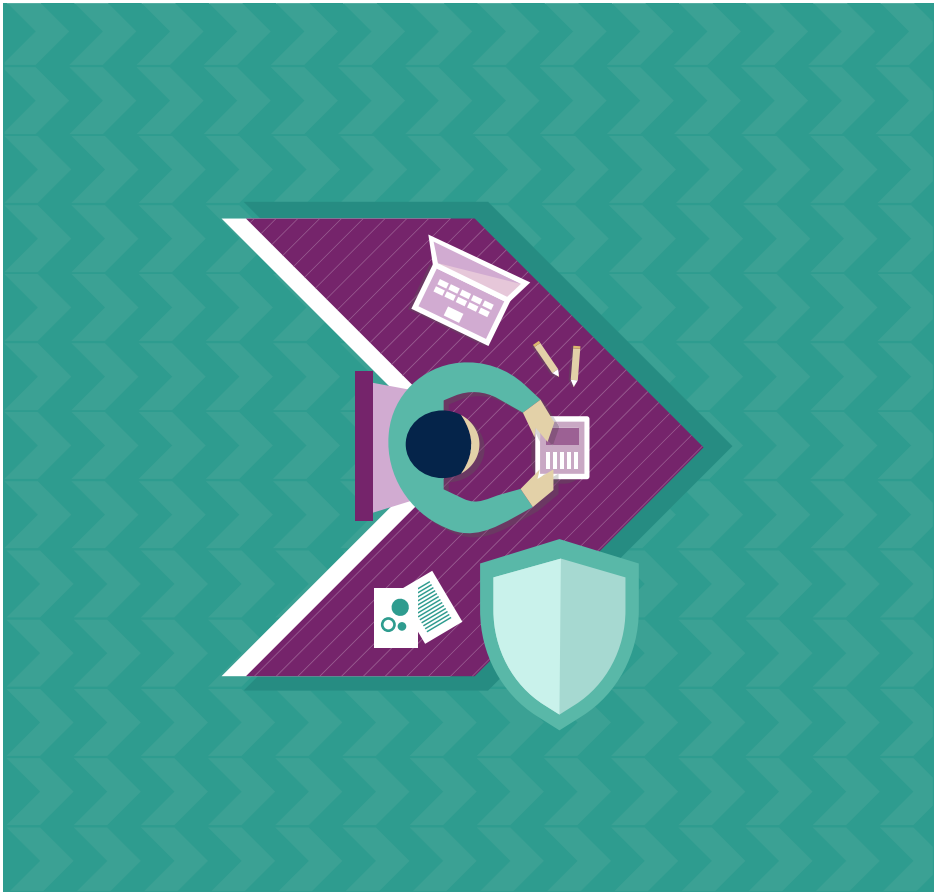
National Cyber Security Centre
a part of GCHQ

Ymarferwyr Blynyddoedd Cynnar:

defnyddio seiberddiogelwch i ddiogelu eich lleoliadau

Sut i ddiogelu gwybodaeth sensitif am eich lleoliad a'r plant yn eich gofal rhag difrod damweiniol a throseddwyr ar-lein.



Cyflwyniad

Mae lleoliadau gofal plant ac addysg y Blynyddoedd Cynnar[1], fel y rhan fwyaf o weithleoedd eraill, yn dibynnu fwyfwy ar dechnoleg.

Mae ffonau clyfar, cyfrifiaduron, gliniaduron a thabledi yn rhan sylfaenol o fywyd modern. O fancio a siopa ar-lein, i e-bost a'r cyfryngau cymdeithasol, i'r dyfeisiau 'clyfar' sy'n monitro ac yn diogelu ein cartrefi a'n safleoedd gwaith - mae'n anodd dychmygu sut bydden ni'n byw a bod hebddyn nhw.

