WhatsApp i wneud y canlynol:

**Aflonyddu arnoch** - er enghraifft, eich peledu'n barhaus â negeseuon difriol drwy gydol y dydd.

**Mewngofnodi i'ch cyfrif** - os bydd gan y troseddwr fynediad i'ch cyfrif, gallai ddarllen eich negeseuon a/neu anfon negeseuon at eich teulu a'ch ffrindiau yn esgus mai chi ydyw.

**Darganfod ble ydych chi** - mae'n bosibl y bydd y troseddwr wedi gosod eich cyfrif i rannu eich lleoliad ag ef.

## Blocio rhywun

Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Privacy' > 'Blocked' > tapiwch 'add new' a theipiwch y rhif yr hoffech ei flocio.

## Rhoi gwybod am y troseddwr

Bydd WhatsApp yn cael y pum neges ddiwethaf a anfonodd y defnyddiwr dan sylw atoch, ac ni fydd y defnyddiwr hwnnw'n cael gwybod.

Agorwch WhatsApp > cliciwch broffil y troseddwr > sgroliwch i lawr a thapiwch 'Report [enw]'.

## Dyfeisiau cysylltiedig

Gallwch gysylltu dyfeisiau eraill â'ch cyfrif, gan gynnwys Windows, Mac a'r we.

Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Linked devices' > os bydd unrhyw ddyfeisiau wedi'u cysylltu â'ch cyfrif, byddant i'w gweld. Os bydd unrhyw rai nad ydych yn eu hadnabod > tapiwch y ddyfais > 'Log out'.

## Gosodiadau preifatrwydd

### Llun proffil

gallwch ddewis pwy fydd yn cael gweld eich llun proffil.

Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Privacy' > 'Profile photo' > dewiswch ba osodiad yr hoffech ei ffurfweddu drwy ei dapio.

### Grwpiau

Gallwch ddewis pwy fydd yn gallu eich ychwanegu chi at grwpiau. Yn hytrach na thapio 'Profile photo', tapiwch 'Groups'. Dewiswch rhwng y gwahanol osodiadau a gyflwynir drwy dapio arnynt.

### Lleoliad byw

Gallwch edrych i weld ym mha sgysiau rydych chi'n rhannu eich lleoliad

Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Privacy' > 'Live location' > os ydych chi'n rhannu eich lleoliad â rhywun arall, analluogwch hynny.

### Cloi sgysiau

Os hoffech guddio unrhyw sgysiau

Tapiwch lun proffil yr unigolyn > sgroliwch i lawr nes y dewch o hyd i 'Lock chat', tapiwch ar y togli i'w droi ymlaen. Gallwch ddatgloi'r sgysiau hyn gan ddefnyddio cod mynediad eich ffôn, Face ID, ôl bys neu god cyfrinachol.

### Prawf dilysu dau gam

Gallwch roi prawf dilysu dau gam ar waith er mwyn ychwanegu haen arall o ddiogelwch.

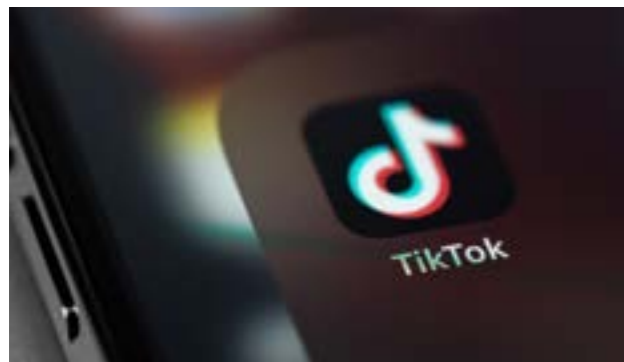
Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Account' ac yna 'Two-step authentication'.

### Diogelu cyfeiriad IP yn ystod galwadau

Er mwyn ei gwneud hi'n anoddach i rywun ganfod eich lleoliad, caiff galwadau ar eich dyfais eu trosglwyddo'n ddiogel drwy weinyddion WhatsApp

Agorwch WhatsApp > ewch i 'Settings' > tapiwch 'Privacy' > sgroliwch i lawr a thapiwch 'Advanced' > galluogwch y togli ar gyfer 'Protect IP address in calls'.

**Noder** - Nid oes ffordd o guddio eich rhif ffôn wrth ddefnyddio WhatsApp.



## TikTok

Llwyfan a gaiff ei ddefnyddio ar gyfer creu a rhannu fideos byr.

### Bydd y troseddwr yn defnyddio TikTok i wneud y canlynol:

**Aflonyddu arnoch** - er enghraifft, eich peledu'n barhaus â negeseuon difrifol drwy gydol y dydd.

**Mewngofnodi i'ch cyfrif** - os bydd gan y troseddwr fynediad i'ch cyfrif, gallai bostio cynnwys amhriodol ar eich proffil. Gallai hefyd ddarllen eich negeseuon a/ neu anfon negeseuon at eich teulu a'ch ffrindiau yn esgus mai chi ydyw.

**Edrych i weld pa gynnwys y byddwch yn ei bostio** - fer enghraifft, gallai edrych ar eich postiau er mwyn gweld â phwy y byddwch yn treulio amser (ffotograffau ohonoch chi gyda theulu neu ffrindiau).

**Ceisio gweld ble ydych chi** - os byddwch wedi symud i ffwrdd oddi wrth y troseddwr, gall edrych ar eich proffil i weld a yw'r cynnwys yn dangos ble ydych chi (er enghraifft, ym mha dref).

### Blocio rhywun

Chwiliwch am broffil y defnyddiwr > tapiwch y tri dot yn y gornel dde uchaf > tapiwch 'Block'.

### Gwnewch eich proffil yn breifat

Bydd hyn yn golygu mai dim ond pobl sy'n eich dilyn chi fydd yn gallu gwyllo eich fideos, eich fideos byw, eich manylion a'r pethau y byddwch yn eu hoffi.

Tapiwch yr eicon proffil yn y gornel dde isaf > agorwch y ddewislen yn y gornel dde uchaf > Settings and privacy > Private account.

### Gallwch atal TikTok rhag awgrymu eich cyfrif

Ewch i'ch proffil > Agorwch y ddewislen yn y gornel dde uchaf > Settings and privacy > Suggest your account to others > diffoddwch y toglau o'ch dewis.

### Diffoddwch y gwasanaethau lleoliad

Tapiwch yr eicon proffil yn y gornel dde isaf > agorwch y ddewislen yn y gornel dde uchaf > Settings and privacy > Privacy > tapiwch Location services > diffoddwch y caniatâd lleoliad.

### Negeseua uniongyrchol

Er mwyn newid pwy sy'n gallu anfon negeseuon uniongyrchol atoch

Ewch i'ch proffil > Agorwch y ddewislen yn y gornel dde uchaf > Settings and privacy > Privacy > tapiwch Direct messages > o blith yr opsiynau, dewiswch 'friends'. Bydd unrhyw ddilynwyr rydych chi'n eu dilyn hefyd yn gallu anfon neges uniongyrchol atoch.

### Crëwch gyfrinair cryf ac unigryw

Tapiwch 'Profile' ar y gwaelod > tapiwch y botwm 'Menu' ar y brig > 'Settings and privacy' > tapiwch 'Account' ac yna tapiwch 'Password'.

### Galluogwch brawf dilysu dau gam

Tapiwch yr eicon proffil yn y gornel dde isaf > agorwch y ddewislen yn y gornel dde uchaf > Settings and privacy > tapiwch Security > tapiwch '2-step verification' a dewiswch o leiaf ddau ddull dilysu.





## Snapchat

Ap sy'n eich galluogi i anfon lluniau neu fideos a elwir yn "snaps" sy'n diflannu ar ôl iddynt gael eu gweld; mae nodwedd sgwrsio ar gael hefyd.

### Bydd y troseddwr yn defnyddio TikTok i wneud y canlynol:

**Aflonyddu arnoch** - er enghraifft, eich peledu'n barhaus â negeseuon difriol drwy gydol y dydd.

**Mewngofnodi i'ch cyfrif** - os bydd gan y troseddwr fynediad i'ch cyfrif, gallai bostio cynnwys amhriodol ar eich proffil. Gallai hefyd ddarllen eich negeseuon a/ neu anfon negeseuon at eich teulu a'ch ffrindiau yn esgus mai chi ydyw.

**Edrych i weld pa gynnwys y byddwch yn ei bostio** - fer enghraifft, gallai edrych ar eich postiau er mwyn gweld â phwy y byddwch yn treulio amser (ffotograffau ohonoch chi gyda theulu neu ffrindiau).

**Ceisio gweld ble ydych chi** - os byddwch wedi symud i ffwrdd oddi wrth y troseddwr, gall edrych ar eich proffil i weld a yw'r cynnwys yn dangos ble ydych chi (er enghraifft, ym mha dref).

### Blocio rhywun

Cliciwch eich rhithffurf yn y gornel chwith uchaf > sgroliwch i lawr eich rhestr ffrindiau a chwiliwch am y person yr hoffech ei flocio > daliwch eich bys i lawr ar ei enw > tapiwch 'Manage friendship' a dewiswch 'Block'.

### Sicrhewch mai dim ond teulu a ffrindiau sydd gennych ar eich Snapchat

Cliciwch eich rhithffurf yn y gornel chwith uchaf > sgroliwch i lawr eich rhestr ffrindiau ac edrychwch i weld a oes unrhyw un yno nad ydych yn ei adnabod neu'n agos ato > i gael gwared ar rywun, daliwch eich bys i lawr ar ei enw > tapiwch 'Manage friendship' a dewiswch 'Remove Friend'.

### Galluogwch 'Ghost Mode'

Er mwyn diogelu eich lleoliad, sicrhewch fod y nodwedd mapiau wedi'i diffodd.

Cliciwch yr eicon map yn y gornel chwith isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > sicrhewch fod y togl ar gyfer 'Ghost Mode' wedi'i alluogi.

### Er mwyn caniatáu i grŵp penodol o ffrindiau yn unig weld eich straeon

Cliciwch eich rhithffurf yn y gornel chwith uchaf > o dan 'My Stories' cliciwch ar y tri dot wrth ymyl 'Add to my Story'. Tapiwch 'Story Settings' > tapiwch 'Friends Only' neu gallwch ddewis pa ffrindiau yr hoffech iddynt weld eich stori drwy dapio 'Custom'.

### Sicrhewch fod eich cyfrinair yn gryf ac yn unigryw

Cliciwch yr eicon map yn y gornel chwith isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > tapiwch 'Password' a newidiwch eich cyfrinair.

### Galluogwch brawf dilysu dau gam

Cliciwch yr eicon map yn y gornel chwith isaf > tapiwch yr eicon gosodiadau yn y gornel dde uchaf > tapiwch 'Two-Factor authentication' a thapiwch 'Continue'.





## Ffugenwau

Bydd pobl yn eu defnyddio i guddio pwy ydyn nhw.

Mewn rhai achosion, pan fydd y troseddwr yn gwybod enwau eich proffiliau cyfryngau cymdeithasol, bydd yn eich peledu'n barhaus â cheisiadau ffrind a cheisiadau negeseuon. Hyd yn oed pan fyddwch yn blocio un cyfrif, bydd yn creu un arall yn ei le. Gall hyn fynd yn flinderus pan fydd yn rhaid i chi flocio cyfrifon diddiwedd a rhoi gwybod amdanynt.

Bydd troseddwr yn ceisio cysylltu â chi ar unrhyw fath o gyfrif ar-lein os bydd modd. Gallai hyn gynnwys dod o hyd i'ch proffil ar lwyfannau chwarae gemau neu ar apiau caru.

Os bydd hyn yn digwydd i chi, dylech ystyried defnyddio ffugenwau ar gyfer eich cyfrifon ar-lein. Bydd defnyddio ffugenw yn ei gwneud hi'n llawer anoddach i'r troseddwr ddod o hyd i chi ar-lein (os o gwbl), a byddwch yn gallu defnyddio eich cyfrifon heb gael eich boddi gan negeseuon a cheisiadau ffrind ffug.

Hefyd, os byddwch yn defnyddio ffugenw, ni ddylai eich llun proffil fod yn llun ohonoch chi, nac yn llun o unrhyw beth a allai ddangos i'r troseddwr mai chi ydyw.

Dim ond teulu a ffrindiau rydych chi'n ymddiried ynddynt a ddylai wybod am y cyfrifon hyn. Po fwyaf o bobl y byddwch yn caniatáu iddynt ddilyn eich cyfrif, mwyaf fydd y tebygolrwydd y gall y troseddwr ddod i wybod amdano.



## Doccio

Cyhoeddi gwybodaeth bersonol adnabyddadwy am unigolyn ar y rhyngwrwyd heb ei ganiatâd.

Bydd troseddwr yn casglu cymaint â phosibl o wybodaeth bersonol a phreifat amdano chi. Bydd yn gallu casglu'r wybodaeth hon o'r rhyngwrwyd, gan drydydd partion (e.e. ffrindiau cyffredin) ac, os na fyddwch wedi blocio'r troseddwr, bydd hefyd yn gallu cael gwybodaeth o'ch cyfrifon cyfryngau cymdeithasol.

Gellir defnyddio'r wybodaeth hon i lunio proffil ohonoch y bydd y troseddwr yn ei bostio ar-lein at ddiben aflonyddu arnoch, eich bygwth neu eich niweidio (e.e. postio ble rydych chi'n byw neu gofnodion meddygol preifat). Mae Facebook, Twitter, ac Instagram yn llwyfannau cyfryngau cymdeithasol poblogaidd y gall y troseddwr eu defnyddio i bostio gwybodaeth amdano.

Mewn achosion lle bydd y troseddwr yn eich doccio, mae Google yn cynnig nodwedd lle y gall unigolyn wneud cais i ddileu gwybodaeth bersonol adnabyddadwy benodol o ganlyniadau chwilio Google. Er enghraifft:

- Cyfeiriad, rhif ffôn, cyfeiriad e-bost
- Rhifau adnabod cyfrinachol (nawdd cymdeithasol, rhif treth ac ati)
- Rhif cyfrif banc/cerdyn credyd
- Cofnodion hynod bersonol, gyfyngedig a swyddogol (e.e. cofnodion meddygol)

Mae Google hefyd yn cynnig y gallu i unigolyn greu rhybuddion 'Google Alert'. Gallwch gael negeseuon e-bost pan fydd canlyniadau newydd am bwnc yn ymddangos yng nghanlyniadau chwilio Google, gan gynnwys gwybodaeth am achosion pan sonnir am eich enw. Gellir gwneud hyn drwy ddilyn y camau canlyno.

Ewch i Google Alerts > teipiwch yr enw yr hoffech ei ddilyn/chwilio amdano > cliciwch 'Show options' > newidiwch y gosodiadau yn unol â'ch dewis (e.e. pa mor aml y byddwch yn cael hysbysiadau, faint o ganlyniadau yr hoffech eu gweld ac ati).

Os cewch rybudd bod gwybodaeth bersonol amdano yn cael ei phostio ar-lein, gallwch wneud cais i ddileu cynnwys (gan ddilyn y canllawiau uchod).

Hefyd, os bydd y troseddwr wedi bod yn postio gwybodaeth bersonol ar y cyfryngau cymdeithasol, dylech chi neu drydydd parti (mewn achosion lle y bydd y troseddwr wedi'i flocio) roi gwybod am y postiad/cyfrif drwy'r llwyfan.



## Cyfrifon dynwared/ffug

Proffil sy'n cynrychioli person, endid neu sefydliad drwy dwyll yw cyfrif dynwared ar y cyfryngau cymdeithasol.

Mae'n bosibl y bydd y troseddwr yn creu cyfrifon cyfryngau cymdeithasol ffug ar eich cyfer ac yn honni mai cyfrifon 'newydd' ydyn nhw. Gall troseddwr greu cyfrifon ffug am nifer o resymau, ac ymhlith y rhai mwyaf cyffredin mae:

**Niwed i enw da** - efallai y bydd troseddwr yn eich dynwared chi er mwyn lledaenu gwybodaeth anwir amdanoch, a allai niweidio eich enw da a pheri gofid i chi.

**Twyllo trydydd partion** - gallai troseddwr dwyllo eich teulu a'ch ffrindiau i gysylltu â'r cyfrif dynwared. Efallai y bydd hyn er mwyn cael gwybodaeth amdanoch, neu greu gwrthdaro rhyngoch chi a thrydydd partion.

**Noder** - gallai troseddwr hefyd greu cyfrifon ffug ar gyfer trydydd partion i'ch cyrraedd chi.

Er mwyn lliniaru'r risg sy'n gysylltiedig â chyfrifon dynwared posibl a chyfyngu ar eu llwyddiant, mae'n bwysig deall un o'r technegau hanfodol y bydd troseddwr yn eu defnyddio:

- **Peirianeg gymdeithasol** - ystyr hyn yw dylanwadu ar unigolion er mwyn iddynt ddatgelu gwybodaeth sensitif neu gyflawni gweithredoedd a fydd yn peryglu diogelwch y goroeswr. Bydd troseddwr yn dylanwadu ar emosiynau drwy greu ymdeimlad o frys, ofn, neu gydymdeimlad. Mewn achosion lle roeddech chi a'r troseddwr yn arfer bod mewn perthynas, bydd hyn yn peri risg arbennig. Y rheswm dros hyn yw y bydd y troseddwr yn gwybod pethau personol amdanoch, a fydd yn ei gwneud hi'n hawdd iddo eich dynwared chi.

Oherwydd hyn, mae'n bwysig eich bod chi a thrydydd partion yn gallu adnabod cyfrifon ffug, ac mae'r arwyddion y dylid bod yn ymwybodol ohonynt fel a ganlyn:

- **Dim llawer o ddilynwyr nac ymgysylltu** - yn aml, bydd gan broffiliau ffug nifer bach o ddilynwyr, ac ni fydd llawer o ymgysylltu â'u postadau. Dylid hefyd ystyried pa gyfrifon y mae'r proffil yn eu dilyn, er enghraifft dim ond eich teulu a'ch ffrindiau.
- **Gwybodaeth a lluniau proffil** - chwiliwch am anghysondebau yn y proffil. Os byddwch wedi blocio'r troseddwr ers peth amser, bydd y lluniau a'r wybodaeth a ddefnyddir ar y proffil ffug wedi dyddio.

- **Gweithgarwch a rhyngweithio** - bydd cyfrif cyfryngau cymdeithasol gwirioneddol/go iawn fel arfer yn ferw o rhyngweithio felly, os bydd y proffil yn ymddangos yn ddisymud, bydd hynny fel arfer yn arwydd mai cyfrif ffug ydyw.
- **Postiadau amheus** - mae'n bosibl y bydd y troseddwr yn rhannu cynnwys sy'n ymddangos yn groes i gymeriad y person y mae'n ei ddynwared.
- **Cyfathrebu anarferol** - mae'n bwysig bod yn wylidwrus o negeseuon na ofynnwyd amdanynt. Bydd hyn yn arbennig o bwysig os bydd y cyfrif yn gofyn am wybodaeth neu arian, neu'n ceisio eich cyfeirio at ddolenni amheus.
- **Iaith ac arddull cyfathrebu** - mae'n bwysig ystyried sut mae'r cyfrif yn cyfathrebu â chi. A yw'r cyfrif yn anfon negeseuon sydd â'r un arddull â'r person go iawn, neu a yw'r arddull yn wahanol? A yw'n siarad â chi mewn ffordd anarferol neu mewn ffordd a allai gael ei hystyried yn groes i gymeriad y person go iawn?
- **A yw'r 'hen' gyfrif cyfryngau cymdeithasol yn dal yn weithredol?** - Os mai cyfrif ffug ydyw, bydd y person go iawn yn dal i ddefnyddio ei gyfrif gwreiddiol/go iawn.

Mae'n bosibl y bydd y troseddwr yn creu cyfrif sy'n eich dynwared chi, aelod o'ch teulu, neu ffrind.

Os byddwch chi neu unrhyw drydydd partion yn ansicr ai cyfrif go iawn neu gyfrif ffug ydyw, yna -

- Holwch am y cyfrif ar lwyfan cyfathrebu lle rydych chi'n gwybod ei fod yn ddiogel a'ch bod yn siarad â'r person go iawn. Gallai hyn fod drwy neges destun neu, er mwyn bod yn sicr, dylech ffonio'r unigolyn neu ei holi wyneb yn wyneb.

**Noder** - Dylech hefyd fod yn ofalus os byddwch yn credu bod cyfrif sy'n cyfathrebu â chi yn un ffug. Hefyd, dylech fod yn ofalus ynglŷn â pha wybodaeth y byddwch yn ei rhannu ar lwyfannau cyfryngau cymdeithasol a bod yn wylidwrus o unrhyw ddolenni amheus y bydd cyfrif a amheuir yn eu rhannu â chi.

Os byddwch yn gwybod bod cyfrif yn un ffug, mae'n bwysig cymryd y camau cywir cyn gynted â phosibl:

- **Casglwch dystiolaeth** - dylech chi a thrydydd partion dynnu sgrinluniau/casglu gwybodaeth berthnasol sy'n profi bodolaeth y proffil ffug. Mae hyn yn cynnwys postadau, negeseuon, a rhyngweithiadau.
- **Rhowch wybod am y dynwaredwr** - dylech chi a thrydydd partion roi gwybod i'r llwyfan cyfryngau cymdeithasol am y cyfrif gan ddefnyddio'r dulliau rhoi gwybod berthnasol (gan gynnwys y dystiolaeth y gwnaethoch ei chasglu).
- **Rhowch wybod i'ch rhwydwaith** - dylech roi gwybod i drydydd partion am y cyfrif dynwared. Bydd hyn er mwyn eu hatal rhag cyfathrebu â'r cyfrif ffug a rhannu gwybodaeth ag ef o bosibl. Dylid gwneud hyn drwy bostiad cyhoeddus ar y llwyfan neu negeseuon preifat, neu wyneb yn wyneb.
- **Daliwch ati i fonitro'r sefyllfa** - dylech chi a thrydydd partion barhau i fod yn wylidwrus am gyfrifon dynwared newydd a rhoi gwybod i'r llwyfan yn brydlon am unrhyw weithgarwch.
- **Adolygwch a diweddarwch eich mesurau diogelwch** - dylech sicrhau bod eich nodweddion diogelwch yn gyfredol ar eich cyfrifon cyfryngau cymdeithasol (rhoddir canllawiau ar dudalennau blaenorol).



## Rhan Dau: Canllawiau ar gyfer Ffonau Symudol (Apple ac Android)



## Negeseuon e-bost

System ar gyfer anfon a derbyn negeseuon drwy ddyfeisiau digidol dros rwydwaith.

Gallai'r troseddwr ysgrifennu negeseuon casineb a bygythiadau a'u hanfon drwy gyfrif dros dro (a grëwyd ganddo er mwyn peidio â datgelu ei brif gyfeiriad e-bost) neu wasanaeth sy'n anfon negeseuon yn ddienw. Mae hefyd yn bwysig nodi y gellir anfon maleiswedd mewn neges e-bost drwy atodi dolen faleisus. Mae'n bosibl mai ysbïwedd fydd y faleiswedd hon.

Os bydd negeseuon casineb neu fygythiadau'n cael eu hanfon atoch drwy e-bost -

- Dylech greu ffolder newydd yn eich cyfrif e-bost ar gyfer yr holl negeseuon sarhaus/aflonyddol. Bydd hyn yn golygu y bydd gennych dystiolaeth os bydd angen yn y dyfodol.
- Blociwch y cyfeiriad e-bost.
- Rhowch wybod i ddarparwr y gwasanaeth e-bost am y negeseuon.
- Mewn rhai achosion, gall y troseddwr gael gafael ar eich cyfeiriad e-bost gwaith, hyd yn oed. Os bydd hynny'n digwydd, dylid rhoi gwybod i'ch cyflogwr am yr amgylchiadau.
- Dylech ystyried defnyddio gwahanol gyfeiriadau e-bost at wahanol ddibenion.
- Crëwch hidlydd; hynny yw, cyfres o reolau sy'n dweud wrth eich gwasanaeth e-bost sut i ymdrin â negeseuon penodol. Gall hidlydd ddileu negeseuon e-bost gan anfonwr penodol yn awtomatig, neu symud pob neges sy'n cynnwys allweddeiriau penodol i ffolder arbennig.
- Gofynnwch i drydydd partïon flocio cyfeiriad e-bost y troseddwr os bydd hynny'n berthnasol.