Dyna pam ei bod hi'n bwysicach nag erioed i ni gymryd camau i ddiogelu'r dyfeisiau hyn (a'r data a storiwn arnyn nhw) rhag difrod damweiniol, neu droseddwyr ar-lein. A dyna pam mae **seiberddiogelwch** yn hollbwysig i **bawb** ohonom. Mae seiberddiogelwch yn golygu diogelu'r dyfeisiau rydyn ni'n dibynnu arnyn nhw, a diogelu'r gwasanaethau sydd eu hangen ar fusnesau, boed fawr neu fach, i weithredu.

Early Learning and Childcare (Yr Alban)); Early Child Education and Care (EU). I'w gyfeirio drwyddi draw fel 'Blynyddoedd Cynnar'

Pam mae seiberddiogelwch yn bwysig i ymarferwyr y Blynyddoedd Cynnar?

Ar gyfer ymarferwyr y Blynyddoedd Cynnar, mae seiberddiogelwch hefyd yn chwarae rôl o ran diogelu'r plant yn eich gofal. Mae seiberddiogelwch da yn golygu diogelu'r wybodaeth bersonol neu sensitif sydd gennych chi am blant a'u teuluoedd.

Mae eich cyngor a'ch deddfwriaeth genedlaethol ar gyfer y Blynyddoedd Cynnar[2] a'r Ddeddf Diogelu Data yn ei gwneud yn ofynnol i chi gadw gwybodaeth a chofnodion cyfrinachol am staff a phlant yn ddiogel, a sicrhau mai dim ond y rhai sydd â hawl neu'r angen proffesiynol i'w gweld nhw (naill ai'n gorfforol neu ar-lein) sy'n gallu cael gafael arnyn nhw.

Efallai nad ydych chi wedi ystyried y peth, ond beth bynnag fo maint a natur eich lleoliad, **mae'r wybodaeth sydd gennych chi o fudd i droseddwr**. Ac er na fyddan nhw efallai yn targedu eich lleoliad chi'n uniongyrchol, mae'n rhy hawdd cael eich taro gan **negeseuon e-bost twyllodrus** y mae seiberdroseddwyr yn eu hanfon at filiynau o fusnesau.

Bydd seiberdroseddwyr yn mynd ar ôl unrhyw un, cyn belled â bod arian i'w wneud. Hyd yn oed os nad ydych chi'n colli arian yn uniongyrchol, gallai achos o **fynediad diawdurdod at ddata** (pan gaiff gwybodaeth a gedwir gan fusnes ei dwyn neu ei defnyddio heb ganiatâd) achosi i'ch lleoliad gau dros dro a niweidio'ch enw da ymhlith y teuluoedd rydych chi'n ymwneud â nhw. Gallai hefyd eich gadael yn agored i ymchwiliad gan **Swyddfa'r Comisiynydd Gwybodaeth (ICO)**.

Efallai fod hyn i gyd yn swnio'n eithaf brawychus, ond pwyll piau hi. Cynhyrchwyd y canllawiau hyn gan yr NCSC i helpu ymarferwyr sy'n gweithio ym maes y Blynyddoedd Cynnar i ddiogelu'r data a'r dyfeisiau rydych chi'n eu defnyddio bob dydd. Gallai arbed amser, arian a hyd yn oed enw da eich lleoliad.

Da chi, darllenwch y canllawiau hyd yn oed os ydych chi'n meddwl na fyddwch chi byth mewn perygl. Bydd dilyn y pedwar cam a amlinellir isod yn lleihau'r tebygolrwydd o ddioddef, a bydd yn eich helpu i ailgodi ar eich traed pe bai'r gwaethaf yn digwydd.

1. **Gwnewch gopi wrth gefn o'ch gwybodaeth bwysig**
2. **Defnyddiwch gyfrineiriau i reoli mynediad i'ch cyfrifiaduron a gwybodaeth**
3. **Diogelwch eich dyfeisiau rhag feirysau a maleiswedd**
4. **Sut i ddelio â negeseuon amheus (ymosodiadau gwe-rwydo)**
5. **Dysgu mwy**

[2] **EYFS statutory framework** (Lloegr); **Health and Social Care Standards** (Yr Alban); **Y Safonau Gofynnol Cenedlaethol ar gyfer gofal plant a reoleiddir** (ar gyfer plant hyd at 12 oed) (Cymru); Minimum Standards for Childminding and Daycare for children under 12 (Gogledd Iwerddon).

1 Gwnewch gopi wrth gefn o'ch gwybodaeth bwysig

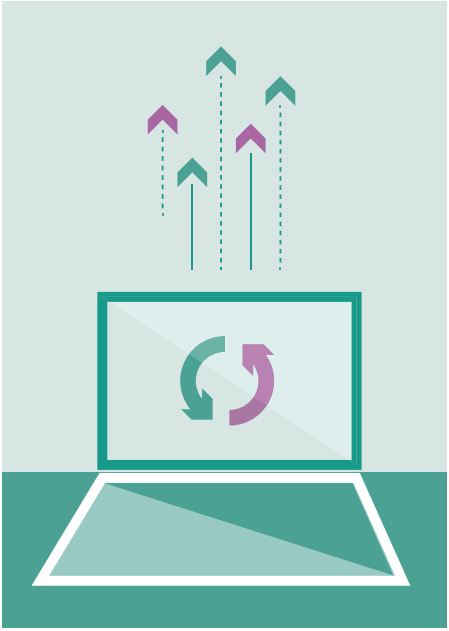
Meddyliwch faint rydych chi'n dibynnu ar dechnoleg i redeg eich lleoliad, a'r wybodaeth sy'n cael ei storio ar eich cyfrifiaduron. Mae hyn yn cynnwys gwybodaeth sensitif am y plant yn eich gofal, eu teuluoedd, cofnodion staff, manylion cyswllt teuluol mewn argyfwng, a gwybodaeth hynod bersonol arall. Hefyd, mae yna ddata hollbwysig i fusnes fel e-bost, taliadau ffioedd, bancio ac anfonebau.

Nawr dychmygwch am faint allwch chi weithredu hebddyn nhw.

Mae'n bwysig cadw copi wrth gefn o'r wybodaeth hanfodol hon rhag ofn i rywbeth ddigwydd i'ch offer TG, neu safle eich lleoliad. Efallai y bydd damwain (fel tân, llifogydd neu golled), rhywun yn dwyn eich offer, neu gallai feirws gyfrifiadurol niweidio, dileu neu gloi eich data hyd nes y bydd rhywun yn talu pridwerth.

Dechreuwch drwy nodi eich gwybodaeth bwysicaf - hynny yw, y wybodaeth na allai'ch lleoliad weithredu hebddi neu wybodaeth y mae **rhwymedigaeth gyfreithiol arnoch i'w diogelu.** Gwnewch gopi wrth gefn ar gof bach USB, gyriant caled allanol, neu '**yn y cwmwl**'. Ar ôl gwneud copi wrth gefn, gwnewch yn siŵr eich bod yn gwybod sut i adfer y wybodaeth ohono. Os ydych chi'n defnyddio meddalwedd rheoli meithrinfa, mae'n debyg y bydd yn cynnwys offer i'ch helpu i wneud hyn. Os nad ydych chi'n defnyddio meddalwedd o'r fath, chwiliwch ar-lein am gyfarwyddiadau. I'ch rhoi ar ben ffordd, dyma rai canllawiau ar sut i sefydlu storfa cwmwl:

- **Apple** (iPhone, iPad ac iPod Touch, a Mac)
- **Google** (Android)
- Dyfeisiau **Microsoft** (Windows 10)



2 Defnyddiwch gyfrineiriau i reoli mynediad i'ch cyfrifiaduron a gwybodaeth

O'u defnyddio'n gywir, mae cyfrineiriau yn ffordd effeithiol o atal rhai heb ganiatâd/awdurdod rhag agor eich cyfrifon e-bost, eich dyfeisiau, a'r data rydych chi'n ei storio arnyn nhw. Mae'r adran hon yn amlinellu rhai pethau i'w cadw mewn cof wrth ddefnyddio cyfrineiriau.