**Note** - mae'n hollbwysig eich bod yn newid cyfrinair eich cyfrif e-bost. Hwn fydd y cyfrif pwysicaf i chi ei gadw'n ddiogel, fwy na thebyg. Mae ein holl gyfrifon yn gysylltiedig â'n cyfrif e-bost ac, os byddwn yn anghofio ein cyfrinair ar gyfer cyfrif, gallwn ei ailosod drwy anfon camau adfer cyfrinair i'n cyfrif e-bost. Os gall y troseddwr gael mynediad at eich negeseuon e-bost, bydd hynny'n agor y drws iddo allu cael mynediad i'ch holl gyfrifon eraill hefyd, a'ch cloi allan ohonynt drwy newid y cyfrinairiau o bosibl. Yn ogystal â hynny, bydd gwybodaeth gyfrinachol a phersonol i'w gweld yn ein cyfrifon e-bost hefyd.



## Rhif Ffôn Symudol a Negeseuon Llais

**Rhif Ffôn Symudol** - Cyfres o ffigurau sy'n dynodi tanysgrifiwr ffôn symudol, a ddefnyddir i wneud galwadau ac anfon negeseuon testun.

**Negeseuon Llais** - Cyfleuster sy'n galluogi pobl i recordio neges pan na fydd derbynnydd yr alwad yn gallu ateb y ffôn.

Gall troseddwr ddefnyddio eich ffôn symudol i'ch peledu â negeseuon drwy gydol y dydd a bydd y negeseuon hyn yn aml, ond nid bob amser, yn fygythiol ac yn ddirfriadol. Gallant hefyd geisio eich ffonio drwy gydol y dydd ac, os na fyddant yn cael ateb, byddant yn gadael negeseuon llais.

**Note** - Cyfarchiad negeseuon llais diofyn y dylech ei ddefnyddio, yn hytrach na'ch llais eich hun. Pe bai'r troseddwr yn ansicr ai eich rhif chi ydyw, yn ei ffonio, ac yn cyrraedd y cyfleuster negeseuon llais, ni fyddai'r cyfarchiad diofyn yn datgelu mai eich rhif chi ydyw.

Dylech flocio rhif ffôn y troseddwr ar eich ffôn symudol:

**iPhone** - 'Settings' > sgroliwch i lawr a thapiwch 'Phone' > sgroliwch i lawr a thapiwch 'Blocked contacts' > tapiwch 'Add New...'

- Os oes gennych iPhone a MacBook, bydd angen i chi flocio'r troseddwr ar y ddwy ddyfais. (Mae IOS a MacOS yn ddwy system wahanol)

**Android** - agorwch 'Messages' > tapiwch yr eicon 'More' yn y gornel dde uchaf > Settings > tapiwch 'Block numbers and spam' > tapiwch 'Block numbers.'

Os oes gennych blant gyda'ch gilydd a bod angen pwynt cyswllt, gallech ystyried defnyddio trydydd parti rydych yn ymddiried ynddo.

Os bydd y troseddwr yn defnyddio rhif arall neu fwy nag un rhif ar ôl i'w brif rif gael ei flocio, yna gallwch flocio'r rhif nad yw wedi'i gadw. Gallwch wneud hyn drwy ddilyn yr un camau â'r rhai a restrir uchod a theipio'r rhif eich hun yn hytrach na defnyddio enw'r person.

Gofynnwch i drydydd partïon flocio rhif ffôn y troseddwr os bydd modd.

Pan fyddwch yn blocio rhif ffôn symudol o'ch ffôn, bydd y troseddwr yn dal i allu gadael negeseuon llais.

- Mae apiau ar gael sy'n eich galluogi nid yn unig i flocio galwadau dieisiau, ond eu negeseuon llais hefyd. Un ap y gellir ei lawrlwytho o Google Play Store ac Apple Store yw Call Control. Partneriaid integredig yr ap yw Nextiva, Cisco a BroadSoft.



## Cyfrifon Apple ID ac iCloud

Cyfrif defnyddiwr gan Apple ar gyfer dyfeisiau a meddalwedd y cwmni yw Apple ID, ac mae'n cynnwys data personol a gosodiadau'r defnyddiwr.

Gwasanaeth gan Apple sy'n storio eich data'n ddiogel yn y cwmwl ac sy'n eu cadw'n gyfredol ar eich holl ddyfeisiau yn awtomatig yw iCloud.

Mewn achosion lle roeddech chi a'r troseddwr yn arfer bod mewn perthynas, mae'n bosibl y bydd y troseddwr wedi creu cyfrif Apple ID/iCloud ar eich cyfer ac yn gallu cael mynediad ato hefyd. Gallai'r troseddwr hyd yn oed ffurfweddu eich cyfrif Apple ID/iCloud mewn ffordd sy'n ei alluogi i gael mynediad heb yn wybod i chi.

Os bydd gan droseddwr fynediad at eich cyfrif Apple ID/iCloud, neu os bydd yn rhannu'r un cyfrif â chi, bydd yn gallu gweld yr hyn y byddwch yn ei lawrlwytho a'i brynu a'ch negeseuon, eich ffotograffau, eich fideos a'ch cysylltiadau. Bydd logiau galwadau hefyd yn cael eu rhannu rhwng y ddau ffôn. Bydd y troseddwr hefyd yn gallu gweld eich lleoliad.

**Settings > Tapiwch yr enw > Sgrolwch i lawr ac edrychwch i weld pa ddyfeisiau sy'n gysylltiedig â'r cyfrif** - Dylid cael gwared ar unrhyw ddyfeisiau nad yw'r defnyddiwr yn eu hadnabod.

**Sign-in & Security > Email & Phone numbers** - Gellir defnyddio'r cyfeiriadau e-bost a rhifau ffôn a restrir i fewngofnodi. Edrychwch i weld a oes unrhyw gyfeiriadau e-bost neu rifau ffôn nad ydych yn eu hadnabod wedi'u cysylltu ac, os felly, dilëwch nhw.

**Family sharing > edrychwch i weld a yw hyn wedi cael ei osod** - Os felly, edrychwch i weld pa ddefnyddwyr sydd wedi'u rhestru a dilëwch unrhyw rai nad ydych yn eu hadnabod.

**Settings > Messages > Send and Receive** - Edrychwch i weld pa gyfeiriadau e-bost a rhifau ffôn sy'n gallu anfon a derbyn negeseuon.

**Safety Check > edrychwch dros yr holl wybodaeth bersonol a gwybodaeth ddiogelwch yn eich cyfrif er mwyn gweld a oes unrhyw wybodaeth y mae rhywun arall wedi'i hychwanegu.**

- Gallech hefyd analluogi iCloud Sync ar eich dyfais, sy'n golygu na fydd data o'ch dyfais yn cael eu storio ar-lein mwyach ac na fydd modd i neb a all fod â mynediad i'r cyfrif iCloud gael gafael arnynt.
- Gallech hefyd alluogi diogelwch data uwch ar gyfer iCloud, sef y lefel uchaf o ddiogelwch data lle y cânt eu diogelu drwy amgryptio o un pen i'r llall.

Gall mewngofnodi i wefan Apple ID alluogi defnyddiwr i fwrw golwg dros yr holl wybodaeth bersonol a gwybodaeth ddiogelwch yn ei gyfrif er mwyn gweld a oes unrhyw wybodaeth y mae rhywun arall wedi'i hychwanegu.

Fe'ch cyngorir yn gryf i roi prawf dilysu dau gam ar waith ar gyfer Apple ID – hyd yn oed os bydd rhywun yn gwybod y cyfrinair, ni fydd yn gallu cael mynediad i'r cyfrif heb y PIN.



## Cyfrifon Android

Cafodd system weithredu Android ei datblygu gan Google. Er mwyn cael mynediad at e-bost, cysylltiadau a'r calendr, a chael apiau o'r Google Play Store, rhaid creu cyfrif Google, a bydd gwybodaeth sy'n gysylltiedig â'r cyfrif hwnnw'n cysoni â'r ffôn.

Mewn achosion lle roeddech chi a'r troseddwr yn arfer bod mewn perthynas, mae'n bosibl y bydd y troseddwr wedi creu cyfrif Google ar eich cyfer ac yn gallu cael mynediad ato hefyd. Gallai'r troseddwr hyd yn oed ffurfweddu eich cyfrif Google mewn ffordd sy'n ei alluogi i gael mynediad heb yn wybod i chi.

Os bydd gan droseddwr fynediad at eich cyfrif Google, neu os bydd yn rhannu'r un cyfrif â chi, bydd yn gallu gweld eich negeseuon, eich ffotograffau, eich fideos a'ch cysylltiadau. Bydd logiau galwadau hefyd yn cael eu rhannu rhwng y ddau ffôn. Bydd y troseddwr hefyd yn gallu gweld eich lleoliad.

Mae ffonau Android yn defnyddio cyfrif Google. Os oes gennych gyfrif Android, mae sawl ffordd y gallwch edrych i weld a oes gan ddyfais arall fynediad i'ch cyfrif.

- **Google account > security > your devices > manage all devices.** Bydd hyn yn eich galluogi i weld pa ddyfeisiau sydd wedi'u mewngofnodi i'ch cyfrif Google, neu a oedd wedi'u mewngofnodi'n ddiweddar. Gallwch edrych i weld pa fath o wybodaeth y mae gan y ddyfais/sesiwn honno fynediad ati drwy'r cyfrif Google.
- **Ap Google Messages** - gall troseddwr gysylltu un o'i ddyfeisiau â'ch ap negeseua a thrwy negeseua cwmwl.
- **Google family link** - edrychwch i weld a yw Google Family Link wedi'i osod ar eich ffôn. (Gall defnyddwyr Apple ddefnyddio hwn hefyd)
- Gallwch edrych i weld a yw eich ffôn wedi cael ei ffurfweddu i guddio apiau. **Settings > Display > Home screen > Hide apps.**
- **Life360** - dyma ap arall y gellir ei ddefnyddio i'ch tracio a'ch monitro, yn enwedig mewn achosion lle y byddwch wedi gadael perthynas orfodaethol o bosibl.

Newidiwch gyfrinair y cyfrif Google – dylech sicrhau na all y troseddwr gael mynediad i'ch cyfrif Google (efallai y bydd hyn yn bosibl/yn debygol os oeddech chi a'r troseddwr mewn perthynas â'ch gilydd o'r blaen).

**Newidiwch gyfrinair eich cyfrif Google;** bydd hyn yn atal mynediad o bell. I newid cyfrinair cyfrif Google:

- Settings > Google > Manage your Google Account > ar y brig, tapiwch Security > 'How you sign in to Google' > tapiwch Password (efallai y bydd angen i chi fewngofnodi) > Teipiwch eich cyfrinair newydd > tapiwch Change Password.



## Sut i greu cyfrineiriau cryf a rhoi prawf dilysu dau gam ar waith

Gan y Ganolfan Seiberddiogelwch Genedlaethol (NCSC)

Os bydd y troseddwr yn gwybod eich cyfrineiriau ar gyfer eich cyfrifon, ac os nad yw prawf dilysu dau gam wedi'i alluogi gennych, bydd hyn yn peri risg y bydd yn gallu cael mynediad i'ch cyfrifon unrhyw bryd. Fel y soniwyd yn flaenorol, gall troseddwr gael mynediad i'ch cyfrifon er mwyn cael gwybodaeth am eich gweithgareddau ar-lein yn ogystal â gwybodaeth breifat. Bydd y troseddwr yn gallu defnyddio'r wybodaeth hon yn eich erbyn a hyd yn oed ddefnyddio cyfrifon penodol i achosi niwed, er enghraifft, cael mynediad i'ch cyfrif e-bost ac ysgrifennu neges e-bost niweidiol at eich cyflogwr.

### Tri gair ar hap

Mae'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC) yn annog pobl i ddefnyddio tri gair ar hap fel techneg ar gyfer greu cyfrineiriau.

Yn ôl NCSC (2024):



**“Longstanding advice around making your passwords very complex (which suggests we should create passwords full of random characters, symbols, and numbers) is not helpful. This is because most of us have lots of passwords, and memorising lots of complex passwords is almost impossible.”**

Bydd dewis tri gair ar hap yn golygu y bydd yn anodd iawn i droseddwr ddyfalu eich cyfrinair ac yn cymryd llawer iawn o amser i gyfrifiadur ei ddatrys. Hefyd, gall fod yn llawer haws ei gofio.

### Rheolwr cyfrineiriau

Mae gorfod greu gwahanol gyfrineiriau ar gyfer yr holl gyfrifon sydd gennym yn golygu ei bod yn rhaid i ni gofio'r holl wahanol gyfrineiriau hynny, a gall rheolwr cyfrineiriau helpu gyda hyn. Math o ap sy'n storio eich cyfrineiriau yw rheolwr cyfrineiriau, felly ni fydd angen i chi eu cofio. Gall llawer o reolwyr cyfrineiriau hefyd roi eich cyfrineiriau i mewn ar wefannau ac apiau'n awtomatig (fel na fydd yn rhaid i chi eu teipio bob tro y byddwch yn mewngofnodi).

Mae llawer o wahanol apiau rheolwr cyfrineiriau ar gael, felly dylech ymchwilio i'r apiau cyn dewis un i'w ddefnyddio.

Noder – bydd rhai rheolwr cyfrineiriau hyd yn oed yn greu cyfrineiriau cryf ar eich rhan.



### Prawf dilysu dau gam

Nodweddd ddiogelwch hollbwysig y dylai pawb ei rhoi ar waith (yn enwedig ar gyfer cyfrifon e-bost) yw prawf dilysu dau gam. Hyd yn oed os bydd y troseddwr neu unigolyn arall yn gwybod eich cyfrineiriau, ni fydd yn gallu cael mynediad i'ch cyfrifon os bydd prawf dilysu dau gam wedi'i alluogi.

Bydd hyn yn gweithio drwy anfon PIN neu god (yn aml drwy neges destun neu e-bost) y bydd angen i chi ei deipio cyn gallu cael mynediad i'r cyfrif.

Os bydd prawf dilysu dau gam ar gael ar gyfer cyfrif, bydd yr opsiwn i'w alluogi fel arfer i'w weld yng ngosodiadau diogelwch y cyfrif.

Yn debyg i reolwr cyfrineiriau, mae apiau trydydd parti ar gael i'w lawrlwytho a fydd yn cynnig dull dilysu i'r defnyddiwr. Unwaith eto, dylid ymchwilio i'r apiau sydd ar gael cyn dewis un i'w ddefnyddio.



## ‘Find My’ a nodweddion eraill sy’n dangos lleoliad (Apple)

Gellir defnyddio ‘Find My’ ar iPhone i weld lleoliad dyfais ar fap. Os bydd y ddyfais ar-lein, byddwch yn gweld ei lleoliad a bydd yn chwarae sain er mwyn eich helpu i ddod o hyd iddi. Os bydd y ddyfais all-lein, byddwch yn gweld ei lleoliad, ond ni fydd yn chwarae sain.

Os bydd troseddwr yn gallu cysylltu â'ch nodwedd ‘Find My’ neu unrhyw nodwedd arall sy’n dangos lleoliad, bydd yn gwybod ble yn union ydych chi. Gall hyn fod yn annogel, oherwydd gallai fynd i'r un lle â chi, creu helynt, neu hyd yn oed eich bygwth/ceisio eich niweidio.

**Find my iPhone/friend** - mae'r nodwedd hon yn boblogaidd ymhlith teulu a ffrindiau sydd ag iPhones. Mae'n galluogi person i rannu ei lleoliad â rhywun am awr, tan ddiwedd y dydd, neu am gyfnod amhenodol.

Dylech edrych i weld â phwy rydych chi'n rhannu eich lleoliad ar yr ap hwn. Os bydd unrhyw ddyfeisiau anghyfarwydd yn gallu gweld eich lleoliad, dylid eu dileu. I wneud hyn –

- Find My > People > dyma restr o bobl sy'n rhannu eu lleoliad nhw â chi, rydych chi'n rhannu eich lleoliad chi â nhw, neu'r ddau. I edrych i weld a ydych yn rhannu eich lleoliad â'r person hwnnw, tapiwch ei enw > sgroliwch i lawr – byddwch yn gweld naill ai ‘Share my location’ neu ‘Stop sharing my location’. Os byddwch yn rhannu eich lleoliad â dyfais ddieisiau, tapiwch ‘Stop sharing my location’.

Sicrhewch nad oes trydydd partion i'r troseddwr yn gallu gweld eich lleoliad. Gallai hyn ddigwydd mewn achosion pan fyddwch yn dal mewn cysylltiad/yn dal i gwrdd â theulu neu ffrindiau'r troseddwr.



**Apple messages** - mewn achosion lle y bydd gennych chi a'r troseddwr eich rhifau ffôn eich gilydd o hyd a lle y byddwch yn defnyddio ap negeseua iPhone fel dull cysylltu, dylech edrych i weld a yw eich lleoliad yn cael ei rannu ag ef. Gellir gwneud hyn drwy ddilyn y camau canlynol:

- Messages > tapiwch y sgwrs â'r person dan sylw > tapiwch ei lun > os byddwch yn rhannu eich lleoliad, bydd ‘Stop sharing my location’ i'w weld fel opsiwn. Os felly, tapiwch ‘Stop sharing my location’.

**Noder** - Mae apiau masnachol ar gael y gellir eu gosod ar ddyfais (fel Life360 a Google Maps) ac y gellir eu defnyddio i dracio eich lleoliad. Bydd hyn yn bosiblwydd tebygol os oeddech mewn perthynas â'r troseddwr o'r blaen.

Edrychwch i weld pa apiau sydd wedi'u gosod ar eich ffôn. Os gwelwch apiau anghyfarwydd ar eich dyfais, dylech ymchwilio iddynt ar ddyfais ddiogel. Os bydd ap tracio wedi'i osod ar eich ffôn, dylech dynnu sgrinluniau a dadosod yr ap.

Dylech hefyd edrych i weld a oes unrhyw apiau cudd ar eich dyfais. Un ffordd o ddatgelu apiau cudd yw newid y cyfyngiadau yn eich gosodiadau –

- Settings > screen time > content & privacy restrictions > apps > allow all.

**Noder** - Mae apiau cudd ar iPhone yn nodwedd ar systemau iOS18 ac uwch.





## Google Location (Android)

Gyda Google Location Sharing, gallwch ddewis pwy sy'n gallu gweld eich lleoliad ac am faint o amser yr hoffech rannu eich lleoliad.

Os bydd troseddwr yn gallu cysylltu â'ch nodwedd 'Find My' neu unrhyw nodwedd arall sy'n dangos lleoliad, bydd yn gwybod ble yn union ydych chi. Gall hyn fod yn anniwel, oherwydd gallai fynd i'r un lle â chi, creu helynt, neu hyd yn oed eich bygwth/ceisio eich niweidio.

### Ap Find My Device

Pan gaiff cyfrif Google ei ychwanegu at ddyfais Android, caiff Find My Device ei droi ymlaen yn awtomatig. Bydd lleoliad mwyaf diweddar y ddyfais ar gael i'r cyfrif cyntaf a gafodd ei alluogi ar y ddyfais.

Gallwch edrych i weld â phwy rydych chi'n rhannu eich lleoliad a dileu'r dyfeisiau hynny drwy ddilyn y camau canlynol –

- Find My Device > Shared device > Settings > edrychwch i weld â phwy y mae'r ddyfais yn rhannu ei lleoliad. I ddileu dyfais, wrth ymyl y person tapiwch More > Stop sharing.
- Os bydd y troseddwr yn gwybod manylion eich cyfrif Google, bydd yn gallu defnyddio ap Find My Device i fewngofnodi fel chi a dod o hyd i'ch dyfais (caiff y nodwedd hon ei defnyddio yn yr ap os bydd dyfais 'ar goll'). Mae'n bwysig eich bod yn newid eich cyfrinair ar gyfer y cyfrif Google.



### Google Maps location

Mae'r nodwedd hon eich galluogi i rannu eich lleoliad amser real. Mae'n galluogi defnyddiwr iPhone i dracio defnyddiwr Android, ac fel arall.

Dylai goroeswyr edrych i weld a yw eu lleoliad yn cael ei rannu ag unrhyw ddyfeisiau ar yr ap hwn, a gallant hefyd ddileu dyfais drwy ddilyn y camau canlynol -

- Ap Google Maps > tapiwch eich proffil > Location sharing > edrychwch i weld â phwy y mae'r ddyfais yn rhannu ei lleoliad. I ddileu dyfais, tapiwch ei phroffil > tapiwch Stop.

**Note** - Dylid nodi bod apiau masnachol ar gael y gellir eu gosod ar ddyfais goroeswr (fel Life360) ac y gellir eu defnyddio i dracio lleoliad goroeswr. Bydd hyn yn bosiblwydd tebygol os oedd y goroeswr mewn perthynas â'r troseddwr o'r blaen.

Dylai goroeswyr edrych i weld pa apiau sydd wedi'u gosod ar eu ffôn. Os byddant yn gweld apiau anghyfarwydd ar eu dyfais, dylent ymchwilio iddynt ar ddyfais ddiogel. Os bydd ap tracio wedi'i osod ar eu ffôn, dylent ddadosod yr ap.

- Dylai goroeswyr hefyd edrych i weld a oes unrhyw apiau cudd ar eu dyfais.



## Cyfrifon Plant ar Android ac Apple

Caiff cyfrifon plant ar iPhones a dyfeisiau Android eu defnyddio gan rieni sydd am reoli a diogelu gweithgareddau digidol eu plant yn effeithiol.

Gall troseddwr ffurfweddu eich dyfais fel cyfrif plentyn er mwyn iddynt allu rheoli rhannau o'i gweithrediad. Mae hyn yn fath o reolaeth drwy orfodaeth ac mae'n eu galluogi i gael dylanwad dros bwy y gallwch siarad â nhw a pha apiau y gallwch eu defnyddio, a bydd yn eu galluogi i weld eich lleoliad unrhyw bryd.

Gellir defnyddio hyn ar ddyfeisiau eich plant hefyd, pan fyddwch chi a'r troseddwr wedi gwahanu ond wedi cael plant gyda'ch gilydd – gallai'r troseddwr fod wedi gosod dyfeisiau'r plant â chyfrifon plant arnynt. Er y gall hyn edrych fel ffordd o ddiogelu'r plant, bydd fel arfer yn cael ei wneud er mwyn gallu camdefnyddio nodweddion fel nodweddion dangos lleoliad.



Pan fydd eich dyfais/dyfeisiau wedi'i/wedi'u ffurfweddu fel cyfrif plentyn, gall y troseddwr wneud y canlynol:

- **Rheoli sgysiau a negeseuon testun** - Rheoli sgysiau a negeseuon testun – bydd y troseddwr yn gallu penderfynu pa gysylltiadau y gallwch siarad â nhw ac anfon negeseuon testun atynt, a phryd y gallwch wneud hynny. (Noder: ni fydd rheolaethau rhieni'n galluogi'r troseddwr i ddarllen negeseuon testun)
- **Rheoli/gweld gweithgarwch ar apiau a gwefannau** - bydd hyn yn galluogi'r troseddwr i ddewis pa apiau/nodweddion y gallwch eu defnyddio a phryd ac am ba mor hir y gallwch eu defnyddio, a gweld eich gweithgarwch ar apiau a gwefannau.
- **Gweld lleoliad** - bydd y troseddwr yn gallu atal newidiadau i rai gosodiadau preifatrwydd, gan gynnwys gosodiadau 'Share My Location'. Bydd hyn yn golygu y gall y troseddwr ffurfweddu eich ffôn i rannu eich lleoliad ag ef drwy'r amser.

### Sut i edrych i weld a yw dyfais wedi'i ffurfweddu fel cyfrif plentyn:

#### Apple

Agorwch settings > Apple ID > tapiwch Family > os bydd yn gofyn i chi osod cyfrif teulu, yna nid yw'r cyfrif yn gysylltiedig â chyfrif teulu. Os bydd yn mynd â chi i ddechrau'r broses o greu cyfrif teulu, tapiwch eich enw.

Yma fe welwch a yw'r plentyn wedi'i ffurfweddu fel cyfrif plentyn, a bydd sawl ffordd o wybod hyn:

- Bydd oedran y cyfrif wedi'i osod rhwng 13 a 17 oed.
- Bydd dyfeisiau'n gysylltiedig â'r adran 'Parents/Guardian'.
- Bydd yr adran rhannu lleoliad yn rhannu lleoliad y ddyfais â dyfeisiau eraill a enwir.