Gweithredu diogelwch cyfrinair (neu opsiynau 'mewngofnodi' eraill)

Gwnewch yn siŵr fod angen cyfrinair ar ddyfeisiau yn eich gwaith (gliniaduron, cyfrifiaduron personol a thabledi) wrth eu hagor. Pe bai'n well gennych chi beidio â defnyddio cyfrinair, dewiswch ddull arall o 'gloi' eich dyfais, fel olion bysedd, PIN, patrwm sgrin neu adnabod wyneb. Os oes angen help arnoch i wneud hyn, rydym wedi cynnwys rhai dolenni isod:

1. Opsiynau mewngofnodi ar gyfer Windows 10
2. Opsiynau mewngofnodi ar gyfer Android
3. Opsiynau mewngofnodi ar gyfer macOS
4. Opsiynau mewngofnodi ar gyfer iPhone

Defnyddio cyfrineiriau cryf

Ceisiwch osgoi defnyddio cyfrineiriau amlwg (fel dyddiadau, enwau teuluol ac anifeiliaid anwes), a pheidiwch â **defnyddio'r cyfrineiriau mwyaf cyffredin** y gall troseddwyr eu dyfalu'n hawdd (fel 'passw0rd'). I greu cyfrinair cofiadwy sy'n anodd i rywun arall ei ddyfalu, gallwch **gyfuno tri gair ar hap** i greu cyfrinair (er enghraifft 'dogtreecereal').

Mae'n bwysig iawn **peidio** ag ailddefnyddio'r un cyfrinair ar gyfer eich cyfrifon ar-lein gwahanol. Yn benodol, defnyddiwch **gyfrinair cryf ar wahân ar gyfer eich e-bost.** Os bydd haciwr yn gallu agor eich blwch negeseuon e-bost, gall gael gafael ar wybodaeth am eich taliadau, anfonebau, plant (a'u teuluoedd), yn ogystal ag anfon negeseuon e-bost ffug yn eich enw chi.

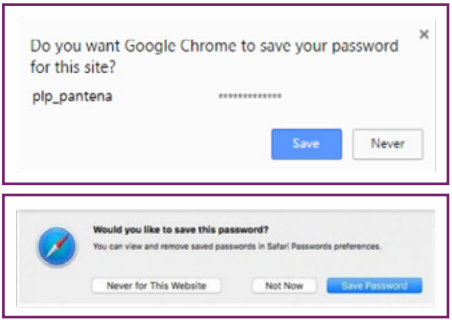
Cofiwch warchod eich cyfrineiriau

Wrth gwrs mae gan y rhan fwyaf ohonom lawer o gyfrifon ar-lein, felly mae'n anodd creu cyfrineiriau gwahanol i bob un

ohonyn nhw (a'u cofio). Fodd bynnag, er mwyn gwneud hyn yn haws, gallwch:ohonyn nhw (a'u cofio). Fodd bynnag, er mwyn gwneud hyn yn haws, gallwch:

1. Ysgrifennu eich holl gyfrineiriau ar ddarn o bapur a'i gadw yn rhywle diogel (i **ffwrdd** o'ch cyfrifiadur)
2. Gadewch i'ch **porwr gadw eich cyfrineiriau** ar eich cyfer - **mae'n ddiogel eu cadw pan ofynnir i chi**, ar yr amod eich bod yn fodlon i gydweithwyr ddefnyddio'r cyfrifiadur yn eich lleoliad.

Os oes mwy nag un person yn defnyddio'ch cyfrifiadur, dylai pawb gael cyfrifon a chyfrineiriau gwahanol, yn ddelfrydol. Os nad yw hyn yn bosibl, gofalwch eich bod yn gwybod pwy sy'n cael defnyddio dyfeisiau, pwy sy'n gwybod y cyfrinair, a'ch bod yn iawn gyda hyn. **Peidiwch** ag ysgrifennu'r cyfrinair ar bapur Post-it wrth y cyfrifiadur, lle gallai unrhyw un weld eich manylion. Am yr un rhesymau, defnyddiwch **sgrin gloi** pan fyddwch i ffwrdd o'ch desg, a chofiwch newid eich cyfrineiriau pan fydd aelod o staff sy'n gallu defnyddio'ch dyfeisiau yn gadael.