Os bydd dyfais wedi'i ffurfweddu fel cyfrif plentyn, yna mae'n bosibl y bydd modd gadael y nodwedd 'Family Sharing'. Os bydd oedran y cyfrif rhwng 13 a 17 oed, gall dyfais adael 'Family Sharing' os na fydd y 'rhiant' neu'r 'gwarcheidwad' wedi troi 'Screen time' ymlaen ar gyfer cyfrif y ddyfais. Os bydd wedi gwneud hynny, ni fydd y ddyfais yn gallu gadael y grŵp heb ganiatâd y trefnydd.

#### Android

- Gallwch edrych i weld a yw dyfais yn rhan o grŵp teulu drwy edrych ar y cyfrif Google sy'n gysylltiedig â'r ddyfais. Ar y cyfrif Google, fel Apple, dylai ddangos oedran y person sy'n gysylltiedig â'r cyfrif Google.
- Hefyd, os ewch i mewn i ap Family Link, fe welwch ryngwyneb lle y gallwch weld pa 'aelodau' sy'n rhan o'r grŵp y mae eich cyfrif Google yn gysylltiedig ag ef.

Os bydd y cyfrif Google yn gyfrif plentyn o dan 13 oed, yna bydd yn rhaid i'r 'rhiant' neu'r 'gwarcheidwad' roi caniatâd i'r cyfrif adael Family Link.

Ar gyfer dyfeisiau Apple ac Android, mae'n bosibl y bydd yn gallu ailosod y ddyfais i'r gosodiadau ffatri. Fodd bynnag, mae gan Apple ac Android nodweddion sy'n golygu na fydd modd defnyddio'r ddyfais gyda chyfrif Apple ID neu Google arall hyd yn oed ar ôl ailosod i'r gosodiadau ffatri. Mae hyn wedi'i fwriadu ar gyfer achosion pan fydd dyfais wedi cael ei dwyn, neu er mwyn atal plentyn rhag osgoi goruchwyliaeth.



## Ysbiwedd

Mae ysbiwedd, a elwir hefyd yn feddalwedd stelcio, yn cyfeirio at fath o ap neu feddalwedd sydd wedi'i dylunio i gael ei chuddio oddi wrth berchennog dyfais. Mae hyn yn galluogi rhywun i ysbïo ar weithgarwch unigolyn, tracio ei leoliad, neu hyd yn oed gofnodi trawiadau bysellau.

Gall troseddwr osod ysbiwedd ar eich dyfais er mwyn gallu eich monitro drwy eich ffôn. Er enghraifft, gallant wyllo unrhyw beth sydd yng ngolwg camera eich ffôn a hyd yn oed gael mynediad at eich microffon.

Mewn achosion lle mai cyn-bartner yw'r troseddwr, mae'n bosibl y bydd wedi gosod meddalwedd stelcio/ysbiwedd ar eich dyfeisiau.

Dyma rai arwyddion cyffredin y gall fod gennych ysbiwedd ar eich dyfais:

- Problemau perfformiad – bydd ysbiwedd yn gweithio'n galed yn y cefndir drwy'r amser ac yn cyrchu data person, a dyma pam y bydd eich dyfais yn rhedeg yn arafach nag arfer o bosibl.
- Y batri'n rhedeg allan yn anarferol o gyflym – gall tracio dyfais gan ddefnyddio ysbiwedd a chasglu data o'r ddyfais beri i fatri eich ffôn redeg allan yn gyflym.

Gallwch edrych i weld pa apiau sy'n defnyddio eich batri drwy ddilyn y camau canlynol:

iPhone ac Android: Settings > Battery > Battery usage by app. Gallwch edrych i weld a oes unrhyw apiau amheus/anhysbys yn defnyddio eich batri.

- Tymheredd y ffôn yn codi'n sydyn – mae'n arferol i dymheredd ffôn godi pan fydd yn cael ei wefru neu'n defnyddio ap am gyfnod hir, ond ni ddylai hynny ddigwydd pan fydd eich ffôn yn segur neu'n cyflawni tasgau ysgafn.
- Y ffôn yn troi ymlaen ac yn diffodd ar hap.

Dylid nodi y dylid ystyried yr arwyddion hyn, ond ni fyddant o reidrwydd yn golygu bod ysbiwedd ar eich ffôn (mae'n bosibl y bydd rhesymau diniwed eraill drostynt).

Edrychwch i weld pa apiau sydd wedi'u gosod ar eich ffôn. Dylid nodi y gall ysbiwedd guddio drwy edrych fel ap arall (e.e. cyfrifiannell, dyddiadur ac ati). Dylech ddileu unrhyw apiau sy'n anghyfarwydd.

Os byddwch mewn sefyllfa lle y byddwch yn amau bod meddalwedd stelcio/ysbiwedd wedi cael ei gosod ar eich dyfais, neu os ydych wedi bod mewn sefyllfa o'r fath o'r blaen, fe'ch cynghorir i ailosod y ddyfais i'r gosodiadau ffatri. Y rheswm dros hyn yw am fod apiau ysbiwedd i'w cael na fyddant yn ymddangos fel ap arferol (dylid gwneud copi wrth gefn o ddata pwysig).

Nodweddion apiau cudd ar iPhone ac Android:

- Dylech fod yn ymwybodol bod iOS18 bellach yn eich galluogi i guddio apiau. Un ffordd o ddatgelu apiau cudd yw newid y cyfyngiadau yn eu gosodiadau:
- Settings > Screen time > Content & privacy restrictions > Apps > Allow all.
- Ffordd arall o ddatgelu apiau cudd yw edrych ar yr apiau a brynwyd yn yr App Store.

Dylech hefyd edrych i weld a yw eich ffôn Android wedi cael ei ffurfweddu i guddio apiau. Settings > Display > Home screen > Hide apps.

Os gwelwch ap yr hoffech ei ddadosod:

### iPhone

Edrychwch drwy sgrin hafan y ffôn a chwiliwch am yr ap yr hoffech ei ddileu > tapiwch a daliwch eich bys ar yr ap > dewiswch 'Remove app' > cadarnhewch drwy bwysu 'Delete app'.

### Android

Settings > Apps > tapiwch 'see all apps' > chwiliwch am yr ap yr hoffech ei ddileu > tapiwch 'Uninstall' > tapiwch 'ok'.



## Ffurfweddu gwasanaethau brys

Gyda'r ap Emergency SOS, gallwch ffonio am help a rhoi gwybod i'ch cysylltiadau brys yn gyflym ac yn hawdd.

Os bydd troseddwr yn tracio eich lleoliad neu'n eich dilyn chi, gellir ffurfweddu gwasanaethau brys ar eich ffôn. Mae hyn wedi'i fwriadu ar gyfer sefyllfaoedd lle y byddwch yn teimlo'n anniogel yn gadael eich cartref, lle y bydd y troseddwr yn eich dilyn chi yn y fan a'r lle, a/neu lle y bydd y troseddwr yn ymddwyn mewn ffordd ymosodol/bygythiol.

**Noder** - Ar iPhone 14 ac uwch, gallwch ddefnyddio lloeren i anfon neges destun at y gwasanaethau brys pan na fydd gennych signal ffôn na Wi-Fi. I roi cynnig ar y fersiwn brawf, ewch i Settings > Emergency SOS > sgroliwch i lawr i 'Emergency SOS via satellite' a thapiwch 'Try Demo'.

### Ffonio'r gwasanaethau brys yn gyflyms:

#### iPhone

- Pwyswch a daliwch y botwm ochr a'r naill fotwm sain neu'r llall nes i'r llithryddion ymddangos a'r ôl-gyfrif ar Emergency SOS ddod i ben > rhyddhewch y botymau.
- Ffordd arall o alluogi iPhone i ddechrau Emergency SOS yw pwysu'r botwm ochr bum gwaith yn gyflym.
  - Settings > Emergency SOS > trowch 'Call with 5 Presses' ymlaen

Pan ddaw galwad frys i ben, bydd eich ffôn yn rhoi gwybod i'ch cysylltiadau brys ble ydych chi – byddant hefyd yn cael diweddariadau pan fydd eich lleoliad yn newid.

#### I ychwanegu cysylltiadau brys

- Agorwch yr ap Health > tapiwch eich proffil > tapiwch 'Medical ID' > Edit > sgroliwch i 'Emergency Contacts' > tapiwch y botwm 'Add' > tapiwch yr unigolyn cyswllt > ychwanegwch pa berthynas ydyw i chi.
- 'Call Quietly' (ar gael ar iOS 16.3 a diweddarach) – pan fydd 'Call Quietly' ymlaen a byddwch yn ceisio gwneud galwad frys, bydd unrhyw larymau a fflachiadau wedi'u diffodd.

I alluogi hyn -

- Settings > Emergency SOS > Trowch 'Call quietly' ymlaen.

#### Android

- Settings > Safety and Emergency (mae'n bosibl y bydd hyn o dan 'Advanced features') > Emergency SOS.
  - Pan fydd y nodwedd hon wedi'i throï ymlaen, gallwch bwysu'r botwm ochr (y botwm pŵer fel arfer) bum gwaith yn gyflym.
- Gallwch hefyd ffurfweddu eich dyfais i anfon neges at eich cysylltiadau brys. Bydd y negeseuon yn cynnwys gwybodaeth am eich lleoliad, recordiad sain gan ddefnyddio microffon eich ffôn, cais ysgrifenedig am help, a rhybudd os bydd batri eich ffôn bron â marw.

Gellir gwneud hyn drwy ddilyn y camau canlynol -

- Settings > Safety and Emergency > 'Share info with Emergency contacts' > Dewiswch pa gysylltiadau yr hoffech eu hysbysu os bydd Emergency SOS wedi'i alluogi.



# Dyfeisiau Cysylltiedig



## AirPods/Clustffonau

Seinyddion cludadwy sy'n ffitio yng nghlustiau pobl ac sy'n gallu cysylltu ag unrhyw ddyfais sy'n cynhyrchu sain gan ddefnyddio technoleg sain Bluetooth.

Gall troseddwr ddefnyddio AirPods a chlustffonau di-wifr eraill i'ch monitro chi a gwybod ble ydych chi.

**Note** - Mae'n bosibl na fyddwch yn gwybod bod gennych AirPods, neu fath arall o glustffonau sy'n gallu rhannu eich lleoliad, yn agos atoch (gallai'r troseddwr fod wedi'u rhoi yn eich bag, yn eich poced ac ati). Fe'ch cynghorir i edrych drwy eich bagiau a'ch pocedi, yn enwedig mewn achosion lle roedd perthynas rhyngoch chi a'r troseddwr/lle mae perthynas rhyngoch o hyd.

Gallwch wybod ble mae AirPods a chlustffonau di-wifr eraill (e.e. Beats) gan ddefnyddio dyfais iOS drwy ddefnyddio ap Find My Apple, a nodweddion fel 'Lost Mode' a 'Family Sharing'.

- Family Sharing – mae'n eich galluogi i rannu lleoliad eich AirPods ag aelodau o'r teulu. Mae hyn yn golygu y gallai troseddwr gysylltu â'ch AirPods a thracio eich lleoliad. Gallwch edrych i weld pwy sydd wedi cysylltu â'ch AirPods drwy fynd i 'Find my' > 'Devices' neu 'People'. Dilëwch unrhyw ddyfeisiau sy'n anadnabyddadwy neu'n ddieisiau.
- Hyd yn oed os bydd AirPods wedi'u diffodd neu'n farw, mae 'Lost Mode' ar gael er mwyn dod o hyd iddynt. Drwy nodi eu bod 'ar goll', gallwch gael rhybuddion os cânt eu cysylltu â dyfais iOS arall, gallwch gael gwybod lleoliad y sawl sydd wedi 'dod o hyd iddynt', a gallwch anfon neges wedi'i phersonoli. Dim ond y perchennog, gan ddefnyddio cyfrif y perchennog, a all ysgogi hyn, felly, os mai rhodd gan y troseddwr oedd yr AirPods, bydd hyn yn rhywbeth i'w ystyried.
- Os mai rhodd i chi gan y troseddwr oedd yr AirPods, bydd yn rhaid ailosod yr AirPods, a dim ond y perchennog fydd yn gallu gwneud hyn. Os bydd yr AirPods yn dal gennych/os byddwch yn dal i'w defnyddio, fe'ch cynghorir i gael gwared arnynt.



## Watshys clyfar

Dyfais gludadwy a gaiff ei gwisgo ar yr arddwrn ac sy'n cefnogi apiau ac yn gweithredu fel estyniad i'ch ffôn symudol yw watsh glyfar.

Gall troseddwr ddefnyddio watshys clyfar i'ch monitro chi a gwybod ble ydych chi.

### Apple watch

Yn debyg i AirPods, gellir gosod Apple Watch ar 'Family Sharing', a fydd yn galluogi unrhyw ddyfais sy'n defnyddio'r nodwedd honno i dracio'r watsh a gwybod ble mae hi. Dylech edrych i weld a yw eich Apple Watch wedi'i chysylltu â'r nodwedd 'Family Sharing' ac, os felly, pa ddyfeisiau sy'n eich galluogi i wybod ble mae'r watsh.

- Settings > [eich enw] > os gwelwch 'Set up Family Sharing', nid ydych yn defnyddio 'Family Sharing' ar gyfer yr Apple ID dan sylw NEU os gwelwch eicon 'Family Sharing', gallwch ei dapio i weld yr aelodau a'u rolau. Wedyn, cliciwch 'Remove' ar enw'r aelod.

**Note** - Os nad chi yw 'trefnydd' y grŵp Family Sharing ond eich bod yn aelod sy'n oedolyn, gallwch dapio eich enw > Stop using family sharing.

Gellir rhannu lleoliad ar 'Find My' hefyd – gallai troseddwr fod wedi gosod hyn ar eich Apple Watch. I roi'r gorau i rannu eich lleoliad, tapiwch enw'r 'ffrind' ar y sgrin 'Find People' > wedyn tapiwch 'Stop Sharing'.

Yn yr un modd ag AirPods, os mai'r troseddwr a roddodd y watsh i chi a'i bod wedi cael ei gosod gan ddefnyddio ei gyfrif gyda'r clo ysgogi wedi'i alluogi, ni fydd modd datgysylltu'r watsh heb Apple ID a chyfrinair y troseddwr. Mewn achos o'r fath, fe'ch cynghorir i gael gwared ar y watsh.



### Watshys clyfar Garmin

Nodwedd tracio sy'n galluogi unigolyn i rannu ei lleoliad amser real a gwybodaeth dracio â phobl o'u dewis yw Garmin LiveTrack. Bydd yn gweithio wrth dracio gweithgaredd, fel rhedeg neu feicio, ond hefyd pan fydd y defnyddiwr yn gwisgo ei watsh fel arfer.

- Gallwch edrych i weld a yw LiveTrack wedi'i alluogi drwy fynd i ap Garmin Connect ar eich ffôn. Dewiswch 'More' (yn y gornel dde isaf) > 'Safety & Tracking' neu 'LiveTrack' > Dewiswch 'LiveTrack' > Dewiswch y tri dot (yn y gornel dde uchaf) > Dewiswch 'LiveTrack Data & Privacy' > Os bydd 'LiveTrack' wedi'i alluogi, dewiswch 'Opt Out'.

**Note** - Mae watshys clyfar eraill ar gael sy'n cynnwys nodweddion rhannu lleoliad/tracio. Os ydych yn berchen ar watsh glyfar, dylech fwrw golwg dros ffurfweddadau'r ap sydd wedi'i baru â hi. Mae canllawiau ar sut mae'r nodweddion rhannu lleoliad/tracio yn gweithio i'w cael ar-lein.





## AirTags a Chipolo

Bydd AirTags a Chipolo (yn ogystal â thagiau eraill) yn cyfathrebu â ffonau clyfar gan ddefnyddio Bluetooth – caiff y rhain eu defnyddio i dracio lleoliad eitemau.

Gall troseddwr ddefnyddio tagiau clyfar i'ch monitro chi a gwybod ble ydych chi.

### Smart tags

Mae tagiau clyfar yn ddull a ddefnyddir yn eang i dracio goroeswyr a gwybod ble maen nhw. Gall y tracwyr hyn amrywio o ran maint, siâp a lliw, yn dibynnu ar eu gwneuthuriad (bydd rhai mor fach â cheiniog, hyd yn oed).

Os bydd y troseddwr yn tracio eich lleoliad heb i chi wybod sut, mae'n bosibl y bydd wedi gosod traciwr yn rhywle. Gall tracwyr gael eu rhoi mewn bagiau, pyrsiau, pocedi cotiau, y tu mewn i geir ac ati.

Mae'n bwysig eich bod yn edrych drwy eich dillad a'ch bagiau, yn enwedig pan fyddwch ar eich ffordd allan o'r tŷ.

Dylech hefyd edrych drwy deganau, bagiau a dillad eich plant (os bydd hyn yn berthnasol) gan ei bod yn bosibl y bydd y troseddwr wedi gosod dyfeisiau tracio ynddynt.

### AirTags

Cyn i Apple gyflwyno nodweddion diogelwch newydd er mwyn helpu i atal tracio anwirfoddol, byddai pobl yn defnyddio AirTags yn eang i dracio pobl a gwybod ble roedden nhw.

Sut y gallwch wybod a oes AirTag yn eich tracio chi? Er mwyn helpu i wybod a oes AirTag yn eich tracio chi, bydd iPhone y person yn rhoi gwybod i chi pan fydd AirTag anhysbys yn teithio gyda chi. Pan fyddwch yn tapio'r hysbysiad, bydd map yn dangos i chi pryd y cafodd yr AirTag anhysbys sy'n teithio gyda chi ei ganfod gyntaf.

Mae hyd yn oed nodwedd 'chwarae sain' ar gael, a fydd yn ysgogi sŵn bipian er mwyn eich galluogi i ddod o hyd i'r AirTag yn haws.

Os mai dyfais Android sydd gennych yn hytrach nag un Apple, y cyngor gan Apple yw i bobl lawrlwytho 'Tracker Detect'. Mae'r ap hwn yn helpu defnyddwyr Android i ddarganfod AirTags a dyfeisiau eraill cydnaws â 'FindMy' sy'n agos atynt.

Os dewch o hyd i AirTag anhysbys, gallwch atal y perchennog rhag eich canfod chi drwy wthio cefn yr AirTag i lawr a'i droi'n wrthglocwedd > tynnu'r caead i ffwrdd a thynnu'r batri allan.

**Noder** - Nid yw hyn yn golygu bod y nodweddion diogelwch newydd yn gwbl ddibynadwy, felly dylech edrych i wneud yn siŵr nad oes AirTags yn agos atoch o hyd.

### Chipolo (y dewis gorau ar gyfer Android)

Un cynnyrch gan Chipolo yw 'Card Point'. Mae'n ffitio mewn waled ac mae'n hawdd i bobl beidio â sylwi arno. Mae'n defnyddio nodwedd 'Find My Device' Google a dim ond ar ddyfeisiau Android y mae ar gael.

Os dewch o hyd i un o'r 'Card Points' hyn, gallwch > chwilio am y botwm yng nghornel chwith isaf y ddyfais > pwyso a dal y botwm am tua 30 eiliad nes iddo ddechrau bipian unwaith yr eiliad > rhyddhewch y botwm ar ôl y degfed bip > pan fydd y ddyfais wedi'i hanalluogi, bydd sain i gadarnhau hynny.

**Noder** - Mae llawer o wahanol fathau o dagiau clyfar ar gael y gall y troseddwr eu defnyddio. Os dewch o hyd i draciwr arnoch neu'n agos atoch, dylech chwilio am rywle diogel a chyhoeddus i'w analluogi drwy ddilyn y cyfarwyddiadau ar wefan y gwneuthurwr.



## Rhan Tri: Canllawiau ar gyfer Apiau Ar-lein

Diffinnir ap fel pecyn meddalwedd hunangynhwysol sy'n galluogi defnyddwyr i gyflawni tasgau penodol ar ddyfais symudol neu gyfrifiadur.



## Bancio Ar-lein

Mae bancio ar-lein yn eich galluogi i gyflawni trafodion ariannol drwy'r rhyngwrwyd. Mae bancio ar-lein yn cynnig bron pob gwasanaeth sydd ar gael yn draddodiadol drwy gangen leol, gan gynnwys adneuron, trosglwyddiadau, a thalu biliau ar-lein.

Gall troseddwr anfon trafodion i'ch cyfrif banc a chynnwys negeseuon (sy'n aml yn ddifriol) ym maes cyfeirnod y taliad. Hefyd, os bydd ganddynt fynediad at eich ap bancio ar-lein, gallant wedyn fwrw golwg dros eich trafodion a ble y cawsant eu gwneud. Mae hyn yn golygu y bydd yn gallu gweld ble ydych chi neu ble rydych chi wedi bod.

Os oeddech yn arfer rhannu manylion eich cerdyn â'r troseddwr, neu os bydd manylion eich cerdyn yn dal wedi'u storio ar ffôn y troseddwr, fe'ch cynghorir i wneud cais am gerdyn banc newydd. Bydd hyn er mwyn atal y troseddwr rhag defnyddio eich manylion banc.

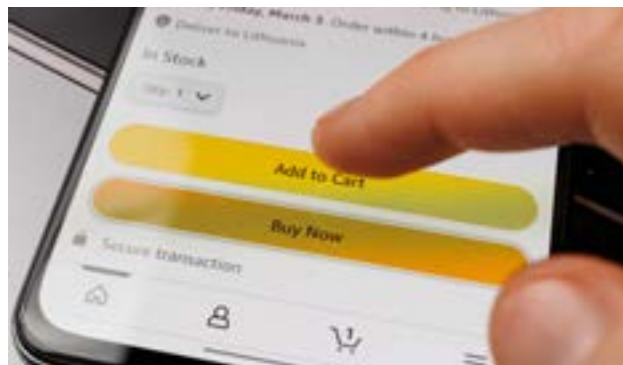
Hyd yn oed os byddwch wedi gwneud cais am gerdyn newydd neu os byddwch wedi cael eich cerdyn newydd, bydd y troseddwr yn dal i allu anfon trafodion i'ch cyfrif banc. Gall hyn fod yn broblem (yn enwedig os bydd taliadau cynhaliaeth plant yn cael eu gwneud), gan fod achosion wedi bod lle y gwnaeth troseddwr gamddefnyddio'r system dalu drwy gynnwys geiriau a negeseuon difriol ym maes cyfeirnod y taliad.

I'r rhai sydd wedi bod mewn perthynas â'r troseddwr, mae'n bosibl na fyddant wedi bod yn rheoli eu materion ariannol a'u trefniadau bancio eu hunain. Yn ffodus, mae llawer o fanciau bellach wedi ymrwmo i God Ymarfer Cam-drin Ariannol UK Finance (cod ymarfer gwirfoddol sydd â'r nod o gefnogi goroeswyr cam-drin ariannol).

**Note** - Dylai'r banciau allu atal cyfrif penodol rhag gadael neges ym maes cyfeirnod eich cyfrif. Bydd hyn yn arbennig o ddefnyddiol pan fydd angen i'r troseddwr wneud taliadau cynhaliaeth plant. Hefyd, os na fydd rheswm i'r troseddwr anfon arian atoch, dylai'r banciau allu rhwystro trafodion o gyfrif y troseddwr.

Mae'r ddelwedd isod yn dangos yr holl fanciau sydd wedi ymrwmo i'r cod cam-drin ariannol. Os oes gennych chi gyfrif gydag un o'r banciau hyn, ewch i'r dudalen gymorth ar gam-drin ariannol ar wefan y banc. Ar y dudalen we, fe welwch wybodaeth gyswllt er mwyn eich helpu gyda'r problemau sy'n eich wynebu mewn perthynas â'ch cyfrif banc.





## Apiau Siopa a Chludfwyd

**Cyfrifon Siopa** – Prynu nwyddau neu wasanaethau dros y rhyngwrdd.

**Cyfrifon Cludfwyd** - Llwyfannau ar gyfer prynu nwyddau groser, bwydydd o fwytaï a gwasanaethau eraill.

### Pam mae'n bwysig sicrhau bod y cyfrifon hyn yn ddiogel?

**Manylion banc** - Os bydd manylion eich cerdyn banc wedi'u storio yn y cyfrif, bydd y troseddwr yn gallu defnyddio'r cerdyn i brynu pethau.

**Cyfeiriad cartref** - Os bydd gan y troseddwr fynediad i'r cyfrif o hyd, bydd yn gallu gweld eich cyfeiriad cartref.

Dylech fwrw golwg dros y gwahanol gyfrifon siopa a chludfwyd ar-lein sydd gennych a newid eich manylion ynddynt. Dan rai amgylchiadau, mae'n bosibl y byddwch chi a'r troseddwr wedi defnyddio'r un cyfrifon siopa a chludfwyd. Os felly, mae ambell beth y gallwch ei wneud:

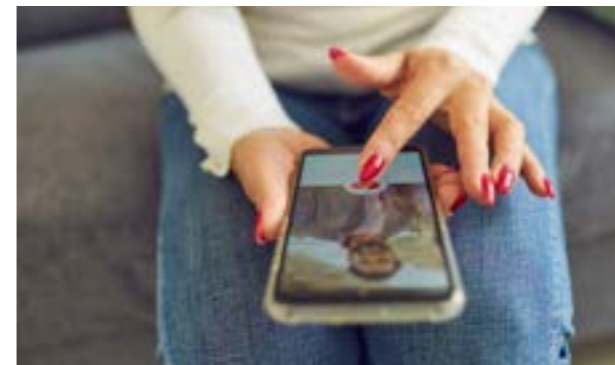
Newidiwch gyfrinair y cyfrif – os bydd eich cyfeiriad e-bost wedi'i gysylltu â'r cyfrif siopa (y cyfeiriad e-bost a ddefnyddiwyd i greu'r cyfrif), dylech newid y cyfrinair yn un cryf a diogel.

Hefyd, sicrhewch fod prawf dilysu dau gam wedi'i alluogi os oes modd. Bydd hyn er mwyn atal mynediad heb awdurdod hyd yn oed os bydd rhywun yn gwybod y cyfrinair.

**Noder** - Gallwch weld sut i newid y cyfrinair a galluogi prawf dilysu dau gam yn adran gosodiadau'r cyfrif.

Crëwch gyfrif newydd – os mai'r cyfeiriad e-bost y troseddwr yw'r un sy'n gysylltiedig â'r cyfrif, dylech ddileu eich holl fanylion personol o'r cyfrif, allgofnodi o'r cyfrif a chreu un newydd.

**Noder** - Er mwyn i'r cyfrif barhau i fod yn ddiogel, dylai'r cyfrif e-bost a ddefnyddir ar gyfer y cyfrifon hyn fod yn ddiogel hefyd. Y rheswm dros hyn yw, os bydd gan y troseddwr fynediad i'r cyfrif e-bost, y bydd wedyn yn gallu defnyddio nodwedd adfer cyfrinair a newid y cyfrinair yn ôl.



## Apiau caru

Gwasanaeth caru ar-lein a gyflwynir drwy ap ffôn symudol.

Gall troseddwr fonitro apiau caru i weld a oes gennych broffil, a gallant ddefnyddio eich proffil fel ffordd o gasglu gwybodaeth. Er enghraifft, os byddwch wedi symud i ffordd oddi wrth y troseddwr, bydd yn gallu gweld pa leoliad y byddwch wedi'i osod ar eich cyfrif (tref neu ddinas). Gallai hefyd greu cyfrif ffug er mwyn 'paru' â'ch proffil chi a siarad â chi (mae hyn yn fath o swyno drwy dwyll).

Mae llawer o ragofalon diogelwch y dylech fod yn ymwybodol ohonynt wrth ddefnyddio apiau caru. Er enghraifft, mae Refuge Tech Safety (2024) yn awgrymu:

- Os byddwch yn defnyddio apiau caru, dylech gyfyngu ar y wybodaeth bersonol adnabyddadwy y byddwch yn ei rhannu.
- Dylech hefyd sicrhau nad yw eich proffil ar yr ap yn gysylltiedig â'ch cyfrifon cyfryngau cymdeithasol, er mwyn osgoi datgelu rhagor o wybodaeth amdanoch chi eich hun.
- O ran nodwedd lleoliad apiau caru, gosodwch eich lleoliad eich hun a dewiswch un nad yw'n rhy benodol. O ran y ffotograffau y byddwch yn eu lanlwytho i'r ap, sicrhewch nad ydynt yn cynnwys trydydd partion. Bydd hyn yn atal y troseddwr rhag cael gwybodaeth amdanynt drwy ddod o hyd i'w cyfrifon cyfryngau cymdeithasol o bosibl. Dylech hefyd sicrhau nad yw'r ffotograffau y byddwch yn eu postio'n datgelu unrhyw beth (fel eich lleoliad).
- Byddwch yn ofalus â phroffiliau y byddwch yn cyfathrebu â nhw (er enghraifft drwy wneud chwiliad delwedd â'u lluniau) er mwyn cadarnhau p'un a ydynt yn broffiliau dilys ai peidio.
- Parhewch i gyfathrebu â'r proffiliau ar yr ap caru yn hytrach na symud i gyfathrebu y tu allan i'r ap.
- Sicrhewch fod eich gosodiadau diogelwch wedi'u haddasu a'ch bod yn rhoi mesurau diogelwch ar waith fel prawf dilysu dau gam, a defnyddiwch gyfeiriad e-bost gwahanol i'ch un rheolaidd.

Dylid nodi hefyd y gallwch flocio rhai proffiliau rhag dod o hyd i chi ar rai apiau caru drwy roi rhif ffôn y cyn-bartner/troseddwr.



## Apiau cludiant

**Uber** - Llwyfan ar gyfer archebu a darparu siwrneiau, prydau bwyd a nwyddau.

**Trainline** - Llwyfan ar gyfer archebu tocynnau trenau a bysiau.

Mae'n hollbwysig eich bod yn sicrhau nad yw'r troseddwr yn gallu cael mynediad i gyfrifon fel Uber neu Trainline. Y rheswm dros hyn yw y gall y troseddwr edrych drwy eich hanes siwrneiau manwl a gweld eich patrwm teithio o ddydd i ddydd a ble y gallwch fod ar adegau penodol o bosibl.

Yn debyg i apiau siopa a chludfwyd, dylech fwrw golwg dros y cyfrifon cludiant sydd gennych/rydych chi'n eu defnyddio. Os oeddech yn rhannu'r un cyfrifon cludiant â'r troseddwr, bydd un neu ddau o bethau i'w hystyried:

- Newidiwch gyfrinair y cyfrif – os bydd eich cyfeiriad e-bost wedi'i gysylltu â'r cyfrif cludiant (y cyfeiriad e-bost a ddefnyddiwyd i greu'r cyfrif), newidiwch y cyfrinair yn un cryf a diogel.
- Hefyd, sicrhewch fod prawf dilysu dau gam wedi'i alluogi os oes modd. Bydd hyn er mwyn atal mynediad heb awdurdod hyd yn oed os bydd rhywun yn gwybod y cyfrinair.

**Noder** - Gallwch weld sut i newid y cyfrinair a galluogi prawf dilysu dau gam yn adran gosodiadau'r cyfrif.

Crëwch gyfrif newydd – os mai'r cyfeiriad e-bost y troseddwr yw'r un sy'n gysylltiedig â'r cyfrif, dylech ddileu eich holl fanylion personol, allgofnodi a chreu cyfrif newydd.

**Noder** - Er mwyn i'r cyfrif barhau i fod yn ddiogel, dylai'r cyfrif e-bost a ddefnyddir ar gyfer y cyfrifon hyn fod yn ddiogel hefyd. Y rheswm dros hyn yw, os bydd gan y troseddwr fynediad i'r cyfrif e-bost, y bydd wedyn yn gallu defnyddio nodwedd adfer cyfrinair a newid y cyfrinair yn ôl.

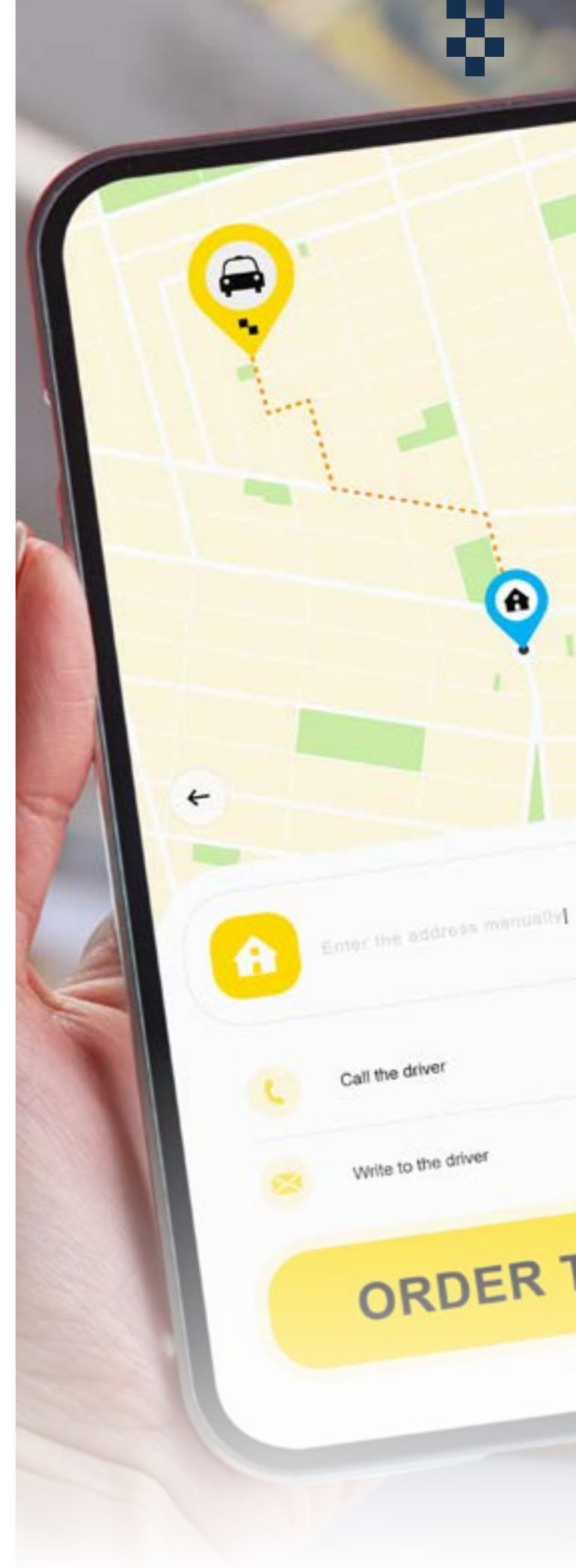


## Uber

Ar Uber, mae nodwedd sy'n galluogi mwy nag un teithiwr. I ddileu teithiwr:

Agorwch ap Uber > ewch i'r adran 'Riders' lle y gallwch weld yr holl deithwyr rydych wedi'u hychwanegu at y cyfrif > chwiliwch am enw'r teithiwr yr hoffech ei ddileu a thapiwch ar ei enw > wedyn dylech weld opsiwn i ddileu/tynnu'r teithiwr o'ch cyfrif.

**Noder** - Pan fyddwch yn dileu teithiwr o'ch cyfrif Uber, caiff ei ddata ei dynnu o'ch cyfrif, ac ni fydd yn gallu cael mynediad i'ch cyfrif er mwyn archebu siwrneiau mwyach.





## Apiau rhedeg (Strava)

Llwyfan ar gyfer tracio metrigau iechyd a pherfformiad. Mae hefyd yn cynnig lle i storio gwybodaeth am eich sesiynau ymarfer, rhedeg a gweithgareddau eraill.

Gall troseddwr ddefnyddio'r apiau hyn i fonitro eich llwybrau rhedeg a'u gweld ar fap. Os na fyddwch wedi ffurfweddu gweledd eich map i guddio dechrau a diwedd eich llwybr, bydd posiblwydd y gall y troseddwr ddarganfod ble rydych chi'n byw.

**Noder** - Ni fydd gweithgareddau a wneir gyda'r gosodiadau "Followers" ac "Only you" yn gymwys i ymddangos ar sgorfyrddau segmentau cyhoeddus ac mae'n bosibl na fyddant yn gymwys ar gyfer rhai heriau neu gyflawniadau.

Mae apiau rhedeg ac apiau ffitrwydd tebyg yn dod yn fwy poblogaidd, felly mae sicrhau bod y rheolaethau preifatrwydd cywir ar waith yn hanfodol ar gyfer eich diogelwch. Gallai troseddwr ddefnyddio'r apiau hyn i gasglu gwybodaeth amdanoch.

Er enghraifft, mae Strava (2024) wedi rhannu gwybodaeth am y ffordd y mae'n galluogi defnyddwyr eraill i weld manylion am broffil rhywun os na fydd rheolaethau preifatrwydd wedi'u galluogi:

### Tudalen broffil

Os mai "Everyone" a nodir yn y rheolaethau preifatrwydd yn hytrach na "Followers", bydd hynny'n golygu y gall cymuned gyfan Strava weld manylion llawn eich proffil. Pan fydd yr opsiwn "Followers" wedi'i ddewis ar gyfer y proffil, bydd yn rhaid i bobl wneud cais am gael dilyn y proffil. Sicrhewch mai teulu a ffrindiau yw'r unig bobl sy'n eich dilyn a bod y manylion ar eich cyfrif yn gyfyngedig. I newid gosodiadau proffil:

- Ap Strava > agorwch y gosodiadau o'r eicon yng nghornel dde uchaf y tab 'You' > tapiwch 'Privacy controls' > dewiswch 'Profile page' > dewiswch 'Followers'.

### Gweithgareddau

Bydd eich tudalen weithgareddau'n dangos data am eich gweithgareddau ar Strava (e.e. dyddiad ac amser, mapiau (lleoliad) ac ati). Os bydd y troseddwr yn gallu gweld y data hyn, bydd yn gallu darganfod eich patrymau rhedeg (e.e. pa amser o'r dydd y byddwch yn rhedeg) a'r llwybrau y byddwch yn eu dilyn. Sicrhewch mai'r opsiwn "Followers" neu "Only you" sydd wedi'i ddewis ar gyfer eich gosodiadau gweithgareddau. Gellir gwneud hyn drwy ddilyn y camau canlynol

- Ap Strava > agorwch y gosodiadau o'r eicon yng nghornel dde uchaf y tab 'You'

> tapiwch 'Privacy controls' > o dan 'Activities', dewiswch naill ai 'Followers' neu 'Only you'.

### Gweithgareddau grŵp

Un o'ch gweithgareddau sydd wedi cael ei grwpio ag un neu fwy o weithgareddau eraill gan athletwr gwahanol yw gweithgaredd grŵp. Pan fyddwch yn dewis yr opsiwn 'Followers' ar gyfer y gosodiad preifatrwydd hwn, ni fydd pobl nad ydynt yn eich dilyn:

- yn gallu eich gweld wedi eich grwpio yn eu gweithgareddau
- yn gallu gweld eich bod wedi bod yn rhan o grŵp athletwr arall
- yn gallu gweld eich bod wedi cael eich grwpio ag athletwyr eraill yn eich gweithgareddau eich hun.

Sicrhewch mai'r opsiwn "Followers" sydd wedi'i ddewis ar gyfer gosodiadau gweithgareddau grŵp neu, i fod yn fwy gofalus, "No one". Gellir gwneud hyn drwy ddilyn y camau canlynol:

- Ap Strava > agorwch y gosodiadau o'r eicon yng nghornel dde uchaf y tab 'You' > tapiwch 'Privacy controls' > o dan 'Group activities', dewiswch naill ai 'Followers' neu 'No one'.

### Flyby

Adnodd Strava Labs sy'n eich galluogi i chwarae eich gweithgaredd yn ôl, yn ogystal â gweithgareddau pobl gerllaw, ar fap a llinell amser yw hwn. Mae dau opsiwn ar gael ar gyfer y gosodiad hwn, sef "Everyone" neu "No one". Os byddwch yn dewis "Everyone", bydd holl athletwyr Strava:

- yn gallu gweld a wnaeth eich llwybrau groesi neu a oeddech gerllaw ar Flyby
- yn gallu clicio ar eich rhithffurf Flyby i agor eich gweithgareddau Strava.

Sicrhewch mai'r opsiwn "No one" sydd wedi'i

ddewis ar gyfer gosodiadau Flyby. Gellir gwneud hyn drwy ddilyn y camau canlynol:

- Ap Strava > agorwch y gosodiadau o'r eicon yng nghornel dde uchaf y tab 'You' > tapiwch 'Privacy controls' > o dan 'Flybys', dewiswch 'No one'.

### Gweledd map

Bydd hyn yn eich galluogi i guddio rhannau o fap eich gweithgaredd oddi wrth athletwyr eraill Strava. Mae hefyd opsiwn i osod dewis diofyn er mwyn i'ch gweithgareddau gael eu lanlwytho â'r dewis hwn yn awtomatig. Gyda nodweddion gweledd map, gallwch bersonoli faint o ddechrau neu ddiwedd gweithgaredd a gaiff ei guddio hyd at radiws o filltir, neu gallwch guddio'r map cyfan. I wneud hyn

- So Ap Strava > agorwch y gosodiadau o'r eicon yng nghornel dde uchaf y tab 'You' > tapiwch 'Privacy controls' > tapiwch 'Edit map visibility'.

### Blocking an athlete

If you wish to block an athlete, you can do this by:

- Open the app > from the profile of the athlete you'd like to block, tap the three-dot icon > select 'Block this Athlete'.

**Note** - Dylech hefyd ystyried apiau ffitrwydd eraill y byddwch yn eu defnyddio a dysgu am y nodweddion preifatrwydd y gallwch eu gosod. Gallwch wneud hyn drwy fynd i wefan yr ap ffitrwydd, neu drwy edrych ar osodiadau preifatrwydd yr ap.



## Apiau sy'n cysylltu â cheir

Mae'r rhain yn cynnig y gallu i reoli eich cerbyd o'ch ffôn ac anfon gorchmynion o bell.

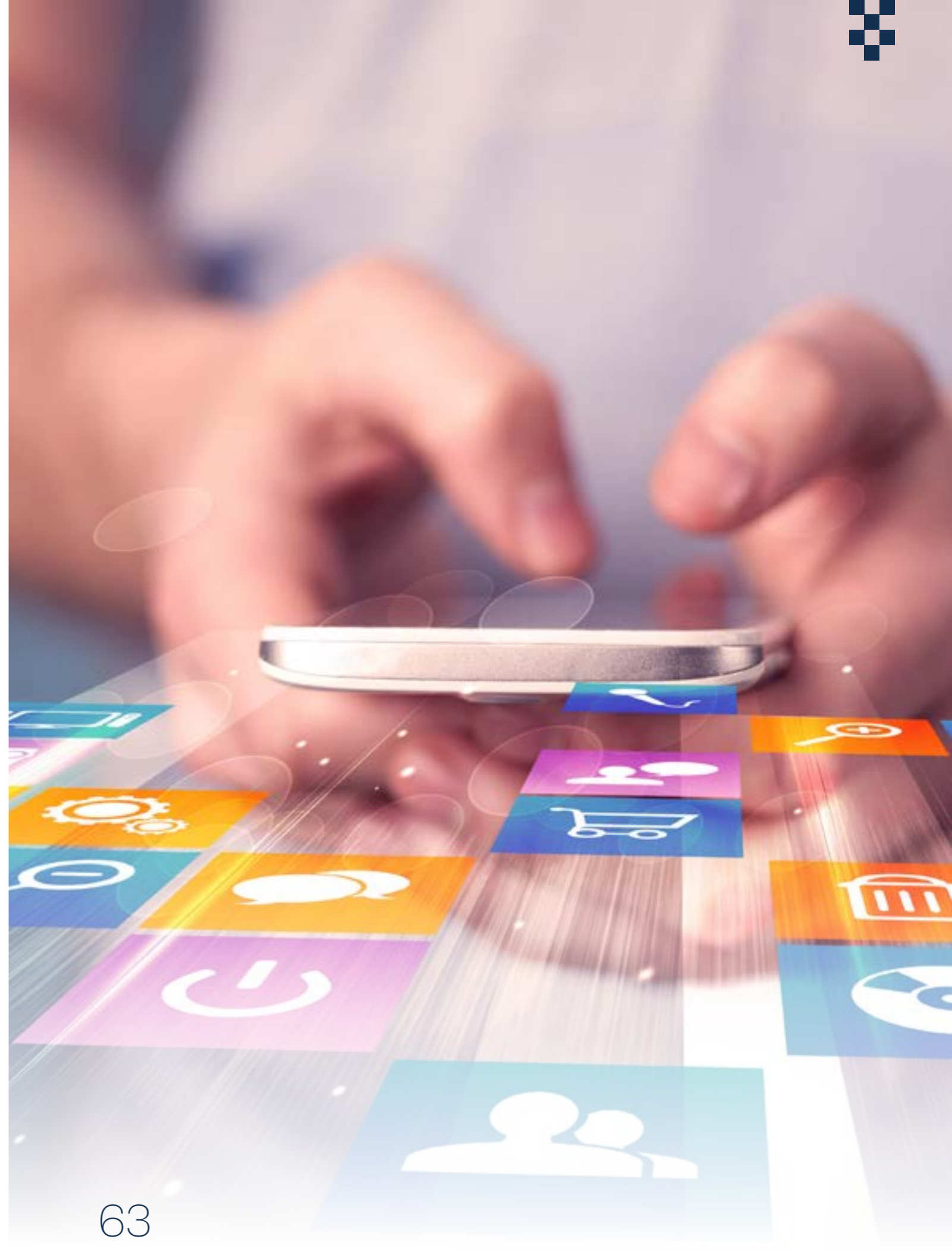
Gallai troseddwr gael mynediad at yr ap sy'n cysylltu â'ch car. Gallent ddefnyddio'r ap hwn i dracio ble mae'r car, yn ogystal â defnyddio'r nodwedd cloi/datgloi i allu cael mynediad ffisegol i'r car.

**Noder** - Gallwch geisio diddymu hawl mynediad ap i gar drwy ddod o hyd i'r allwedd ailosod meistr yn y gosodiadau. Gallwch weld sut i wneud hyn yn llawlyfr y car.

Erbyn hyn, mae gan rai gwneuthurwyr ceir ap sy'n galluogi perchennog y car i gael ap ffôn clyfar sy'n cysylltu â'r car. Mae'r ap hwn yn galluogi'r perchennog i gloi/datgloi cerbyd, gweld ble mae'r car, cychwyn/stopio o bell ac ati.

Mewn achosion lle y byddwch yn defnyddio'r math hwn o ap, dylech newid manylion mewngofnodi'r cyfrif sy'n cysylltu â'r car. Mae apiau ffôn clyfar i'w cael sy'n galluogi mwy nag un person i gael mynediad at yr un car, a gall hyn fod yn broblem o ran tracio lleoliad y car a chael mynediad ffisegol iddo. Dylech sicrhau mai dim ond eich dyfais chi sy'n cysylltu â'r car.

- FordPass – gallwch gael sawl defnyddiwr ar FordPass, a bydd angen i bob defnyddiwr fod â Rhif Adnabod Cerbyd (VIN) a'i roi i mewn i'r ap. I ddileu defnyddiwr, gellir ailosod y gosodiadau cysylltedd neu ailosod i'r gosodiadau meistr.
- Remote Connect (Toyota) – mae'r ap hwn yn galluogi perchennog car i weld ble y cafodd ei gerbyd ei barcio ddiwethaf. Mae'n galluogi'r defnyddiwr penodedig i awdurdodi gyrrwr arall i ddefnyddio Remote Connect ar gyfer ei gerbyd. I atal defnyddiwr rhag cael mynediad i Remote Connect > tapiwch 'Remove Driver' ar brif ap dashfwrdd y cerbyd.
- Mae BMW, Audi, Volvo, Mini, Volkswagen a llawer o geir eraill bellach yn cynnig apiau sy'n cysylltu â ffonau clyfar ac sy'n galluogi person i wybod ble mae ei gerbyd. Mae hyn yn rhywbeth i'w ystyried wrth ymdrin ag achosion lle roedd/mae perthynas rhyngoch chi a'r troseddwr.



## Rhan Pedwar: Canllawiau ar gyfer Adloniant Ar-lein

Mathau amrywiol o gynnwys, fel ffilmiau, rhaglenni teledu, cerddoriaeth, gemau, a ffrydiau byw dros y rhynggrwyd.



### Chwarae gemau

Chwarae gêm fideo electronig, a hynny'n aml ar gonsol gemau, cyfrifiadur neu ffôn clyfar.

Gall troseddwr gysylltu â chi, neu eich plant (os bydd hynny'n berthnasol) drwy lwyfannau chwarae gemau. Bydd troseddwr yn aml yn defnyddio'r plant sydd gan y ddau ohonoch i'ch cyrraedd chi. Gallai hyn beri risg mewn gemau sy'n cynnig ystafell sgwrsio ar-lein. Mae'n bosibl y gallai'r troseddwr greu cyfrif ffug a cheisio siarad â chi neu eich plant (math o swyno drwy dwyll).