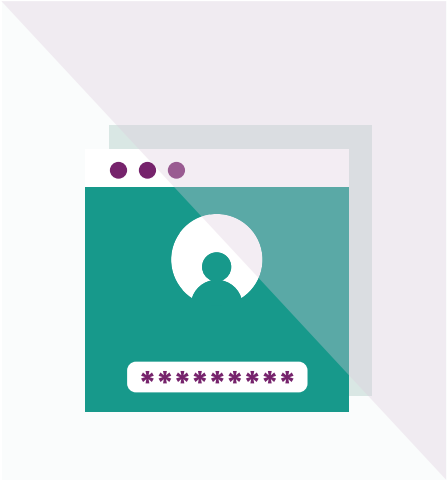
Mae'n ddiogel gadael i borwyr gadw eich cyfrineiriau.

Sefydlu prawf dilysu dau gam

Mae llawer o gyfrifon a gwasanaethau ar-lein yn caniatáu i chi sefydlu prawf dilysu dau gam **(2FA)** sy'n golygu na fydd haciwr yn gallu cael mynediad i'ch cyfrifon hyd yn oed os yw'n gwybod eich cyfrinair. Fel arfer, mae'n gweithio drwy anfon PIN neu god atoch (a anfonir yn aml trwy neges destun), y byddwch yn ei gofnodi wedyn i brofi taw chi sydd wrthi mewn gwirionedd.
Os cewch chi'r opsiwn hwn, mae'n werth neilltuo amser i sefydlu 2FA ar eich cyfrifon pwysicaf (fel e-bost a bancio) - dim ond ychydig funudau gymerith hi, ac fe fyddwch chi'n llawer saffach ar-lein o ganlyniad.

Cyfathrebu'n ddiogel â'ch teuluoedd (gan gynnwys y cyfryngau cymdeithasol)

Os byddwch yn anfon cylchlythyrau, negeseuon cyfryngau cymdeithasol, neu unrhyw wasanaethau eraill sy'n cynnwys lluniau neu fanylion plant yn eich gofal, gwnewch yn siŵr eich bod yn rheoli pwy sy'n gallu eu gweld nhw. Er enghraifft, dylech ddiogelu cylchlythyrau gan ddefnyddio cyfrinair fel mai dim ond teuluoedd sydd wedi cael y cyfrinair all eu hagor. Hefyd, dylech wirio'r gosodiadau preifatrwydd ar draws unrhyw gyfrifon cyfryngau cymdeithasol, fel mai dim ond gofalwyr y plentyn all gael mynediad iddyn nhw (**mae'r NCSC wedi cyhoeddi canllawiau i'ch helpu i wneud hyn**).



3 Diogelwch eich dyfeisiau rhag feirysau a maleiswedd

Math o raglen faleisus yw feirysau sy'n gallu niweidio dyfeisiau fel cyfrifiaduron a gliniaduron. Unwaith y bydd eich dyfais wedi'i heintio, gall **meddalwedd faleisus** ddwyn eich data, ei ddileu'n llwyr, neu hyd yn oed eich cloi allan o'ch dyfais.

Yn union fel feirysau bywyd go iawn, mae feirysau cyfrifiadurol yn ymledu'n hawdd. Gall eich dyfeisiau gael eu heintio drwy lawrlwytho atodiad e-bost yn ddamweiniol sy'n cynnwys feirws, neu drwy blygio cof bach/USB i mewn sydd eisoes wedi'i heintio. Gallwch hyd yn oed gael eich heintio o wefan amheus y cawsoch eich twyllo i ymweld â hi.

Mae'r adran hon yn cynnwys awgrymiadau ar sut i ddiogelu eich dyfeisiau rhag y difrod a achosir gan feirysau a mathau eraill o faleiswedd.