Os ydych chi'n hoffi chwarae gemau neu os oes gennych blant sy'n hoffi chwarae gemau, dylech sicrhau eu bod yn ddiogel fel na fydd y troseddwr yn gallu cysylltu â chi na chael gwybodaeth bersonol drwy gael mynediad at y cyfrif(on).

- Os oeddech yn rhannu cyfrifon chwarae gemau neu os mai'r troseddwr a greodd eich cyfrifon chwarae gemau, dylech greu rhai newydd. Yn ddefnyddol, dylai'r cyfrifon newydd gael eu creu gan ddefnyddio cyfeiriad e-bost newydd ar wahân i'ch cyfrif personol, a grëwyd yn benodol ar gyfer chwarae gemau.
- Wrth greu cyfrifon ar gyfer y cyfrif chwarae gemau newydd hwn, dylech sicrhau bod prawf dilysu dau gam ar waith hefyd. Dylech hefyd sicrhau bod y manylion adfer yn gysylltiedig â chi.
- Er mwyn atal y troseddwr rhag dod o hyd i'r plentyn drwy chwarae gemau ar-lein, ni ddylai enw na llun y cyfrifon â chi allu cael eu cysylltu â chi.

**Noder** - Mae ffurfweddiadau ar gael y gall rhiant eu gwneud er mwyn atal cyfrif plentyn rhag cael mynediad at sgwrsio llais ac anfon a derbyn negeseuon.

Mewn achosion lle mae gennych blant sy'n chwarae gemau, fe'ch cynghorir i roi gosodiadau rhieni ar waith. Mae'n bosibl y bydd y troseddwr wedi rhoi gosodiadau rhieni ar waith o'r blaen. Os felly, mae'n bosibl y bydd angen ystyried ailosod i'r gosodiadau ffatri, yn enwedig pan fydd angen creu cyfrifon newydd.



## Cyfrifon ffrydio (Netflix, Disney+, Amazon Prime ac ati)

Gwasanaethau sy'n cynnig amrywiaeth eang o raglenni teledu, ffilmiau, rhaglenni dogfen a mwy ar ddyfeisiau sydd â chysylltiad â'r rhyngwyd.

Gall y troseddwr ddefnyddio llwyfannau ffrydio i adael negeseuon i chi, a hynny drwy olygu enwau'r proffiliau yn yr adran 'Who's watching?'. Ar ben hynny, gall y troseddwr hefyd gael gwybodaeth bersonol amdanoch, fel eich cyfeiriad e-bost, eich rhif ffôn a'ch manylion bilio.

Os cafodd y cyfrif ei greu gan ddefnyddio eich cyfrif e-bost chi, dylech newid y cyfrinair ac allgofnodi'r cyfrif o bob dyfais. Rhoddir canllawiau isod:

### Amazon Prime video

Gallwch gadw'r cyfrif hwn yn ddiogel drwy ddilyn y camau canlynol:

- **Ailosodwch eich cyfrinair a defnyddiwch un cryf ac unigryw** - bydd eich cyfrif Prime Video yn gysylltiedig â'ch cyfrif Amazon. Rhaid i chi newid cyfrinair eich cyfrif Amazon er mwyn sicrhau bod Prime Video yn ddiogel. I wneud hyn, ewch i Amazon > hofrwch dros 'Accounts & Lists' yn y gornel dde uchaf a thapiwch 'Account' > tapiwch 'Login & Security' > mewngofnodwch i'ch cyfrif > dylai hyn fynd â chi i'r dudalen 'Login & Security', ac ar y dde i 'Password' tapiwch 'Edit' > teipiwch gyfrinair cryf a diogel.
- **Rhowch brawf dilysu dau gam ar waith** - dilynwch yr un camau â'r rhai a restrir uchod nes cyrraedd 'Password', wedyn tapiwch 'Advanced Security Settings' > tapiwch 'Get started' ar yr ochr dde i 'Two-Step Verification'.
- **Dilëwch unrhyw ddyfeisiau nad ydych yn eu hadnabod o'ch cyfrif Amazon** - i ddileu dyfeisiau o'ch cyfrif Amazon, ewch i Amazon > hofrwch dros 'Accounts & Lists' yn y gornel dde uchaf a thapiwch 'Content and Device' > mewngofnodwch i'ch cyfrif > tapiwch 'Devices' > dewiswch y dyfeisiau nad ydych yn eu hadnabod a thapiwch 'Deregister'.

### Netflix

Gallwch gadw eich cyfrif yn ddiogel drwy ddilyn y camau canlynol:

- **Ailosodwch eich cyfrinair a dewiswch gyfrinair newydd cryf ac unigryw** - gallwch newid eich cyfrif o dudalen eich cyfrif, neu gallwch anfon neges e-bost neu neges destun ailosod cyfrinair atoch chi eich hun.
- I ychwanegu, newid neu ddileu rhif ffôn o'ch cyfrif, ewch i'r dudalen 'Change phone number' > dilynwch y cyfarwyddiadau i gadarnhau pwy ydych chi. Wedyn, gallwch ychwanegu, golygu neu ddileu rhif ffôn.
- **Allgofnodwch o ddyfeisiau nad ydych yn eu defnyddio neu'n eu hadnabod** - gallwch naill ai allgofnodi o bob dyfais neu allgofnodi o ddyfeisiau penodol nad ydyn eu defnyddio neu eu hadnabod o'r dudalen 'Manage Access & Devices'.

### Now TV

Gallwch gadw'r cyfrif hwn yn ddiogel drwy ddilyn y camau canlynol:

- **Ailosodwch y cyfrinair a defnyddiwch un cryf ac unigryw** - i ddiweddarau eich cyfrinair ar gyfer NOW > ewch i'r adran 'Personal details' yn 'My Account' (mewngofnodwch os na fyddwch wedi gwneud hynny'n barod) > sgröliwch i lawr i 'Security details' a dewiswch 'Reset password' > rhowch eich cyfeiriad e-bost i mewn a dewiswch 'Continue' > cliciwch y ddolen yn eich negeseuon e-bost i ailosod eich cyfrinair.
- **Rheoli dyfeisiau** - ni allwch allgofnodi'r cyfrif hwn o un ddyfais unigol. Fodd bynnag, gallwch allgofnodi o BOB dyfais. I wneud hyn, ewch i'r adran 'Devices' yn 'MyAccount' > dewiswch 'Sign out of all devices'. Noder – bydd y ddyfais y byddwch yn ei defnyddio i allgofnodi yn parhau i fod wedi'i mewngofnodi, felly byddwch yn ei gweld yn eich rhestr o ddyfeisiau.

### Disney+

Gallwch gadw'r cyfrif hwn yn ddiogel drwy ddilyn y camau canlynol:

- **Ailosodwch y cyfrinair a defnyddiwch un cryf ac unigryw** - i ddiweddarau eich cyfrinair ar Disney+, ewch i DisneyPlus.com > dewiswch 'Log in' > Rhowch eich cyfeiriad e-bost i mewn a dewiswch 'Continue' > dewiswch 'Forgot Password' > chwiliwch am neges e-bost gan Disney+ a theipiwch y cod dilysu chwe digid i gadarnhau eich cyfeiriad e-bost > teipiwch eich cyfrinair newydd.
- **Rheoli dyfeisiau** - edrychwch dros y dyfeisiau ac allgofnodwch o unrhyw rai nad ydynt yn eu hadnabod. I wneud hyn, mewngofnodwch i Disney+ > dewiswch 'Profile' > 'Account' > o dan 'Access & Security' dewiswch 'Manage Devices' > dewiswch 'Log out' ar gyfer unrhyw ddyfeisiau nad ydych yn eu hadnabod.
- Hefyd, i allgofnodi o bob dyfais, dewiswch 'Access & Security' a thapiwch 'Log out of everywhere' > teipiwch y cyfrinair untro a gaiff ei anfon i'r cyfeiriad e-bost sy'n gysylltiedig â'r cyfrif Disney a thapiwch 'Confirm' > dewiswch 'Log out' er mwyn allgofnodi o bob sesiwn a phob ap.

I gael rhagor o ganllawiau ar gadw eich llwyfannau ffrydio'n ddiogel, ewch i'r tudalennau cymorth ar eu gwefannau.



## **Rhan Pump: Canllawiau ar gyfer llwybryddion Wi-Fi**

Teclyn sy'n anfon gwybodaeth o'r rhyngwyd i ddyfeisiau personol.

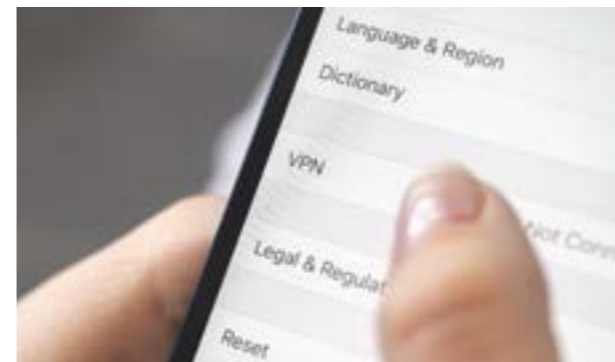


Sicrhewch fod eich llwybrydd yn gwbl ddiogel. Bydd hyn yn atal troseddwr rhag monitro eich traffig i mewn ac allan, ac yn eich galluogi i reoli'r hawliau mynediad sydd gan ddyfeisiau sydd wedi'u cysylltu â'r llwybrydd Wi-Fi hwnnw.

Newidiwch fanylion mewngofnodi eich cyfrif gweinyddwr. Mae'r camau ar gyfer gwneud hyn fel a ganlyn:

- Bydd angen i chi wybod y cyfrinair diofyn er mwyn ei newid. Fel arfer, bydd hwn i'w weld ar waelod y llwybrydd neu, fel arall, yn y ddogfennaeth a ddaeth gyda'r llwybrydd neu ar wefan y gwneuthurwr. (Mewn achosion lle bydd y troseddwr wedi newid y cyfrinair diofyn, bydd yn rhaid i chi ailosod y llwybrydd. Fel arfer, gellir gwneud hyn drwy ddal y botwm ailosod i lawr am 10-15 eiliad, neu fwy efallai, neu drwy ddefnyddio pin i bwysu'r botwm os yw ar y tu mewn i'r llwybrydd.)
- Teipiwch gyfeiriad IP rhyngwyneb gweinyddol y llwybrydd ym mar cyfeiriad y porwr gwe. (noder – ni fydd rhai llwybryddion yn galluogi newidiadau gweinyddol drwy gysylltiadau di-wifr, felly mae'n bosibl y bydd yn rhaid i chi gysylltu â'r llwybrydd gan ddefnyddio cebl Ethernet.)
- Rhowch enw defnyddiwr a chyfrinair eich llwybrydd. Ar ôl mewngofnodi, chwiliwch am dudalen y gosodiadau diogelwch a newidiwch fanylion eich cyfrif gweinyddwr. Sicrhewch fod y cyfrinair newydd yn gryf ac yn gymhleth.
- Edrychwch i weld beth yw eich gosodiadau amgryptio di-wifr** - WPA2 yw'r safon amgryptio y dylech ei defnyddio, yn hytrach na WPA, sy'n safon hŷn. Dylai WPA2 fod ar waith yn ddiogel, ond mae'n bosibl y bydd llwybryddion hŷn yn defnyddio'r protocol hŷn; Mae'n werth edrych i weld pa brotocol sydd wedi'i alluogi.

- Analluogwch fynediad o bell at y llwybrydd** - Bydd mynediad o bell at y llwybrydd yn galluogi unrhyw un nad yw wedi'i gysylltu'n uniongyrchol â'ch rhwydwaith Wi-Fi i gael mynediad at osodiadau'r llwybrydd. Gallwch analluogi mynediad o bell yng ngosodiadau gweinyddol y llwybrydd (isod ceir canllawiau ar sut i newid gosodiadau'r llwybrydd).
- Creu rhwydwaith Wi-Fi i westeion** - bydd y prif rwydwaith Wi-Fi yn rhoi mynediad i rywun at yr holl ddyfeisiau a ffeiliau sydd ar y rhwydwaith. Fodd bynnag, bydd rhwydwaith i westeion yn galluogi ymwelwyr i ddefnyddio'r rhyngwyd heb gyrraedd adnoddau lleol. Bydd hyn yn gwella diogelwch ac yn atal feirysau a allai ddod i mewn i'r rhwydwaith o ddyfais gwastai rhag lledaenu. I greu rhwydwaith i westeion:
  - Ewch i mewn i osodiadau eich llwybrydd** - eipiwch gyfeiriad IP eich llwybrydd mewn porwr gwe i agor ei osodiadau. (Os na fyddwch yn siŵr beth yw'r cyfeiriad IP, edrychwch ar gefn eich llwybrydd neu yn y llawlyfr).
  - Chwiliwch am y gosodiadau ar gyfer rhwydwaith i westeion** - Chwiliwch am y gosodiadau ar gyfer rhwydwaith i westeion ym mhanel gweinyddol eich llwybrydd.
  - Ffurweddwch y rhwydwaith i westeion** - Crëwch y rhwydwaith i westeion gan ddefnyddio enw (SSID) a chyfrinair unigryw. Sicrhewch fod yr SSID yn wahanol i SSID y prif rwydwaith, er mwyn gallu ei adnabod yn hawdd. Dylai'r cyfrinair fod yn un cryf er mwyn cadw'r rhwydwaith yn ddiogel.
  - Personolwch y gosodiadau** - Newidiwch y gosodiadau ar gyfer y rhwydwaith i westeion yn unol â'r hyn sy'n addas i chi.
  - Cadwch eich newidiadau a phrofwch y rhwydwaith** - Cadwch eich gosodiadau a phrofwch y rhwydwaith i westeion er mwyn sicrhau ei fod yn gweithio'n iawn.



## Rhwydweithiau Preifat Rhithwir (VPNs)

Mae rhwydweithiau preifat rhithwir yn diogelu eu defnyddwyr drwy amgryptio eu data a chuddio eu cyfeiriadau IP.

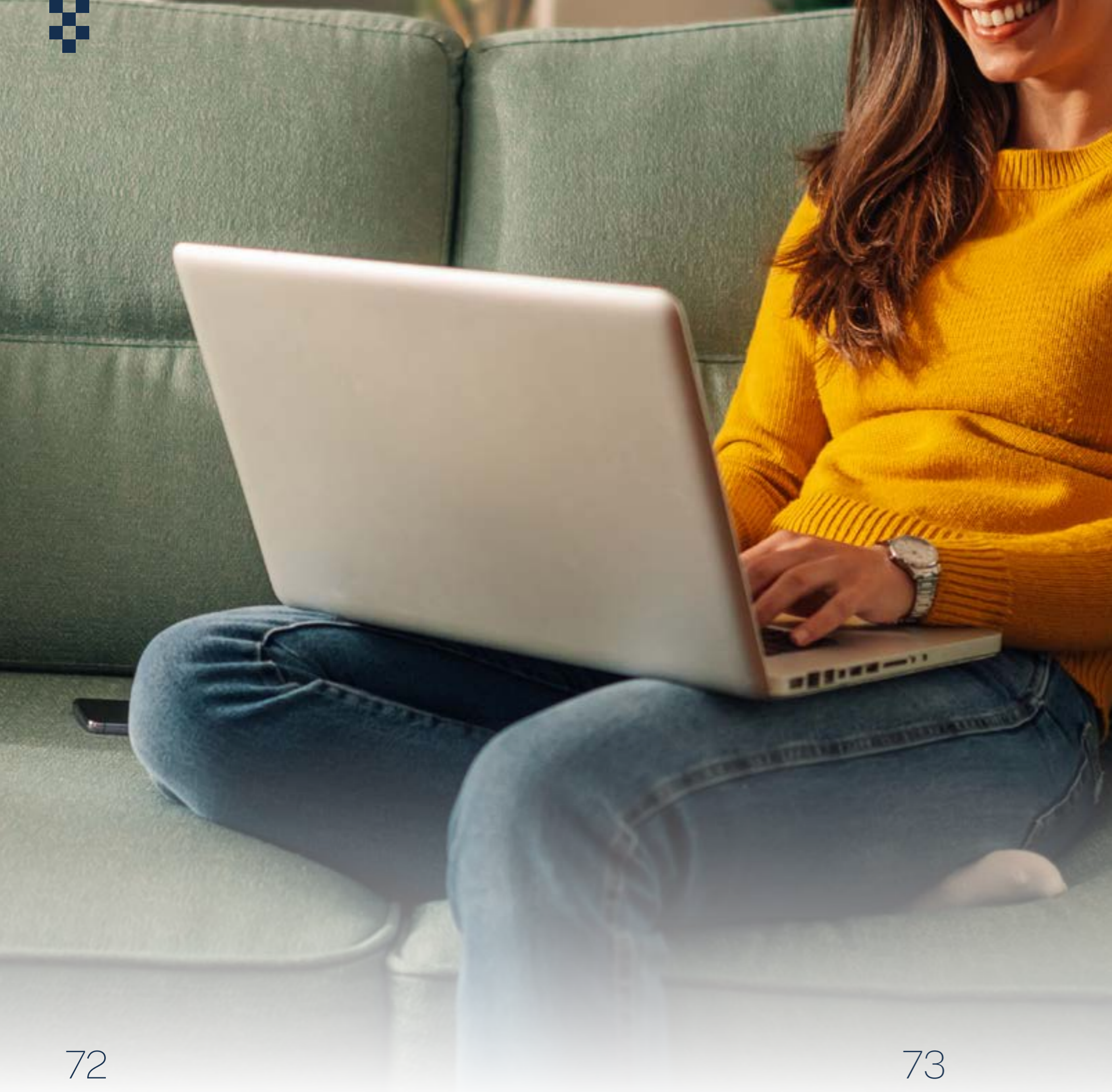
Os bydd gan droseddwr fynediad at eich llwybrydd Wi-Fi, byddant yn gallu gweld eich traffig i mewn ac allan, sef dull y byddant yn ei ddefnyddio i fonitro eich gweithgarwch ar y rhyngwyd. Hefyd, bydd eich holl draffig yn gysylltiedig â chyfeiriad IP, a fydd yn gallu cael ei ddefnyddio i ddangos eich lleoliad.

Mae defnyddio VPN yn fesur diogelwch y dylai pob unigolyn ei ddefnyddio, ond yn enwedig goreswyr seiberstelcio. Un o'r manteision mwyaf a gewch o ddefnyddio VPN yw y bydd yn rhoi lefel uwch o anhysbysrwydd i chi. Pan fyddwch yn cysylltu â VPN, caiff eich holl draffig ar-lein ei lwybro drwy dwnnel wedi'i amgryptio – bydd hyn yn ei wneud yn annarllenadwy i drydydd partion (gan gynnwys y troseddwr). Bydd hyn yn golygu y gallwch ddefnyddio'r rhyngwyd yn breifat ac yn ddiogel.

Bydd yn gweithio drwy ffugio eich cyfeiriad IP, sy'n golygu mai dim ond cyfeiriad IP gweinydd y VPN y byddwch wedi'i gysylltu ag ef y bydd y troseddwr/seiberstelciwr yn gallu ei weld. Bydd hyn yn cuddio eich lleoliad, gan eich amddiffyn rhag y troseddwr.

**Noder** - gellir defnyddio VPN ar bob dyfais – bydd hyn yn arbennig o fanteisiol os byddwch yn defnyddio mwy nag un ddyfais (sy'n wir am y rhan fwyaf o bobl). Hefyd, bydd hyn yn cynnig diogelwch ychwanegol i bobl sydd â phlant. Bydd hyn yn golygu na all troseddwr gael mynediad at wybodaeth drwy ddefnyddio dyfeisiau'r plant, fel lleoliad IP.

Gallwch ddod o hyd i fersiynau am ddim o VPNs sydd ar gael ar-lein, yn dibynnu ar y nodweddion y bydd eu heisiau arnoch, ac mae VPNs y codir tâl misol amdanynt ar gael hefyd. Cyn lawrlwytho VPN, cofiwch ddarllen y manylebau sydd i'w gweld ar wefan y gwneuthurwr yn ofalus a sicrhau ei fod yn wasanaeth dilys.



## **Rhan Chwech: Canllawiau ar gyfer Gliniaduron/ Cyfrifiaduron**



## Dyfeisiau Mac

Teulu o gyfrifiaduron personol wedi'u dylunio a'u marchnata gan Apple.

Gall troseddwr gael mynediad at eich gliniadur/cyfrifiadur o bell neu osod maleiswedd arno i'ch monitro. Mae'n bosibl y bydd hefyd am gael mynediad at eich ffeiliau preifat ar eich dyfais, yn enwedig ffeiliau sy'n gysylltiedig ag achos sy'n dal i fynd rhagddo yn ei erbyn. Hefyd, gallai chwilio am ffeiliau cyfrinachol fel cofnodion meddygol, a hyd yn oed ddileu ffeiliau.

Os oedd gan y troseddwr fynediad at eich gliniadur/cyfrifiadur o'r blaen, bydd angen i chi ystyried ambell beth fel rhagofal.

Dyfeisiau Mac – os oedd gan y troseddwr fynediad at eich gliniadur/cyfrifiadur o'r blaen, mae'n bosibl y gallai ffurfweddiadau a meddalwedd fod wedi cael eu gosod eu mwyn monitro/ysbio ar yr hyn a wnewch. Hyd yn oed os na fydd gan y troseddwr fynediad at y ddyfais ffisegol mwyach, nid yw hynny'n golygu na fydd yn gallu cael mynediad o bell. Dyma rai pethau i fwrw golwg drostynt ar ddyfais Mac:

74

## Mynediad o Bell

**Mewngofnodi o bell** - Gall cyfrifiaduron sy'n rhedeg ar system weithredu macOS fewngofnodi i'ch Mac gan ddefnyddio Secure Shell (SSH).

- Camau i'w cymryd i fwrw golwg dros y gosodiadau mewngofnodi o bell – dewislen Apple > System settings > General > Sharing > Remote login > os oes tic wrth ymyl 'Remote login', tynnwch y tic i ffwrdd.
- Os bydd unrhyw ddefnyddwyr nad ydych yn eu hadnabod yn y rhestr, gallwch eu dileu drwy fynd i'r rhestr > dewis y defnyddiwr > ac yna glicio'r botwm Remove.

**Remote desktop gyda rheoli o bell** - mae'n bosibl mewngofnodi i gyfrifiadur sy'n rhedeg ar macOS drwy alluogi Remote Desktop gyda rheoli o bell.

- Camau i'w cymryd i fwrw golwg dros y gosodiadau rheoli o bell – dewislen Apple > System settings > General > Sharing > Remote management > os oes tic wrth ymyl 'Remote management', tynnwch y tic i ffwrdd.
- Os bydd unrhyw ddefnyddwyr nad ydych yn eu hadnabod yn y rhestr, gallwch eu dileu drwy fynd i'r rhestr > dewis y defnyddiwr > ac yna glicio'r botwm Remove.

**Rhannu sgrin** - mae hefyd yn bosibl rhannu sgrin, a fydd yn galluogi unigolyn i weld sgrin rhywun mewn amser real.

- Camau i'w cymryd i fwrw golwg dros y gosodiadau rhannu sgrin – dewislen Apple > System settings > General > Sharing > Screensharing > os oes tic wrth ymyl 'Screensharing', tynnwch y tic i ffwrdd.
- Os bydd unrhyw ddefnyddwyr nad ydych yn eu hadnabod yn y rhestr, gallwch eu dileu drwy fynd i'r rhestr > dewis y defnyddiwr > ac yna glicio'r botwm Remove.

**Noder** - Os bydd dyfais Mac yn cael ei monitro, bydd yn dangos dau betryal yn y gornel dde uchaf yn agos at gloc y cyfrifiadur.

Gyda'r opsiynau mewngofnodi o bell a rhannu, byddai angen cyfrif/enw defnyddiwr ar droseddwr i fewngofnodi o bell. Er mwyn gweld yr holl ddefnyddwyr ar y Mac, gellir defnyddio gorchymyn ym modd terfynell Mac:

- **dscl . list /Users | grep -v '^\_'**
  - Os bydd unrhyw gyfrifon i'w gweld nad ydych yn eu hadnabod, mae'n bosibl mai'r troseddwr fydd wedi'u creu. Er mwyn gweld pryd y gwnaeth yr holl ddefnyddwyr fewngofnodi ddiwethaf, teipiwch last i mewn yn y modd terfynell. Bydd hyn yn rhestru dyddiadau ac amseroedd pob mewngofnodiad. Os bydd dyddiadau ac amseroedd anarferol ar gyfer cyfrif, mae'n bosibl bod rhywun yn mewngofnodi i'r ddyfais Mac o bell.

## Cofnodwyr bysellau

**Cofnodwyr bysellau masnachol** - mae'n bosibl y bydd troseddwr wedi gosod cofnodwr bysellau ar eich dyfais Mac er mwyn monitro'r hyn a wnewch (gall rhai cofnodwyr bysellau hyd yn oed dynnu sgrinluniau o'r bwrdd gwaith). Os byddwch yn credu bod y troseddwr yn eich monitro drwy eich Mac, mae ffyrdd posibl o edrych i weld a oes cofnodwyr bysellau wedi'u gosod.

- **Activity monitor** - dyma'r 'rheolwr tasgau' ar gyfer dyfeisiau Mac, a bydd yn eich galluogi i weld pa raglenni/offer sy'n rhedeg ar eich gliniadur/cyfrifiadur ar hyn o bryd. I agor Activity Monitor:
  - Applications > Utilities > chwiliwch am Activity Monitor a lansiwch ef.

75

- Gallwch edrych i weld a oes unrhyw raglenni/offer anhysbys yn rhedeg. Bydd enwau gwahanol i rai cofnodwyr bysellau yn Activity Monitor, felly ymchwiliwch i'r enw drwy chwilio amdano ar-lein ar ddyfais rydych chi'n gwybod ei bod yn ddiogel.
- **Edrych i weld beth yw'r cyfuniadau bysellau diofyn** - bydd gan gofnodwyr bysellau gyfuniad bysellau a fydd yn gwneud iddynt ymddangos ar y sgrin. Rhai cofnodwyr bysellau cyffredin:
  - Perfect keylogger: ctrl-alt-J
  - Elite Keylogger: ctrl-alt-S
  - Refog: option-shift-command-R
  - Spyrix: ctrl-alt-A
  - Revealer: ctrl-alt-F9

**Note** - These are default key combinations, the offender may have changed them.

- Edrych drwy'r rhestr o raglenni gan ddefnyddio Full Disk Access – rhaid i'r rhan fwyaf o gofnodwyr bysellau gael mynediad llawn at y disg neu hygyrchedd. I weld hyn: System preferences > Security & privacy > Privacy > Accessibility and Full disk access.

**Maleiswedd cofnodi bysellau** - mae gan system weithredu MacOS ei thechnoleg wrthfeirysau integredig ei hun o'r enw XProtect.

- Os bydd meddalwedd wrthfeirysau wedi dod o hyd i faleiswedd cofnodi bysellau, dylech chwilio am y feddalwedd/ffeiliau maleisus a'u dileu.



## Maleiswedd

Meddalwedd faleisus y gellir ei rhedeg ar ddyfais a gwneud iddi redeg cod sy'n gallu cyflawni gweithgareddau ar eich dyfais yw maleiswedd. Gall ysbïwedd (math o faleiswedd) ymddangos ar ddyfeisiau symudol a hefyd ar ddyfeisiau eraill, fel gliniaduron/cyfrifiaduron.

Gall troseddwr osod ysbïwedd ar eich dyfais Mac er mwyn monitro'r hyn a wnewch. Gellir gosod ysbïwedd naill ei drwy gael mynediad ffisegol at y ddyfais neu drwy glicio dolen mewn neges e-bost faleisus.

Enw'r amddiffyniad gwrth-faleiswedd integredig ar MacOS X yw XProtect. Mae'n sganio rhaglenni a ffeiliau am feirysau a maleiswedd gan ddefnyddio cronfa ddata y bydd Apple yn ei diweddarau'n ddyddiol. Os bydd yn dod o hyd i faleiswedd ar ffeil neu raglen, bydd yn rhoi gwybod i'r defnyddiwr ar unwaith ac yn rhwystro'r bygythiad.

### Er mwyn edrych i weld a yw XProtect wedi'i alluogi:

Apple > System settings > General > Software Update > Advanced > Cadarnhewch fod tic wrth ymyl 'Install system data files and security updates' neu 'Install security responses and system files' (yn dibynnu ar ba fersiwn o'r system weithredu sydd gennych).

Hefyd, bydd Mac Malware Removal Tool yn sganio'r system gyfan yn rheolaidd er mwyn gwneud yn siŵr nad oes dim byd wedi llithro heibio i XProtect. Os daw o hyd i unrhyw god maleisus, bydd yn ceisio ei analluogi ar unwaith.

**Noder** - Er bod nodweddion diogelwch Mac yn effeithiol, ni ddylai hynny eich atal rhag defnyddio offer trydydd parti ochr yn ochr ag XProtect.

## Canllawiau eraill ar gyfer dyfeisiau Mac:

**Sicrhewch fod y Wi-Fi yn ddiogel** - gall llwybrydd Wi-Fi unigolyn fod yn fan gwan a all gynnig mynediad at ei ddyfeisiau os na fydd wedi'i ddiogelu'n briodol. Mae canllawiau ar gadw llwybryddion Wi-Fi yn ddiogel i'w gweld ar dudalennau blaenorol..

**Edrychwch i weld beth sydd â mynediad at y microffon a'r camera** - edrychwch i weld pa apiau sy'n gallu cael mynediad at eich microffon a'ch camera.

- System preferences > Security & Privacy – Bydd rhestr o apiau'n ymddangos.
  - Cliciwch 'Camera' a 'Microphone' yn unigol er mwyn edrych i weld pa apiau sydd â hawl mynediad. Os bydd unrhyw apiau i'w gweld nad ydych yn eu hadnabod, bydd angen eu dileu.

**Sicrhewch fod diweddariadau awtomatig wedi'u galluogi** - dylai diweddariadau awtomatig fod wedi'u galluogi'n ddiodyn ar ddyfeisiau Mac, ond dylech edrych i wneud yn siŵr bod eich dyfais Mac yn eu lawrlwytho.

- System preferences > Software update > Advanced a sicrhewch fod tic ym mhob blwch.

**Gwnewch yn siŵr bod wal dân Mac wedi'i galluogi** - mae waliau tân yn canfod traffig maleisus ac yn amddiffyn eich dyfais rhagddo, a dylent fod wedi'u galluogi drwy'r amser. Er mwyn edrych i weld a yw eich wal dân wedi'i galluogi:

- Mac Settings > Network > Firewall

**Defnyddio porwr preifat a VPN** - mae system weithredu MacOS yn cynnwys ei phorwr preifat ei hun sy'n eich galluogi i fynd i wefannau a'u pori heb iddynt dracio eich gweithgarwch o un sesiwn i'r llall. Mae'r modd preifat hefyd yn sicrhau na chaiff tudalennau gwe eu storio yn iCloud. Mae hyn yn golygu na fydd y tudalennau y byddwch yn ymweld â nhw i'w gweld ar ddyfeisiau eraill a fydd wedi'u cysylltu ag iCloud. I bori'n breifat bob amser:

- Safari > Preferences > cliciwch 'General' > cliciwch 'Safari opens with' yna dewiswch 'a new private browser'.

Dylech hefyd sicrhau eich bod yn defnyddio VPN ar ddyfeisiau Mac. Meddyliwch yn ofalus cyn clicio neu osod unrhyw beth – os cewch neges destun, neges e-bost, neges ar y cyfryngau cymdeithasol neu unrhyw fath arall o neges sy'n edrych yn amheus, bydd angen i chi osgoi clicio unrhyw ddolenni. Fe'ch anogir i roi gwybod am negeseuon amheus i:

- Negeseuon testun - anfonwch nhw ymlaen i 7726
- Negeseuon e-bost - report@phishing.gov.uk

**Cyfrineiriau diogel** - crëwch gyfrinair cryf ar gyfer mewngofnodi i'ch dyfais Mac.

- Mewngofnodi awtomatig – sicrhewch fod mewngofnodi awtomatig wedi'i analluogi. Bydd hyn yn sicrhau na all neb gael mynediad i'r ddyfais (os caiff ei dwyn) a mewngofnodi'n syth.
- Clowch y ddyfais Mac yn awtomatig pryd bynnag y bydd yn segur – bydd hyn yn sicrhau na fyddai neb yn gallu cael mynediad i'r ddyfais Mac pe bai'n cael ei gadael heb oruchwyliaeth am ba reswm bynnag.

**Defnyddiwch reolwr cyfrineiriau (neu iCloud Keychain)** - er ei bod yn bwysig sicrhau bod y cyfrinair ar gyfer eich dyfais Mac yn gryf ac yn ddiogel, mae'n hollbwysig gosod cyfrineiriau diogel ar eich cyfrifon eraill hefyd. Oherwydd hyn, mae'n aml yn gallu bod yn anodd cofio'r holl gyfrineiriau (a dyma pam y bydd y rhan fwyaf o bobl yn defnyddio'r un cyfrineiriau ar gyfer eu holl gyfrifon). Mae iCloud Keychain yn cadw manylion mewngofnodi, cyfrineiriau a gwybodaeth am gardiau talu ac yn eu storio'n ddiogel gan ddefnyddio amgryptio AES. I osod hyn ar ddyfais Mac:

- Dewislen Apple > System preferences > cliciwch eich enw > cliciwch Cloud > Trowch Passwords & Keychain ymlaen.

**Noder** - Mae rheolwyr cyfrineiriau allanol ar gael y gellir eu defnyddio ar wahanol systemau gweithredu (OS). Gall hyn fod yn ddefnyddiol os bydd gennych amrywiaeth o wahanol ddyfeisiau OS.

**Crëwch allwedd mynediad** - ffordd o fewngofnodi i gyfrif ap neu wefan heb fod angen creu a chofio cyfrinair yw allwedd mynediad. Bydd allwedd mynediad yn defnyddio Touch ID neu Face ID i'ch adnabod chi.

**Galluogwch brawf dilysu dau gam iCloud** - bydd hyn yn cynnig haen ychwanegol o ddiogelwch lle y bydd gofyn i chi fewnbynnu cod untro a grëwyd ar hap ynghyd â chyfrinair eich cyfrif pan fyddwch yn ceisio mewngofnodi i'ch cyfrifon. I osod hyn:

- System settings > Apple ID > Password & security > cliciwch 'Two-Factor Authentication' > wedyn gofynnir i chi roi eich rhif ffôn er mwyn i'r cyfrinair untro gael ei anfon iddo.

**Crëwch gyfrifon nad ydynt yn gyfrifon gweinyddwr** - fel rhagofal diogelwch, dylech greu cyfrif defnyddiwr safonol i'w ddefnyddio pan na fydd angen hawliau gweinyddwr (rheoli a dileu defnyddwyr, gosod a thynnu meddalwedd a newid gosodiadau). Pe bai troseddwr yn cael mynediad i'ch cyfrifiadur, byddai hyn yn cyfyngu ar y posibilrwydd o gamweithredu. Er enghraifft, pe bai'r troseddwr am osod ysbïwedd, ni fyddai'n gallu gwneud hynny heb hawliau gweinyddwr. I ychwanegu defnyddiwr neu grŵp ar ddyfeisiau Mac:

- Dewislen Apple > Settings > cliciwch 'Users & Groups' > 'Add user' o dan y rhestr o ddefnyddwyr ar y dde (mae'n bosibl y gofynnir i chi roi eich cyfrinair) > New user > dewiswch y math o ddefnyddiwr a dilynwch y cyfarwyddiadau.



## Dyfeisiau Windows

Cyfes o systemau gweithredu wedi'u datblygu a'u marchnata gan Microsoft.

Gall troseddwr gael mynediad at eich gliniadur/cyfrifiadur o bell neu osod maleiswedd arno i'ch monitro. Mae'n bosibl y bydd hefyd am gael mynediad at eich ffeiliau preifat ar eich dyfais, yn enwedig ffeiliau sy'n gysylltiedig ag achos sy'n dal i fynd rhagddo yn ei erbyn. Hefyd, gallai chwilio am ffeiliau cyfrinachol fel cofnodion meddygol, a hyd yn oed ddileu ffeiliau.

Dyfeisiau Windows – os oedd gan y troseddwr fynediad at eich gliniadur/cyfrifiadur o'r blaen, mae'n bosibl y gallai ffurfweddiadau a meddalwedd fod wedi cael eu gosod eu mwyn monitro/ysbio ar yr hyn a wnewch. Hyd yn oed os na fydd gan y troseddwr fynediad at y ddyfais ffisegol mwyach, nid yw hynny'n golygu na fydd yn gallu cael mynediad o bell. Dyma rai pethau i fwrw golwg drostynt ar ddyfais Windows:

### Mynediad o Bell

- Os byddwch yn credu bod arwyddion o fynediad o bell, y peth cyntaf y dylech ei wneud yw datgysylltu'r ddyfais o'r rhyngwyd.

**Noder** - Er mwyn i droseddwr allu gosod Microsoft Remote Desktop Connection (RDC), bydd yn rhaid i'ch dyfais fod yn rhedeg ar Windows 10 Pro neu Enterprise / Windows 11 Pro neu Enterprise.

Edrychwch i weld pa fersiwn sy'n rhedeg ar eich dyfais ac, os na fyddwch yn siŵr, gallwch gael gwybod drwy ddilyn y camau canlynol: Settings > System > About > Windows specifications.

Os bydd y manylebau hyn gennych, dylech edrych i weld a yw RDC wedi'i alluogi drwy ddilyn y camau canlynol:

- Settings > System > Remote Desktop > os bydd tic wrth ymyl 'Enable Remote Desktop', tynnwch y tic.
- Os bydd RDC wedi'i alluogi, o dan 'User accounts' ar y dudalen 'Remote Desktop', cliciwch 'Select users that can remotely access this PC'. Os bydd unrhyw gyfrifon defnyddwyr anghyfarwydd neu ddeisiau wedi'u rhestru yn y blwch, cliciwch y defnyddiwr ac yna cliciwch 'Remove'.

Un peth arall i'w sicrhau yw bod Windows Firewall yn rhwystro'r porth ar gyfer Remote Desktop, sef mesur diogelwch ychwanegol y byddai'r troseddwr wedi'i analluogi o bosibl pe bai wedi gosod RDC. Er mwyn edrych i weld a yw'r wal dân yn rhwystro RDC:

- Settings > chwiliwch am 'Windows Defender Firewall' > ar yr ochr chwith, cliciwch 'Allow and app or feature through Windows Defender Firewall' > wedyn byddwch yn gweld rhestr o'r holl apiau y caniateir iddynt gyfathrebu drwy Windows Firewall. Ar ôl i chi ddod o hyd i'r rheolau ar gyfer Remote Desktop (dylai fod tair – 'Shadow (TCP)', 'User Mode (TCP-in)' ac 'User Mode (UDP-in)'), de-gliciwch ar bob un > cliciwch 'disable'.

Dylid nodi hefyd y gallai'r troseddwr fod wedi gosod rhaglen allanol ar gyfer cael mynediad o bell. Er mwyn edrych i weld hyn, ewch i 'Task Manager' ac edrychwch drwy'r rhestr o raglenni sy'n rhedeg ar hyn o bryd gan chwilio am unrhyw rai amheus neu anghyfarwydd. Ymhlith yr offer mynediad o bell a all fod wedi cael eu gosod heb eich caniatâd mae: VNC, RealVNC, RemotePC, LogMeIn, GoToMyPC, ZoHo Assist a TeamViewer.

- Os gwelwch fod rhaglen mynediad o bell yn rhedeg, bydd angen i chi eu dadosod. Gellir gwneud hyn drwy ddilyn y camau canlynol:
  - Settings > Apps > Apps & features > chwiliwch am yr ap yr hoffech ei dynnu > dewiswch 'More' > Uninstall.

### Cofnodwyr bysellau

**Cofnodwyr bysellau masnachol** - mae'n bosibl y bydd troseddwr wedi gosod cofnodwr bysellau ar eich dyfais Windows er mwyn monitro'r hyn a wnewch (gall rhai cofnodwyr bysellau hyd yn oed dynnu sgrinluniau o'r bwrdd gwaith). Os byddwch yn credu bod y troseddwr yn eich monitro drwy eich dyfais Windows, mae ffyrdd posibl o edrych i weld a oes cofnodwyr bysellau wedi'u gosod:

- Task manager** - dyma'r ffordd gyflym gyntaf o edrych i weld a oes cofnodwr bysellau'n rhedeg yn y cefndir ar eich dyfais Windows. I wneud hyn, ewch i Task Manager > Processes > More details (ar waelod y tab) > yma fe welwch yr holl apiau a raglenni sy'n rhedeg.
  - Gallwch edrych i weld a oes unrhyw raglenni/offer anhysbys yn rhedeg. Bydd enwau gwahanol i rai cofnodwyr bysellau yn Activity Monitor, a gallwch ymchwilio i'r enw drwy chwilio amdano ar-lein ar ddyfais rydych chi'n gwybod ei bod yn ddiogel. Os gwelwch unrhyw raglenni rhyfedd/ anhysbys, de-gliciwch arnynt > dewiswch 'End Task'.
  - Hefyd, dylech edrych drwy 'Startup apps' yn Task Manager (bydd hyn i'w weld ar ochr

chwith y tab) – bydd hyn yn dangos yr holl apiau a fydd yn dechrau pan fydd rhywun yn mewngofnodi i'r ddyfais Windows.

Os gwelwch unrhyw apiau y gwyddoch mai cofnodwyr bysellau ydynt neu apiau sy'n edrych yn amheus, de-gliciwch arnynt > dewiswch 'Disable'.

- Rhaglenni a Nodweddion** - bydd hyn yn eich galluogi i weld yr holl raglenni ar eich dyfais Windows. Gellir gwneud hyn drwy ddilyn y camau canlynol:
  - Control panel > programmes > programmes and features > bydd hyn yn eich galluogi i weld yr holl raglenni sydd ar eich dyfais Windows. Os gwelwch unrhyw raglen y gwyddoch mai cofnodwr bysellau ydyw neu unrhyw beth sy'n edrych yn amheus neu'n anhysbys, de-gliciwch arni > Uninstall.
- Edrychwch drwy'r ffeiliau dros dro** - mae'n bosibl y bydd cofnodwyr bysellau weithiau'n cuddio mewn ffeiliau dros dro er mwyn osgoi cael eu darganfod. Mae'r ffeiliau dros dro yn lle da i raglenni amheus guddio am eu bod mor anhrefnus. Gallwch edrych drwy'r ffeiliau hyn drwy ddilyn y camau canlynol:
  - Settings > System > Storage > cliciwch Temporary files (bydd hyn yn dangos yr holl gynnwys) > chwiliwch am y ffeiliau sy'n edrych yn amheus ac yna pwyswch 'Remove files'.
- Windows Defender** - bydd y rhaglen hon yn canfod cofnodwyr bysellau ac unrhyw faleiswedd arall. I sicrhau bod y nodwedd canfod feirysau a bygythiadau wedi'i galluogi:
  - Windows settings > Update & Security > o dan 'Protection areas' cliciwch 'Virus & threat protection' > Manage settings > trowch 'Real-time protection' ymlaen.



## Maleiswedd:

Meddalwedd faleisus y gellir ei rhedeg ar ddyfais a gwneud iddi redeg cod sy'n gallu cyflawni gweithgareddau ar eich dyfais yw maleiswedd. Gall ysbïwedd (math o faleiswedd) ymddangos ar ddyfeisiau symudol a hefyd ar ddyfeisiau eraill, fel gliniaduron/cyfrifiaduron.

Gall troseddwr osod ysbïwedd ar eich dyfais Windows er mwyn monitro'r hyn a wnewch. Gellir gosod ysbïwedd naill ei drwy gael mynediad ffisegol at y ddyfais neu drwy glicio dolen mewn neges e-bost faleisus.

I ddefnyddwyr Windows, mae Microsoft Defender Antivirus yn adnodd effeithiol sy'n canfod ac yn dileu maleiswedd ar ddyfais Windows. I sganio dyfais Windows a dileu maleiswedd:

Windows security > Virus & threat protection > scan options > dewiswch 'offline scan' > cliciwch 'Scan now'.

**Noder** - Er bod Microsoft Defender yn adnodd effeithiol, ni ddylai hynny eich atal rhag defnyddio offer trydydd parti ochr yn ochr â Microsoft Defender.

## Canllawiau eraill ar gyfer dyfeisiau Windows

**Sicrhewch fod Windows Defender wedi'i osod yn iawn** - rhaglen wrthfeirysau integredig sydd ym mhob fersiwn o Windows yw Microsoft Defender. Mae'n cynnig amddiffyniad amser real yn erbyn mathau o faleiswedd (gan gynnwys ysbïwedd). Esbonnir uchod sut i sicrhau bod Windows Defender wedi'i alluogi. Er bod Windows 10 ac uwch yn diweddarur ddyfais ac yn ei sganio am faleiswedd yn rheolaidd, gallwch gynnal sganiau gwahanol eich hun:

- **Sgan llawn am feirysau** - Windows security > Virus & threat protection > o dan 'current threats' cliciwch 'scan options' > Full scan > cliciwch 'Scan now'.
- **Sgan all-lein am feirysau** - os byddwch yn credu bod ysbïwedd ar eich dyfais o bosibl, gallwch gynnal sgan all-lein er mwyn canfod a dileu maleiswedd anodd ei thrin. Y rheswm dros hyn yw nad oes modd dileu rhai mathau o faleiswedd tra bydd Windows yn rhedeg. I ddechrau sgan all-lein:
  - Windows Security > Virus & threat protection > o dan 'current threats' cliciwch 'Scan options' > Microsoft Defender Offline > cliciwch 'Scan now' > Scan.
- **Microsoft defender firewall** - dylech sicrhau bod eich wal dân wedi'i throi ymlaen drwy'r amser, felly i gadarnhau hyn, dilynwch y camau canlynol:
  - Settings > Update & security > Windows Security > Firewall & network protection > cliciwch 'Turn on'.
- **Amddiffyniad seiliedig ar enw da** - rhagofal diogelwch ychwanegol y gallwch ei roi ar waith yw hwn, ac mae'n gwerthuso i ba raddau y gellir ymddiried mewn meddalwedd a rhaglenni. Os bydd yn canfod ffeil, meddalwedd neu raglen sy'n cael ei



lawrlwytho ac sydd â sgôr enw da isel, bydd y system yn rhybuddio'r defnyddiwr. Bydd yn rhoi opsiynau i'r defnyddiwr, sef rhwystro'r ffeil, ei rhoi mewn cwarantyn, neu ei chaniatáu dan amodau penodol. I alluogi hyn:

- Settings > Privacy & security > Windows security > App & browser control > trowch ef ymlaen.

### Cynhaliwch archwiliad caniatadau a hawliau mynediad

- mae gan ddyfeisiau Windows osodiadau caniatâd er mwyn atal rhaglenni rhag cael mynediad at ddata penodol (gan gynnwys cysylltiadau, lleoliad, camera, microffon ac ati). Dylech fwrw golwg dros eich caniatadau apiau yn rheolaidd er mwyn sicrhau nad oes rhaglenni'n rhoi mwy o ganiatadau nag sy'n angenrheidiol. I weld y caniatadau hyn:

- Settings > Privacy (neu Privacy & security yn Windows 11) > sgrolwch i lawr i'r adran 'App permissions' > ewch drwy'r caniatadau i weld pa apiau sydd â mynediad at ddata nad oes eu hangen arnynt.

**Defnyddiwr borwr preifat a VPN** - pan gaiff tabiau neu ffenestri InPrivate eu defnyddio, ni chaiff data pori (e.e. hanes, ffeiliau rhynggrwyd dros dro a chwcis) eu cadw ar eich dyfais Windows ar ôl i chi orffen. I agor ffenestr InPrivate:

- Microsoft Edge > Settings and More > cliciwch 'New InPrivate window'.

Mae VPNs yn fesur diogelwch ychwanegol a fydd yn gwella preifatrwydd ar-lein ac yn cuddio cyfeiriad IP y defnyddiwr. Mae rhagor o wybodaeth am VPNs i'w chael ar dudalen 80.

**Sicrhewch fod y Wi-Fi yn ddiogel** - gall llwybrydd Wi-Fi fod yn fan gwan a all gynnig mynediad at eich dyfeisiau os na fydd wedi'i ddiogelu'n briodol. Mae canllawiau ar gadw llwybryddion Wi-Fi yn ddiogel i'w gweld ar dudalennau blaenorol.