Gweithredu eich cynnyrch gwrth-feirws

Dylech bob amser ddefnyddio meddalwedd gwrth-feirws ar liniaduron a chyfrifiaduron eraill yn eich lleoliad. Mae'n aml yn cael ei gynnwys am ddim, felly dim ond ei danio a'i ddiweddaru sydd ei angen. Does dim angen **meddalwedd gwrth-feirws** ar y rhan fwyaf o ffonau clyfar a thabledi modern, ar yr amod mai dim ond apiau a meddalwedd o siopau swyddogol fel Google Play ac App Store Apple rydych chi'n eu gosod.

Cofiwch ddiweddaru eich holl ddyfeisiau TG.

Peidiwch ag osgoi diweddaru eich apiau a meddalwedd eich dyfais. Mae'r diweddariadau hyn yn cynnwys amddiffyniad rhag feirysau a mathau eraill o faleiswedd, a byddan nhw'n aml yn cynnwys gwelliannau a nodweddion newydd. Defnyddio a derbyn diweddariadau meddalwedd yw un o'r pethau pwysicaf y gallwch ei wneud i ddiogelu eich dyfeisiau. Ewch ati i ddiweddaru'r holl apiau a system weithredu eich dyfais pan gewch chi'ch ysgogi i wneud hynny. Hefyd, gallwch roi 'diweddariadau awtomatig' ar waith yng ngosodiad eich dyfais, os yw ar gael. Bydd hyn yn golygu nad oes rhaid i chi gofio derbyn y diweddariadau.

Os ydych chi'n amau bod eich dyfais yn cynnwys feirws (neu unrhyw fath arall o faleiswedd), **darllenwch ganllawiau'r NCSC ar sut i adfer dyfais heintiedig**.

4 Sut i ddelio â negeseuon amheus (ymosodiadau gwe-rwydo)

Negeseuon e-bost twyllodrus sy'n ceisio'ch darbwyllo i glicio ar ddolenni i wefannau amheus, neu lawrlwytho atodiadau peryglus – dyna yw e-byst gwe-rwydo. Efallai y bydd y gwefannau'n ceisio eich twyllo i ildio gwybodaeth sensitif (fel manylion banc), a gall yr atodiadau gynnwys feirysau cyfrifiadurol a fydd yn heintio eich peiriant.

Ar hyn o bryd, mae llawer o negeseuon e-bost gwe-rwydo **yn chwarae ar ofnau am COVID-19**, ond gall troseddwyr hefyd ddefnyddio dulliau eraill i'ch twyllo, fel anfon negeseuon testun (SMS), neu dros y ffôn. Fodd bynnag, defnyddir y term 'gwe-rwydo' yn bennaf i ddisgrifio sgamiau sy'n cyrraedd drwy **e-bost**.

Mae'r adran hon yn disgrifio sut i adnabod arwyddion amlycaf e-bost gwe-rwydo, a beth i'w wneud os ydych chi'n meddwl eich bod wedi clicio ar ddolen amheus.

Awgrymiadau ar gyfer sylwi ar negeseuon amheus

Mae'n anodd sylwi ar negeseuon e-bost twyllodrus, ond mae pethau i gadw llygad amdanyn nhw yn cynnwys:

- negeseuon swyddogol yr olwg am 'ailosod cyfrineiriau', 'derbyn iawndal', 'dyfeisiau sganio' neu 'danfon parsel a gollwyd'
- e-byst sy'n llawn 'iaith dechnolegol' a gynlluniwyd i swnio'n fwy credadwy
- anogaeth i weithredu ar unwaith neu o fewn amserlen gyfyngedig

Bydd y neges yn aml yn honni ei bod yn dod gan rywun neu o rywle ag awdurdod (fel banc, neu gwmni ynni). Cofiwch, fydd eich banc (nac unrhyw sefydliad swyddogol arall) **byth** yn gofyn i chi ddarparu gwybodaeth bersonol.
Os oes gennych chi unrhyw amheuon, cysylltwch â'r sefydliad yn uniongyrchol gan ddefnyddio eu gwefan swyddogol neu eu sianeli cyfryngau cymdeithasol. Peidiwch â defnyddio'r dolenni na manylion cyswllt unrhyw negeseuon a anfonwyd atoch.