**Cyfrineiriau diogel** - dylech sicrhau eich bod yn creu cyfrinair cryf ar gyfer mewngofnodi i'ch dyfais Windows.

- Dylech hefyd sicrhau fod mewngofnodi awtomatig wedi'i analluogi. Bydd hyn yn sicrhau na all neb gael mynediad i'r ddyfais (os caiff ei dwyn) a mewngofnodi'n syth.

### Crëwch gyfrifon nad ydynt yn gyfrifon gweinyddwr

- fel rhagofal diogelwch, dylech greu cyfrif defnyddiwr safonol i'w ddefnyddio pan na fydd angen hawliau gweinyddwr (rheoli a dileu defnyddwyr, gosod a thynnu meddalwedd a newid gosodiadau). Pe bai troseddwr yn cael mynediad i'ch cyfrifiadur, byddai hyn yn cyfyngu ar y posibilrwydd o gamweithredu. Er enghraifft, pe bai'r troseddwr am osod ysbïwedd, ni fyddai'n gallu gwneud hynny heb hawliau gweinyddwr.

- Settings > Accounts > Family & other users > ar yr ochr dde, cliciwch 'Add someone else to this PC'.



## Rhan Saith: Canllawiau ar Wneud Copïau wrth Gefn o'ch Data

Copi o'ch data pwysig a gaiff ei storio  
mewn lleoliad diogel ar wahân.



## Canllawiau ar Wneud Copïau wrth Gefn o'ch Data

Copi o'ch data pwysig a gaiff ei storio mewn lleoliad diogel ar wahân.

Mae'n bosibl y gallai'r troseddwr gael mynediad at unrhyw ddata y byddwch yn gwneud copïau wrth gefn ohonynt gan ddefnyddio'r cwmwl os bydd yn gwybod eich manylion mewngofnodi. Gall hyn fod yn risg fawr os byddwch wedi bod yn casglu tystiolaeth o'i ymddygiad a'i weithredoedd.

Caiff copïau wrth gefn o ddata eu storio ar y rhyngwrwyd (storfa gwmwl) neu ar ddyfeisiau caledwedd (cofau bach USB, cardiau SD neu yriannau caled). Pan fyddwch yn gwneud copi wrth gefn o'ch data, hyd yn oed os byddwch yn colli mynediad at y data gwreiddiol, bydd bodd eu hadfer gan ddefnyddio'r copi wrth gefn.

Y rhesymau pam y dylem wneud copïau wrth gefn o'n data:

- Pan fyddwn yn cael dyfeisiau newydd ac am gopïo ffeiliau sydd gennym eisoes iddynt.
- Pan fydd dyfais yn mynd ar goll neu'n cael ei dwyn.
- Pan fydd dyfais sydd â data pwysig arni yn torri.
- Pan gaiff data ar ein dyfeisiau eu dileu ar ddamwain.
- Pan fydd feirws ar ein dyfais.

Er mai rhain yw'r rhesymau pam y bydd pob un ohonom yn gwneud copïau wrth gefn o'n data, bydd gan oroeswyr stelcio ac aflonyddu digidol resymau ychwanegol. Mae'n hollbwysig eich bod yn cadw tystiolaeth y gellir ei defnyddio yn erbyn y troseddwr er mwyn helpu eich achos yn ei erbyn.

Oherwydd hyn, mae'n hanfodol eich bod yn gwneud copïau wrth gefn o'ch data er mwyn sicrhau y caiff y dystiolaeth ei chadw mewn lle diogel bob amser hyd yn oed os bydd y troseddwr yn llwyddo i gael gafael ar eich dyfeisiau, neu am y rheswm y sonnir amdano uchod.

### Sut i wneud copïau wrth gefn o ddata

Mae'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC, 2024) yn cynnig canllawiau ac awgrymiadau ar sut y dylai pobl wneud copïau wrth gefn o'u data:

#### Storio cwmwl

Mae'r rhan fwyaf o bobl yn defnyddio cynhyrchion Apple, Google neu Microsoft (Windows) sy'n cynnwys nodweddion storio cwmwl. Gyda'r cyfrifon hyn, caiff hyn a hyn o storfa cwmwl ei rhoi i'r defnyddiwr am ddim,

ac mae'n bosibl y bydd yn ddigon i gadw'r holl ffeiliau pwysig (bydd modd uwchraddio er mwyn cael mwy o le storio os bydd angen).

**Apple iCloud** - bydd ffeiliau a ffolderi y byddwch yn eu storio yn iCloud Drive yn aros yn gyfredol ar bob un o'ch dyfeisiau.

- **I osod iCloud ar iPhone ac iPad** - Settings > tapiwch eich enw > tapiwch iCloud > o dan 'Apps using iCloud, trowch iCloud Drive ymlaen.
- **I osod iCloud ar eich Mac** - dewislen Apple > System preferences > cliciwch eich enw > cliciwch iCloud (mewngofnodwch gan ddefnyddio eich Apple ID os gofynnir i chi wneud hynny) > o dan 'Apps using iCloud', cliciwch iCloud Drive > trowch 'Sync this Mac' ymlaen.
  - I ychwanegu'r ffeiliau o fwrdd gwaith Mac a'ch ffolder 'Documents' at iCloud Drive > trowch 'Desktop and Documents' ymlaen.
- **I osod iCloud ar eich dyfais Windows** - pan fydd iCloud wedi'i osod ar eich dyfais Apple > lawrlwythwch 'iCloud for Windows' ar eich dyfais Windows o'r Microsoft Store > agorwch iCloud for Windows > mewngofnodwch gan ddefnyddio eich Apple ID > ar y dde i iCloud Drive, cliciwch y botwm saeth > trowch 'iCloud Drive' ymlaen.

**Google Drive** - gallwch wneud copïau wrth gefn o gynnwys, data a gosodiadau o'ch ffôn yn eich cyfrif Google.

- **I osod Google Drive ar ddyfais Android** - Settings > Google > Backup (os mai hwn yw'r tro cyntaf, trowch 'Backup by Google One' ymlaen a dilynwch y cyfarwyddiadau) > tapiwch 'Back up now'.
  - Gall Google One gymryd hyd at 24 awr. Pan fydd data'n cael eu cadw, bydd 'On' i'w weld o dan y mathau o ddata y gwnaethoch eu dewis.
- **I osod Google Drive ar ddyfais Mac neu Windows** - lawrlwythwch Google Drive ar eich dyfais Windows neu Mac (bydd dolenni i'w lawrlwytho i'w gweld ar

dudalen we Google Drive) > ar eich dyfais, agorwch GoogleDriveSetup.exe (Windows) neu GoogleDrive.dmg (Mac) > dilynwch y cyfarwyddiadau i gwblhau'r broses.

#### Microsoft OneDrive

- Eicon cwmwl OneDrive > eicon 'Help & settings icon > Settings > cliciwch 'Sync and back up' > dewiswch 'Manage back up' > i ddechrau gwneud copïau wrth gefn o ffeiliau, toglwch unrhyw ffolderi sy'n dweud 'Not backed up' > dewiswch 'Save changes'.

Os byddwch yn defnyddio darparwr cwmwl gwahanol, ewch i'w wefan i gael cyfarwyddiadau ar sut i wneud copïau wrth gefn o ddata.

**Note** - Sicrhewch eich bod yn diogelu eich cyfrifon cwmwl drwy ddefnyddio cyfrineiriau cryf a throi prawf dilysu dau gam ymlaen. Bydd hyn er mwyn atal mynediad heb awdurdod at eich copïau wrth gefn.

**Cyfringau y gellir eu tynnu** - mewn achosion lle y byddwch yn creu copïau wrth gefn arbennig o fawr, fe'ch cynghorir i ddefnyddio cyfringau y gellir eu tynnu i wneud copïau wrth gefn o ffeiliau a ffolderi.

Gallwch wneud copïau wrth gefn o'ch data i'r cyfringau canlynol:

- Gyriant caled allanol
- Cof bach USB
- Cardiau SD

**Note** - Pan na fydd cyfringau y gellir eu tynnu'n cael eu defnyddio, dylid eu datgysylltu o'r ddyfais y maent yn gwneud copïau wrth gefn ohoni. Bydd hyn er mwyn atal feirysau posibl ar y ddyfais rhag canfod eu ffordd i'r cyfringau y gellir eu tynnu hefyd.

Mewn achosion lle y byddwch yn casglu ac yn cadw tystiolaeth i'w defnyddio yn erbyn y troseddwr, bydd defnyddio'r cwmwl a chyfringau y gellir eu tynnu i storio'r dystiolaeth yn rhoi sicrwydd ychwanegol i chi ynglŷn â'r posibilrwydd o golli'r data.

## Rhan Wyth:

# Canllawiau ar gyfer Dyfeisiau Clyfar/y Rhyngrwyd Pethau

Rhwydwaith o ddyfeisiau cysylltiedig a thechnoleg sy'n galluogi dyfeisiau a'r cwmwl i gyfathrebu â'i gilydd yw'r Rhyngrwyd Pethau.



## Gwylidwriaeth Cloch Drws

Mae clychau drws fideo yn eich galluogi i sgwrsio o bell ag ymwelwyr a chadw llygad ar nwyddau a gaiff eu danfon o sgrin eich ffôn clyfar. Pan fydd y clychau drws hyn yn dechrau recordio, byddant yn anfon rhybudd atoch ar unwaith.

Gall troseddwr ddefnyddio eich gwylidwriaeth cloch drws i'ch monitro chi. Bydd yn gallu gweld pryd y byddwch yn gadael eich cartref ac yn dychwelyd, a'i defnyddio i weld pwy sy'n ymweld â chi hefyd. Ar ben hynny, gall y troseddwr ddefnyddio'r nodwedd microffon i siarad â chi.

**Noder** - Dylid nodi hefyd, ar gyfer unrhyw fath arall o wylidwriaeth awyr agored a all fod gennych, y dylech edrych i weld pa ddyfeisiau sydd wedi'u cysylltu â'r cyfrif a dileu unrhyw ddyfeisiau anghyfarwydd neu ddieisiau.

Os oes gennych wylidwriaeth cloch drws fel cloch drws Ring, er enghraifft, yna dylech edrych i weld pwy sydd â mynediad ati.

Gellir gwneud hyn drwy ddilyn y camau canlynol:

### Cloch drws Ring:

- Tapiwch y ddewislen ar y brig > Control centre > Authorized client devices.
  - Os bydd dyfeisiau ar y cyfrif yn edrych yn anghyfarwydd neu'n ddieisiau, gallwch ddileu un ar y tro neu bob un ar unwaith (ac eithrio'r ddyfais y byddwch yn ei defnyddio).
- Cofiwch newid y cyfrinair ar gyfer y cyfrif a rhoi prawf dilysu dau gam ar waith hefyd.
- Mewn achosion lle mai'r troseddwr a osododd y gloch drws Ring ac sydd â'r cyfrif gweinyddwr, dylech ailosod y ddyfais i'r gosodiadau ffatri. Bydd hyn yn golygu y gallwch greu eich cyfrif ar wahân eich hun er mwyn cysylltu â'r gloch drws Ring.

### Cloch drws fideo Blink:

- Settings > Account and Privacy > Manage mobile devices. Gallwch ddileu dyfeisiau anhysbys neu ddieisiau drwy glicio'r eicon bin sbwriel ac yna gadarnhau'r weithred pan ofynnir i chi wneud hynny.
- Yn debyg i gloch drws Ring, mae'n bosibl y bydd yn rhaid i chi ailosod cloch drws fideo Blink i'r gosodiadau ffatri os mai'r troseddwr sydd â'r cyfrif gweinyddwr.



## Dyfeisiau Alexa a/neu ddyfeisiau â nodweddion tebyg

Gall Alexa a dyfeisiau eraill ymateb i gwestiynau syml a chyflawni cyfresi cymhleth o dasgau er mwyn rhoi gwybodaeth, adloniant a chymorth cyffredinol i'w defnyddwyr.

Gall troseddwr gael mynediad at eich dyfais Alexa neu Google Home Nest (a dyfeisiau eraill tebyg) os bydd yn gwybod yr enw defnyddiwr a'r cyfrinair ar ei chyfer. Bydd troseddwr yn defnyddio'r dyfeisiau hyn i wrando ar sgysiau, a gallant hyd yn oed eu defnyddio i aflonyddu arnoch. Er enghraifft, gallent ddefnyddio'r nodwedd microffon i siarad â chi a hyd yn oed droi goleuadau ymlaen a'u diffodd.

Mae gan lawer o berchnogion cartrefi ddyfeisiau cartref clyfar fel Alexa a chynhyrchion tebyg erbyn hyn. Mewn llawer o achosion ledled y DU, bydd stelcwyr (cyn-bartneriaid fel arfer) yn defnyddio dyfeisiau Amazon Alexa yn gynyddol i godi braw ar bobl yn eu cartrefi eu hunain.

**Noder** - Mae'n bosibl y bydd troseddwr yn gwranddo ar sgysiau heb yn wybod i chi, felly fe'ch cynghorir i newid cyfrineiriau'r cyfrifon.

## Alexa

Y cam cyntaf i'w gymryd wrth ddiogelu eich dyfeisiau Alexa yw newid y cyfrinair ar gyfer eich cyfrif Amazon, oherwydd dyfais Amazon sy'n cysylltu â'ch cyfrif Amazon yw Alexa. Mae Alexa hyd yn oed wedi integreiddio â chloeon drws clyfar.

Wedyn, bydd angen i chi newid eich cyfrinair Alexa – agorwch yr ap Alexa ar eich dyfais > tapiwch yr eicon dewislen a dewiswch Settings > Account Settings > Change Alexa Password.

- Dylid galluogi prawf dilysu dau gam hefyd. Bydd hyn yn ychwanegu haen arall o ddiogelwch wrth fewngofnodi i gyfrif.

Os oedd gan droseddwr fynediad o'r blaen, neu os hoffech weld pa ddyfeisiau sydd wedi'u cysylltu â dyfais Alexa:

- Agorwch ap Alexa > Devices > Echo and Alexa > Echo device > eicon 'Settings' > Bluetooth devices > 'Forget devices' wrth ymyl y ddyfais yr hoffech ei dileu.

**Note** - Os byddwch yn dal i bryderu ynglŷn â'r mynediad a all fod gan droseddwr i'ch dyfeisiau Alexa, gallwch ailosod y ddyfais i'r gosodiadau ffatri drwy bwysu'r botwm a'i ddal i lawr am 20 eiliad ac aros i'r cylch golau ddiffodd a throi yn ôl ymlaen. Wedyn bydd y ddyfais yn mynd i mewn i'r modd gosod.

## Google Home Nest

Bydd gan ddyfeisiau Google Home Nest bron yn union yr un mesurau diogelwch ag Alexa, ond mae'r ffordd y byddwch yn rhoi'r mesurau hyn ar waith fymryn yn wahanol o bosibl.

- Dylai'r cyfeiriad e-bost a ddefnyddir ar gyfer y Google Nest fod yn ddiogel (edrychwch ar y canllawiau ar gyfer cyfeiriadau e-bost)
- Settings > account > manage account > account security > account password.
- Dylid galluogi prawf dilysu dau gam er mwyn sicrhau diogelwch ychwanegol.

Gallwch edrych i weld pwy sydd â mynediad at eich cartref Nest drwy fynd i ap Nest > Settings > Family & Guests. Yma gallwch weld pwy sydd â mynediad at eich cartref Nest a dileu unrhyw ddyfeisiau dieisiau neu ddyfeisiau nad ydych yn eu hadnabod.

- Ap Google Home > Devices > Settings > o dan enw'r cartref, tapiwch eiconau proffiliau aelodau'r cartref > dewiswch eicon proffil yr aelod yr hoffech ei ddileu > Remove.

Yn wahanol i Alexa, mae gan Google Home Nest nodwedd cyfateb llais sy'n dod i adnabod eich llais dros amser. Mae hyn yn golygu y gall perchennog y ddyfais atal trydydd partion a phobl heb awdurdod rhag defnyddio nodwedd llais Google Home i gael gafael ar wybodaeth sensitif.

- Os hoffech gael gwared ar y nodwedd cyfateb llais, gallwch wneud hynny drwy eich ap Google Home. Settings > Google assistant > Voice match > tynnwch y tic wrth ymyl dyfais i gael gwared ar y nodwedd cyfateb llais.



## Setiau Teledu Clyfar

Teledu sy'n cysylltu â'r rhyngwyd ac sy'n cynnig amrywiaeth o nodweddion ar-lein, fel cynnwys ar alw o apiau a'r gallu i gysylltu â dyfeisiau di-wifr eraill fel ffonau clyfar.

Mae gan setiau teledu clyfar lawer o nodweddion y gellir eu gosod o siop apiau, a gall rhai hyd yn oed gynnwys camerâu a microffonau integredig. Os oes gennych deledu sy'n cynnwys camera a microffon, mae'n bosibl y bydd troseddwr yn camddefnyddio'r nodweddion hyn i'ch monitro chi.

Dylai unrhyw gyfrifon a gaiff eu creu neu y mewngofnodi iddynt ar y teledu clyfar fod yn ddiogel.

- Dylech sicrhau bod gan y cyfrifon a ddefnyddir gyfrineiriau cryf ac na chânt eu rhannu â neb, ac na all neb arall gael mynediad i'r cyfrif e-bost a ddefnyddir.
- Dylid defnyddio prawf dilysu dau gam lle bo modd, yn enwedig wrth geisio prynu pethau. Pe bai rhywun yn ceisio cael mynediad i gyfrifon, ni fyddant yn gallu gwneud hynny heb god mynediad.

- Os bydd y teledu wedi'i osod ac yn cynnwys apiau a osodwyd ymlaen llaw, dylech sicrhau bod yr apiau'n ddiogel drwy fwrw golwg dros eu gosodiadau. Os bydd gennych gamera a microffon ar eich teledu, bydd rhai apiau'n gofyn am ganiatâd i'w defnyddio – dylech wrthod y caniatadau hyn lle bo modd.
- Dylid bwrw golwg dros y gosodiadau pori hefyd. Bydd y rhan fwyaf o borwyr yn cynnig modd 'Safe Browsing' neu ryw beth tebyg, a fydd yn atal dyfeisiau rhag cysylltu a rhannu cynnwys â'r porwr gwe.
- Dylech gyfyngu cymaint â phosibl ar y wybodaeth bersonol ac ariannol a gaiff ei rhannu â'r teledu clyfar.
- Analluogwch (gorchuddiwch) gamera a microffon y teledu - efallai y gallai troseddwr gael mynediad at y nodweddion hyn o bell. Dylech gyfyngu ar gamera a microffon eich teledu neu eu hanalluogi drwy'r gosodiadau. Os byddwch yn dal i bryderu am y camera, gallwch ei orchuddio gan ddefnyddio caead gwe-gamera neu dâp.
- Mae'n bwysig sicrhau bod apiau'n gyfredol (byddant yn diweddarau'n awtomatig fel arfer) a diweddar cadarnwedd y system. Bydd hyn yn sicrhau na fyddwch yn agored i niwed drwy wendidau'r hen feddalwedd.
- Sicrhewch fod y Wi-Fi sy'n cael ei ddefnyddio i gysylltu'r teledu clyfar â'r rhyngwyd yn ddiogel.

Os byddwch yn dal i bryderu ynglŷn â'r mynediad a all fod gan droseddwr, gallwch bob amser ailosod eich teledu i'r gosodiadau ffatri. Bydd hyn yn dileu'r gosodiadau a'r cyfrifon sydd ar y teledu; byddwch yn gallu gosod cyfrifon newydd a chael gafael ar wybodaeth. I ailosod eich teledu i'r gosodiadau ffatri, bydd angen i chi fynd i mewn i'r gosodiadau, a bydd y camau i'w dilyn yn amrywio yn dibynnu ar y gwneuthurwr.



## Camerâu Gwarchod/Gwe-gamerâu

Camera fideo sydd wedi'i dylunio i recordio neu ffrydio i gyfrifiadur neu rwydwaith.

Gall troseddwr gael mynediad at gamerâu gwarchod a gwe-gamerâu o bell; bydd hyn yn eu galluogi i ysbïo arnoch drwy wrando ar sgysiau a gwyllo'r hyn y byddwch yn ei wneud. Bydd rhai gwe-gamerâu hyd yn oed yn eich galluogi i siarad drwyddynt, a bydd y troseddwr yn gallu siarad â chi drwy'r camera gwarchod.

Os oes gennych unrhyw gamerâu gwarchod/gwe-gamerâu yn eich cartref, dyma rai camau y gallwch eu cymryd i'w diogelu:

- Sicrhewch mai dim ond dyfeisiau rydych chi'n eu hadnabod ac wedi'u hawdurdodi sydd wedi'u cysylltu â chyfrif y gwe-gamera – fel arfer, bydd y dyfeisiau cysylltiedig i'w gweld yn adran gosodiadau'r ap a bydd yn hawdd eu tynnu.
- Newidiwch y cyfrinair ar gyfer meddalwedd/ap y camera gwarchod/gwe-gamera. Sicrhewch fod cyfrinair cryf yn cael ei ddefnyddio (gweler y cyngor ar greu cyfrineiriau cryf)
- Sicrhewch fod y rhwydwaith Wi-Fi yn ddiogel (edrychwch ar y canllawiau ar gyfer llwybryddion Wi-Fi). Byddai hyn yn atal y troseddwr rhag cael mynediad at y gwe-gamera drwy dargeddu llwybrydd di-wifr y cartref.
- Diffoddwch y gwe-gamera pan na fyddwch yn ei ddefnyddio, a datgysylltwch ef o'r rhyngwyd. Ni ddylai'r camera gwarchod/gwe-gamera gael ei adael ymlaen drwy'r dydd os na fydd yn cael ei ddefnyddio.
  - Os oes gennych nodweddion gwe-gamera ar eich cyfrifiadur/gliniadur neu unrhyw ddyfeisiau eraill, fe'ch cynghorir i'w gorchuddio pan na fyddant yn cael eu defnyddio.
- Yn dibynnu ar eich rheswm dros ddefnyddio'r camera gwarchod/gwe-gamera, dylech gadw'r microffon mewn cof. Os na fydd angen y microffon, dylid ei analluogi er mwyn atal troseddwr rhag gwranddo ar sgysiau.



## Systemau Hyb Cartref

Caiff hybiau cartref clyfar eu defnyddio i reoli a phweru amrywiaeth o ddyfeisiau cartref clyfar o un lleoliad (yr hyb).

Gall troseddwr gael mynediad at eich hyb cartref (a dyfeisiau eraill tebyg) os bydd yn gwybod yr enw defnyddiwr a'r cyfrinair ar ei gyfer. Gall troseddwr ddefnyddio'r hyb cartref i aflonyddu arnoch. Er enghraifft, gallent ddefnyddio nodweddion yr hyb i droi goleuadau ymlaen a'u diffodd yn eich cartref a rheoli dyfeisiau eraill sydd wedi'u cysylltu â'r hyb.

Mae hybiau cartref wedi dod yn dechnoleg boblogaidd a ddefnyddir yng nghartrefi pobl. Gellir cael mynediad at yr hybiau hyn o bell, sy'n golygu y bydd unrhyw un sydd â mynediad at eich hyb yn gallu monitro'r hyn y byddwch yn ei wneud yn eich cartref neu hyd yn oed wneud newidiadau.

Os oes gennych un o'r hybiau hyn yn eich cartref, dyma rai camau diogelwch y gallwch eu cymryd i sicrhau ei fod yn ddiogel:

- **Sicrhewch fod cyfrinair y cyfrif gweinyddwr wedi cael ei newid** - hyd yn oes os byddwch wedi newid cyfrinairiau cyfrifon defnyddwyr ar yr hyb, bydd y troseddwr yn dal i allu cael mynediad at yr hyb os bydd cyfrinair y cyfrif gweinyddwr ganddo. Gallwch gael canllawiau ar sut i newid cyfrinair y cyfrif gweinyddwr ar wefan yr hyb sydd gennych (e.e. Google, Echo).

**Note** - Mewn rhai achosion lle mai'r troseddwr a osododd yr hyb, mae'n bosibl y bydd yn rhaid ailosod yr hyb i'r gosodiadau ffatri.

- **Edrychwch i weld a yw'r hyb yn storio eich data'n awtomatig** - Efallai mai eich hanes lleoliad fydd y data hyn. Pe bai'r troseddwr yn cael mynediad i'ch cyfrif, gallai gael gafael ar y wybodaeth hon a darganfod ble rydych chi wedi bod neu i ble rydych chi wedi bod yn mynd. Dylech fynd i mewn i osodiadau eich hyb ac ystyried analluogi'r nodwedd hon.