Helpwch eich staff i adnabod ceisiadau anarferol

Ydy cydweithwyr a staff eich lleoliad yn gwybod beth i'w wneud gyda negeseuon e-bost neu alwadau ffôn anarferol, a lle i gael cymorth? Gofynnwch i chi'ch hun a fyddai rhywun sy'n dynwared unigolyn pwysig (rhiant, rheolwr, neu aelod o'r awdurdod lleol) yn cael ei herio.
Meddyliwch sut gallwch chi annog a helpu'ch staff i gwestiynu ceisiadau amheus neu anarferol, hyd yn oed os ydyn nhw gan unigolion pwysig ar yr olwg gyntaf. Mae cael yr hyder i ofyn 'ydy hwn yn ddilys?' yn gallu golygu'r gwahaniaeth rhwng bod yn ddiogel neu gamgymeriad costus.

Adrodd am negeseuon amheus

Os cewch chi neges gan sefydliad neu unigolyn nad yw'n cysylltu â chi fel arfer, neu os nad yw rhywbeth yn teimlo'n iawn, rhowch wybod amdano.
Byddwch yn helpu'r NCSC i leihau gweithgarwch troseddol, a thrwy hyn, yn atal eraill rhag dioddef.

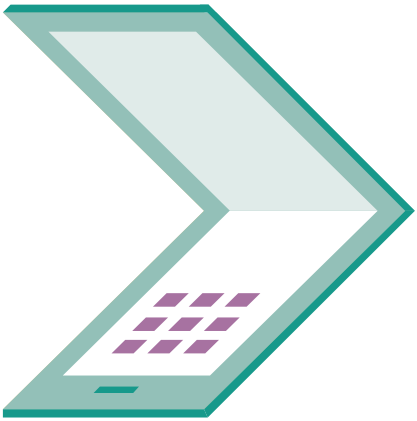
- Os ydych chi wedi derbyn neges e-bost amheus, anfonwch hi i **Suspicious Email Reporting Service** yr NCSC trwy e-bostio **report@phishing.gov.uk.**
- Os ydych chi wedi derbyn **neges destun amheus**, anfonwch hi ymlaen i **7726**. Mae'n wasanaeth rhad ac am ddim ar gyfer rhoi gwybod i'ch cwmni rhwydwaith am negeseuon e-bost twyllodrus

Beth i'w wneud os ydych chi eisoes wedi ymateb

Dyma beth i'w wneud os ydych chi eisoes wedi ymateb:

- Os ydych chi'n meddwl bod unrhyw un o'ch cyfrifon (gan gynnwys cyfrifon e-bost) eisoes wedi'u hacio, darllenwch ein **canllawiau ar adfer cyfrif wedi'i hacio** (sy'n cynnwys beth i gadw llygad amdano).
- Os cawsoch eich twyllo i ddarparu eich manylion banc, cysylltwch â'ch banc a rhowch wybod iddyn nhw.
- Os ydych chi wedi datgelu'ch cyfrinair, dylech **newid y cyfrineiriau** ar unrhyw un o'ch cyfrifon sy'n defnyddio'r un cyfrinair.
- Os ydych chi wedi colli arian, dywedwch wrth eich banc ac **Action Fraud**, y ganolfan riportio seiberdroseddu ar gyfer Cymru, Gogledd Iwerddon a Lloegr.

Gallwch gysylltu â nhw trwy ffonio 0300 123 2040.



Dysgu mwy

I gael rhagor o wybodaeth, ewch i'n gwefan (www.ncsc.gov.uk). Mae'n llawn gwybodaeth ac arweiniad i'ch helpu i ddysgu sut i ddiogelu eich data a'ch dyfeisiau. Efallai y bydd yr adrannau canlynol o fudd i chi:

- **Mynd i'r afael â phroblemau seiber cyffredin**
- **Diogelu eich data a'ch dyfeisiau**
- **CyberAware** (cyngor y llywodraeth ar sut i gadw'n ddiogel ar-lein)