## Dyfeisiau a Gafodd eu Rhoi'n Rhodd gan y Troseddwr

Mae'n bosibl y bydd troseddwr wedi prynu neu osod dyfeisiau gwrando a chamerau. Gall y rhain fod wedi cael eu gosod o fewn llawer o wahanol wrthrychau a chael eu rhoi'n 'rhodd' i chi neu eu gosod yn rhywle yn eich cartref heb yn wybod i chi.

Os oeddech yn arfer bod mewn perthynas â'r troseddwr neu unrhyw fath o berthynas all-lein, dylech geisio cofio unrhyw roddion y gwnaeth y troseddwr eu rhoi i chi. Dylai hyn gynnwys eitemau y gallai fod wedi'u gadael ar ôl yn y tŷ 'ar ddamwain', hyd yn oed, neu eitemau a roddwyd i'r plant (os yw hynny'n berthnasol).

Gall camerau, dyfeisiau gwrando a thracwyr cudd gael eu cuddio mewn unrhyw beth, fwy neu lai. Os bydd y troseddwr yn gwybod manylion sgysiau rydych chi'n eu cael yn eich cartref, neu'n gwybod beth rydych chi'n ei wneud yn eich cartref, mae'n bosibl y bydd camera neu ddyfais wrando ynghudd yn rhywle.

**Noder** - Mae'n bwysig chwilio'n helaeth drwy'r cartref os bydd hynny'n berthnasol.

- **Ysgogi â llais** - os na fyddwch yn defnyddio'r nodwedd ysgogi â llais, dylech ystyried ei thewi/ei hanalluogi ar yr hyb. Y rheswm dros hyn yw, os bydd gan y troseddwr fynediad i'r hyb, y gallai ysgogi'r microffon o bell a gwrando ar sgysiau. Dylech fynd i mewn i osodiadau eich hyb ac ystyried analluogi'r nodwedd hon.
- **Cyfrifon cysylltiedig** - dylech edrych i weld pa gyfrifon sy'n gysylltiedig â'ch hyb. Ni ddylai cyfrifon sy'n cynnwys gwybodaeth bersonol/sensitif amdanoch (manyion bancio, data meddygol ac ati) fod wedi'u cysylltu â'r hyb. Er enghraifft, os bydd y goroeswr yn defnyddio Google neu Echo, dylai ddefnyddio cyfrif Google neu Amazon ar wahân yn benodol ar gyfer yr hyb a dyfeisiau cartref.
- **Diffoddwch yr hyb pan fyddwch oddi cartref** - ni fydd gan yr hyb fotwm i'w bwysu er mwyn ei ddiffodd pan fyddwch oddi cartref (fel arfer). Dylech ddatgysylltu plygiau'r dyfeisiau sydd wedi'u cysylltu â'r hyb na fydd eu hangen arnoch tra byddwch i ffwrdd.
- Dylech ddiffodd cysylltiad eich hyb â'r rhyngwyd pan na fydd yn cael ei ddefnyddio.
- **Sicrhewch fod y Wi-Fi yn gadarn ac yn ddiogel** - mae canllawiau ar lwybryddion Wi-Fi i'w cael ar dudalennau blaenorol yn y ddogfen hon.
- **Diweddariadau meddalwedd** - cofiwch ddiweddaru eich meddalwedd yn rheolaidd, gan y bydd hyn yn sicrhau bod nodweddion diogelwch y ddyfais yn gyfredol ac yn fwy effeithiol.



## Rhan Naw: Canllawiau ar gyfer Tracio Ceir

Monitro lleoliad car neu unrhyw gerbyd sy'n symud gan ddefnyddio'r system GPS.



## Tracwyr Ceir Ffisegol

Gall troseddwr osod traciwr ffisegol ar y tu mewn neu'r tu allan i'ch car er mwyn monitro a dilyn eich lleoliad.

### Canfod lleoliad drwy osod tracwyr

Mewn rhai achosion, bydd troseddwr yn mynd mor bell â gosod system dracio fach ar/yn eich cerbyd.

- Dyfeisiau tracio cerbydau amser real (yn sownd) – gellir prynu'r rhain ar Amazon am gyn lleied ag £20, sy'n eu gwneud yn hygyrth iawn i droseddwr. Caiff rhai o'r tracwyr hyn eu rhoi'n sownd ym matri'r cerbyd, a bydd rhai tracwyr yn fagnetig, hyd yn oed, gan olygu y gellir eu gosod ar y tu mewn neu'r tu mewn i'r cerbyd.
- Dyfeisiau tracio amser real (heb fod yn sownd) – gellir defnyddio'r rhain mewn cerbydau a'u cuddio yn unrhyw le. Bydd y dyfeisiau tracio hyn fel arfer yn fach, sy'n golygu y gallai fod yn anodd eu gweld/darganfod pe baent yn cael eu cuddio mewn cerbyd.

Os bydd gennych chi neu swyddogion reswm dros gredu bod eich cerbyd yn cael ei dracio, dylid defnyddio'r dulliau chwilio cywir (holwch y swyddogion am y camau cywir i'w cymryd mewn perthynas â hyn). Hefyd, mae blocwyr a dryswyr signalau GPS i'w cael y gellir eu prynu ar-lein (fel rhagofal ychwanegol). Mae'r rhain wedi'u dylunio i darfu ar y signalau a anfonir i dracwyr GPS a'u hatal rhag gweithio'n iawn.



## Camerâu Dashfwrdd

Camera fideo bach yw camera dashfwrdd. Caiff ei osod yn sownd yn nashfwrdd neu ffenestr flaen y car mewn safle sy'n cynnig golygfa dda o'r ffordd o'ch blaen. Bydd yn recordio wrth i chi yrru.

Gall troseddwr gael mynediad at fideos eich camera dashfwrdd er mwyn eich monitro a gwybod i ble rydych chi wedi bod yn mynd. Gellir ei ddefnyddio i fonitro eich lleoliad mewn amser real hefyd.

Os oes gennych gamera dashfwrdd, dylech edrych i weld pwy sydd â mynediad at y fideos. Gall troseddwr gael mynediad at y fideos hyn a'u gwyllo er mwyn gweld i ble rydych chi wedi bod yn teithio neu ble ydych chi.

- Bydd y rhan fwyaf o gamerâu dashfwrdd yn defnyddio apiau penodedig â chysylltiad Wi-Fi integredig sy'n galluogi person i gysylltu a chysoni â'r ddyfais o'i ffôn neu lechen a gwyllo'r fideos yn y fan a'r lle.
- Mae'n bosibl y bydd gan eich camera dashfwrdd ap penodedig. Os felly, dylech newid y cyfrinair a sicrhau na fydd gan neb arall fynediad i'r cyfrif.
- Gall rhai camerâu dashfwrdd gynnig nodweddion amgryptio er mwyn atal unigolion heb awdurdod rhag gwyllo'r fideos – dylech edrych ar wefan y camera dashfwrdd i weld a yw'r nodwedd hon ar gael ar gyfer eich camera dashfwrdd chi. Os felly, byddai'n syniad da i chi alluogi'r nodwedd hon.
- Mewn achosion lle mai'r troseddwr a osododd y camera dashfwrdd, mae'n bosibl mai'r troseddwr fydd yr un sydd â mynediad i'r ap penodedig. Os na fyddwch yn gwybod manylion cyfrif yr ap, dylech ailosod y camera dashfwrdd i'r gosodiadau ffatri. Bydd canllawiau ar sut i wneud hynny i'w gweld ar wefan y camera dashfwrdd. Dylai ailosod y camera dashfwrdd i'r gosodiadau ffatri ei ddatgysylltu o'r cyfrif ar yr ap.

## Rhan Deg: Canllawiau ar gyfer Trydydd Partïon

Gall troseddwr swyno/twylo trydydd partïon i ddatgelu gwybodaeth amdanoch wrtho. Hefyd, mae'n bosibl y bydd y troseddwr yn gweld unrhyw beth y bydd trydydd partïon yn ei bostio amdanoch chi ar-lein.

Bydd troseddwr yn aml yn defnyddio teulu a ffrindiau i'ch cyrraedd chi. Bydd y math hwn o dacteg yn haws dan yr amgylchiadau canlynol:

- **Os bydd gennych chi a'r troseddwr ffrindiau cyffredin** - gallai ffrindiau cyffredin fod yn trosglwyddo gwybodaeth amdanoch chi yn ôl i'r troseddwr heb sylweddoli.
  - **Swyno er mwyn cael gwybodaeth am y goroeswr** - os bydd y ffrind cyffredin yn siarad â chi a'r troseddwr yn rheolaidd, bydd hynny'n arwain at risg o rannu gwybodaeth. Er enghraifft, gallai'r troseddwr ofyn i'r ffrind cyffredin sut ydych chi (ymddangos fel pe bai ots ganddo), neu gallai'r ffrind cyffredin sôn am gynlluniau sydd ar y gorwel gyda chi. Gallai'r troseddwr swyno'r ffrind cyffredin i ddatgelu lleoliad y cynlluniau hyn.
  - **Cyfyngau cymdeithasol** - os bydd y ffrind cyffredin yn ffrindiau â chi a'r troseddwr ar y cyfyngau cymdeithasol, ni ddylai fod yn eich tagio chi mewn ffotograffau nac yn datgelu'r lleoliad.

Oherwydd hyn, mae'n bwysig bod trydydd partïon yn cael gwybod am ymddygiad/ gweithredoedd y troseddwr, a dylai sicrhau nad yw'n siarad amdanoch chi â'r troseddwr. Hefyd, ni ddylai ffrindiau cyffredin eich tagio chi mewn ffotograffau ar y cyfyngau cymdeithasol na datgelu gwybodaeth bersonol amdanoch (fel eich lleoliad).

- **Os bydd gennych chi blant gyda'ch gilydd** – gall fod yn anodd torri pob cysylltiad â'r troseddwr pan fydd gennych blant (yn dibynnu ar yr amgylchiadau), felly mae'n bosibl y bydd cyswllt â chi neu aelodau o'ch teulu ynglŷn â'r plant yn berthnasol.
  - **Swyno aelodau o'r teulu am wybodaeth** - yn debyg i ffrindiau cyffredin (y sonnir amdanynt uchod), mae'n bosibl y bydd y troseddwr yn swyno aelodau o'r teulu i ddatgelu gwybodaeth amdanoch chi. Dylai aelodau o'r teulu wneud eu gorau glas i osgoi cael sgysiau amdanoch chi, a siarad am eich plant yn unig.
  - **Cyfyngau cymdeithasol** - os bydd y ffrind cyffredin yn ffrindiau â chi a'r troseddwr ar y cyfyngau cymdeithasol, ni ddylai fod yn eich tagio chi mewn ffotograffau nac yn datgelu'r lleoliad.

Yn y senario orau, byddai trydydd partïon yn blocio'r troseddwr ar eu cyfrifon cyfyngau cymdeithasol, a dylid rhoi gwybod iddynt am unrhyw gyfrifon dynwared y bydd y troseddwr wedi'u creu ohonoch chi.

Ni ddylai trydydd partïon ddatgelu gwybodaeth bersonol amdanoch chi wrth y troseddwr (ffrindiau cyffredin neu deulu), gan gynnwys ble rydych chi'n byw ac yn gweithio, eich cynlluniau cymdeithasol, eich rhif ffôn symudol ac ati.

Bydd troseddwr yn fodlon gwneud unrhyw beth i gael gwybodaeth amdanoch, felly dylai trydydd partïon fod yn ofalus ynglŷn â'r hyn y byddant yn ei ddatgelu ar-lein neu wyneb yn wyneb.

# Rhan Un ar Ddeg: Deddf Camddefnyddio Cyfrifiaduron 1990 a Deddf Troseddau Rhywiol 2003

## Deddf Camddefnyddio Cyfrifiaduron 1990

Deddfwriaeth allweddol yn y DU sy'n gwneud mynediad heb awdurdod at ddata cyfrifiadurol, ac addasu data cyfrifiadurol heb awdurdod, yn anghyfreithlon.

Yn sicr, bydd troseddau sydd wedi'u cynnwys yn adrannau'r Ddeddf Camddefnyddio Cyfrifiaduron (1990) yn berthnasol yn achos goroeswr mewn perthynas â stelcio ac aflonyddu ar-lein.

### Adran 1 o'r Ddeddf Camddefnyddio Cyfrifiaduron

Mae'r adran hon yn ymdrin â throsedd mynediad heb awdurdod at ddeunydd cyfrifiadurol.

**Er enghraifft** - roedd y troseddwr yn gwybod cyfrinair y goroeswr, neu llwyddodd i'w ddyfalu, a chafodd fynediad i gyfrif(on) cyfryngau cymdeithasol y goroeswr heb ganiatâd.

**Noder** - Os bydd y troseddwr wedi cael mynediad at unrhyw gyfrifon ar-lein neu ddyfeisiau sy'n eiddo i'r goroeswr heb ganiatâd, bydd wedi cyflawni trosedd o dan y Ddeddf Camddefnyddio Cyfrifiaduron.

### Adran 2 o'r Ddeddf Camddefnyddio Cyfrifiaduron

Mae'r adran hon yn ymdrin â throsedd mynediad heb awdurdod gyda'r bwriad o gyflawni neu hwyluso trosedd bellach.

**Er enghraifft** - mae'r troseddwr yn cael mynediad i ap bancio ar-lein y goroeswr heb ganiatâd gyda'r bwriad o ddwyn arian.

Mae'n bwysig eich bod chi a'r swyddogion yn ymwybodol o elfennau'r troseddau hyn ac yn eu deall. Drwy wneud hynny, byddwch chi a'r swyddogion yn gallu adnabod y troseddau hyn pan fyddant yn cael eu cyflawni. Bydd hyn yn fodd i gadw tystiolaeth ar gyfer unrhyw gamau y gellid eu cymryd yn erbyn y troseddwr yn y dyfodol.

## Adran 3 o'r Ddeddf Camddefnyddio Cyfrifiaduron

Mae'r adran hon yn ymdrin â throsedd gweithredoedd heb awdurdod gyda'r bwriad o amharu ar weithrediad cyfrifiadur.

**Er enghraifft** - mae'r troseddwr yn cael mynediad i lwybrydd Wi-Fi'r goroeswr heb ganiatâd, yn newid y cyfrinair ac yn datgysylltu ei ddyfeisiau o'r rhyngwyd.

## Adran 3ZA o'r Ddeddf Camddefnyddio Cyfrifiaduron

Mae'r adran hon yn ymdrin â throsedd gweithredoedd heb awdurdod sy'n achosi neu'n creu risg o ddifrod difrifol.

**Noder** - Ni fydd y drosedd hon o dan y Ddeddf Camddefnyddio Cyfrifiaduron yn berthnasol i achosion o stelcio ac aflonyddu ar-lein ac mae wedi'i bwriadu ar gyfer pobl sy'n ceisio ymosod ar seilwaith cenedlaethol allweddol.

## Adran 3A o'r Ddeddf Camddefnyddio Cyfrifiaduron

Mae'r adran hon yn ymdrin â chreu erthyglau (rhaglenni neu ddata ar ffurf electronig), eu cyflenwi neu gael gafael arnynt i'w defnyddio yn adrannau 1, 2 a 3.

**Er enghraifft** - os bydd troseddwr yn cael gafael ar faleiswedd gyda'r bwriad o'i defnyddio ar ddyfais goroeswr, ond heb ei defnyddio neu heb gael cyfle i'w defnyddio eto.

## Deddf Troseddau Rhywiol 2003 fel rhan o Ddeddf Diogelwch Ar-lein 2023

Dylech fod yn ymwybodol ei bod bellach yn drosedd rhannu delweddau neu ffilm o natur bersonol heb gydsyniad, ni waeth p'un a oedd y troseddwr yn bwriadu achosi niwed i'r goroeswr ai peidio.

Mae'r Ddeddf Troseddau Rhywiol (2001), adran 66(b) yn cyflwyno tair trosedd sy'n gysylltiedig â rhannu delweddau o natur bersonol:

1. Person yn rhannu ffotograff neu ffilm sy'n dangos, neu sy'n dangos i bob golwg, rhywun mewn sefyllfa o natur bersonol heb ei gydsyniad, a hynny'n fwriadol.
  2. Person yn rhannu ffotograff neu ffilm sy'n dangos, neu sy'n dangos i bob golwg, rhywun mewn sefyllfa o natur bersonol, a hynny'n fwriadol, gyda'r bwriad o achosi braw, gofid neu gywilydd i'r person hwnnw a heb ei gydsyniad.
  3. Person yn rhannu ffotograff neu ffilm sy'n dangos, neu sy'n dangos i bob golwg, rhywun mewn sefyllfa o natur bersonol, a hynny'n fwriadol, er ei foddhad rhywiol ei hun neu rywun arall, heb gydsyniad y person yn y ffotograff neu'r ffilm, a heb gred resymol ei fod yn cydsynio.
- Mae hefyd yn cyflwyno pedwaredd drosedd, sef bygwth rhannu delweddau o natur bersonol.
4. Person yn bygwth rhannu ffotograff neu ffilm sy'n dangos, neu sy'n dangos i bob golwg, rhywun mewn sefyllfa o natur bersonol. Bydd naill ai'n bwriadu i'r person yn y sefyllfa o natur bersonol honno, neu rywun sy'n ei adnabod, ofni y caiff y bygythiad ei wireddu, neu'n ddiotal ynglŷn ag ofn y person hwnnw y caiff ei wireddu.

## StopNCII.org

Adnodd am ddim sydd wedi'i ddylunio i gefnogi goroeswyr camddefnyddio delweddau o natur bersonol heb gydsyniad yw StopNCII.org. Mae'r adnodd yn gweithio drwy greu hash o'ch delwedd(au)/fideo(s) o natur bersonol. Bydd StopNCII.org yn anfon yr hash at gwmnïau sy'n cymryd rhan er mwyn iddynt helpu i ganfod y delweddau/fideos a'u hatal rhag cael eu rhannu ar-lein.

### Cwmnïau sy'n cymryd rhan:

facebook

TikTok

reddit

Instagram

bumble

OnlyFans

Threads

Porn hub

Snap Inc.

NIANTIC

playhouse

REDGIFS

I gael rhagor o wybodaeth am y prosiect hwn a gynhelir gan y Llinell Gymorth Pornograffi Dial, ewch i'w wefan yn [www.stopncii.org](http://www.stopncii.org).

Hefyd, mae gan Google adnoddau cymorth ar gyfer dileu delweddau o natur bersonol neu anwedus o'r peiriant chwilio.

## Rhan Deuddeg: Deallusrwydd Artiffisial (AI)

Mae'n galluogi cyfrifiaduron i ddysgu a datrys problemau fel person. Defnyddir llawer iawn o wybodaeth i hyfforddi cyfrifiaduron a'u haddysgu i adnabod patrymau ynddi, er mwyn cyflawni tasgau, er enghraifft sgwrsio fel bod dynol.

Mae deallusrwydd artiffisial ar flaen y gad o ran datblygiadau technolegol, ac mae'r potensial sydd ganddo i wella effeithlonrwydd a sicrhau bod gwybodaeth ar gael yn eang bron yn ddi-ben-draw. Fodd bynnag, gan ei fod bellach mor gyffredin, rhaid i ni gydnabod ac ystyried ei effaith ar hwyluso trais yn erbyn menywod a merched:

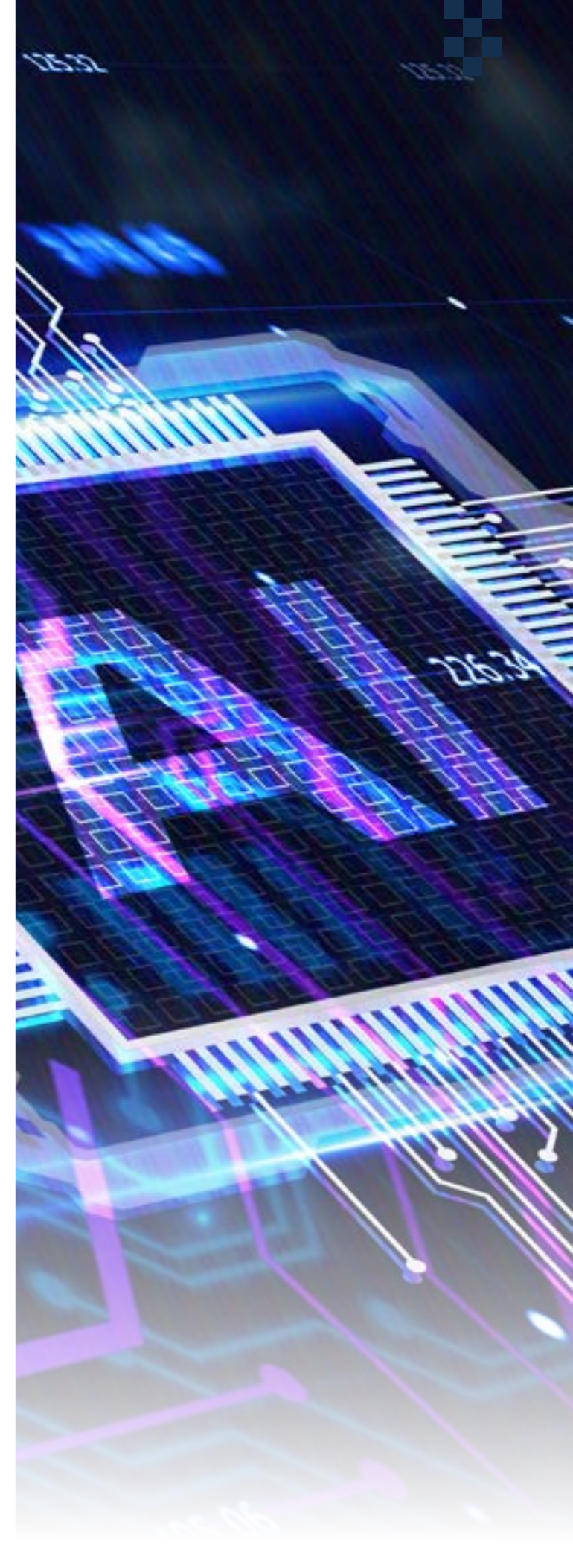
### Yr hyn a all fod yn digwydd

Deallusrwydd Artiffisial a Stelcio – gallai'r troseddwr fod yn defnyddio deallusrwydd artiffisial i'ch monitro a'ch tracio'n fwy cywir ac yn haws. Er enghraifft, gallai algorithmau a bwerir gan ddeallusrwydd artiffisial ddadansoddi a rhagfynegi eich lleoliad drwy gasglu data o ffynonellau fel y cyfryngau cymdeithasol a delweddau â geotagiau.

### Yr hyn y gwyddom ei fod yn digwydd

Ffugio dwfn (ffugio + dysgu dwfn) – mae hyn yn defnyddio algorithmau dysgu dwfn i greu delweddau a fideos ffug argyhoeddiadol. Mae'r dechnoleg hon wedi cael ei defnyddio yn erbyn menywod i greu a dynwared pornograffi heb gydsyniad. Ni fydd angen i'r troseddwr gael gafael ar ddelwedd o natur bersonol mwyach, gan y bydd yn gallu creu un gan ddefnyddio deallusrwydd artiffisial yn lle hynny.

**Note** - O dan y Ddeddf Diogelwch Ar-lein, mae rhannu a chreu ffugiadau dwfn yn drosedd.



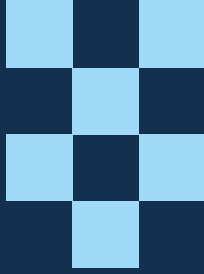


## Cyfeiriadau

Y Swyddfa Ystadegau Gwladol (2023). Experiences of harassment prevalence and nature tables, England and Wales [rhynggrwyd].  
[Cyrchwyd 26 Mehefin 2024]

Asesiad Bygythiad a Risg Strategol i ddod ar ddiwedd 2024 – Ymarfer casglu data wedi'i deilwra ar gyfer pob heddlu mewn perthynas â throseddau a gofnodwyd gan yr heddlu yn 2023/24 er mwyn llywio asesiad o'r bygythiad o drais yn erbyn menywod a merched.

Asesiad Bygythiad a Risg Strategol i ddod ar ddiwedd 2024 – Ymarfer casglu data wedi'i deilwra a gynhaliwyd gan rwydwaith dadansoddwyr CSAE ar gyfer yr Asesiad.



**HEDDLU  
DE CYMRU**  

---

**SOUTH WALES  
POLICE**



Mae'r ddogfen hon hefyd ar gael yn Saesneg.

This document is also available in English.