## Seiberddiogelwch ar gyfer ffermwyr

# Cyngor ymarferol ar sut i gadw'n ddiogel

National Cyber Security Centre
a part of GCHQ

NFU

## Sarah Lyons, Dirprwy Gyfarwyddwr yr Economi ac Ymgysylltu â Chymdeithas NCSC

Mae'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC) yn falch iawn o weithio mewn partneriaeth ag Undeb Cenedlaethol yr Amaethwyr i lunio'r canllaw hwn i helpu'r gymuned ffermio i amddiffyn ei hun rhag yr ymosodiadau seiber mwyaf cyffredin.

Os nad ydych chi'n gyfarwydd â'r NCSC, ni yw awdurdod technegol cenedlaethol blaenllaw Llywodraeth y DU ar gyfer seiberddiogelwch a'n nod yw sicrhau mai'r DU yw'r lle mwyaf diogel i fyw a gweithio ar-lein. Er mwyn ein helpu i gyflawni hyn, rydym yn gweithio'n agos iawn gyda chwmnïau a sefydliadau allweddol o bob maint a sector busnes, gan gynnwys Amaethyddiaeth.

Gan fod manteision technoleg yn effeithio ar bob sector, gan gynnwys ffermio a thyfu, rydym am eich helpu i deimlo'ch bod wedi'ch paratoi'n well i ddeall ac ymateb i'r heriau hefyd, heddiw ac i'r dyfodol. Rydym yn ceisio gwneud hyn drwy wneud seiberddiogelwch yn llai brawychus - gan roi cyngor ac arweiniad, mewn ffordd glir sy'n hawdd ei rhoi ar waith.

Mae hyn yn arbennig o bwysig nawr ar gyfer cymunedau ffermio a gwledig sy'n ceisio addasu i fywyd y tu allan i'r Undeb Ewropeaidd ac ymateb i effaith y pandemig ar fodelau busnes.

Ein nod yw cael busnesau i feddwl am seiber yn yr un ffordd ag y byddent yn meddwl am ddiogelu eiddo rhag mathau eraill o droseddau. I wneud hyn, rydym yn gobeithio y bydd y canllaw hwn yn rhoi digon o wybodaeth i'ch rhoi ar ben ffordd neu y bydd yn gwella'ch cadernid seiber presennol.

Er na allwn roi sicrwydd o ddiogelwch ar gyfer eich busnes yn erbyn pob bygythiad yn sgil troseddau seiber, gallwn wella'ch gallu i ddelio gyda nhw a bod yn fwy ymwybodol o bwy all eich helpu.

Y llyfryn hwn yw'r cyntaf o sawl brosiect ar y cyd ac rydym yn edrych ymlaen at weithio gydag Undeb Cenedlaethol yr Amaethwyr a'r sector amaethyddiaeth ehangach. Dim ond gyda'n gilydd y gallwn amddiffyn y byd ffermio ym maes seiberddiogelwch, heddiw ac i'r blynyddoedd a ddaw.

## Pam mae seiberddiogelwch yn bwysig wrth Ffermio

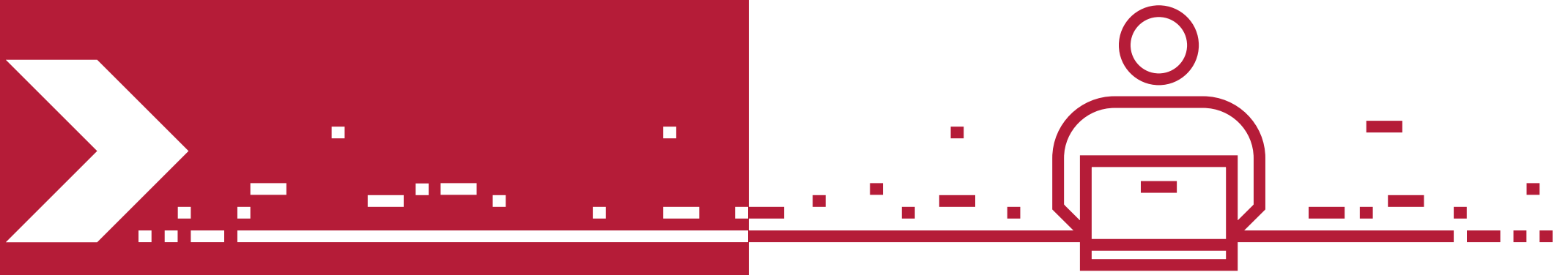
Mae pob un ohonom yn cadw gwybodaeth am ein hunain a'n busnesau yn electronig. Mae hyn yn arbennig o wir yn y sector amaethyddol, sy'n gwneud defnydd o sawl system rhyngrwyd 'clyfar' ynghyd â'r pecynnau e-bost a chyfrifyddu arferol.

Mae'r technolegau cysylltiedig â'r rhyngrwyd hyn wedi dod yn ganolog i'r ffordd rydym ni'n byw ac yn cyflawni ein gwaith bellach. O ganlyniad uniongyrchol i hynny, maen nhw wedi dod yn darged deniadol i droseddwyr seiber. Dyna pam ei bod mor bwysig diogelu pob elfen ddigidol o'ch busnes.

Felly, beth yw elfennau digidol eich busnes chi? Yn gyntaf, eich TG a'ch cyfarpar cyfrifiadurol arall. Mae hyn yn golygu popeth o'r cyfrifiadur lle'r ydych chi'n creu eich negeseuon e-bost ac yn defnyddio'ch meddalwedd rheoli fferm, i'r peiriannau awtomataidd, camerâu diogelwch a ffonau clyfar sy'n eich helpu i redeg eich fferm.

Mae'r ail elfen yn ymwneud â'ch gweithgarwch ar-lein. Mae'n rhaid i chi ystyried yr holl gyfrifon ar-lein rydych chi'n eu defnyddio. Mae hyn yn golygu bancio, e-bost a'r  cyfryngau cymdeithasol yn ogystal â phethau fel y gwasanaeth Taliadau Gwledig, gwasanaethau ar-lein CThEM, siopa ar-lein a storio dogfennau yn y cwmwl (e.e. Office365, Google Docs, Dropbox ac ati).

Mae'r canllaw hwn wedi'i lunio gan NCSC ac Undeb Cenedlaethol yr Amaethwyr er mwyn eich helpu i ddiogelu'ch dyfeisiau a'ch cyfrifon rhan sylw digroeso Troseddwyr Seiber. Trwy ddilyn y camau yn y canllaw hwn, dylech fod mewn lle llawer mwy diogel a chadarn.



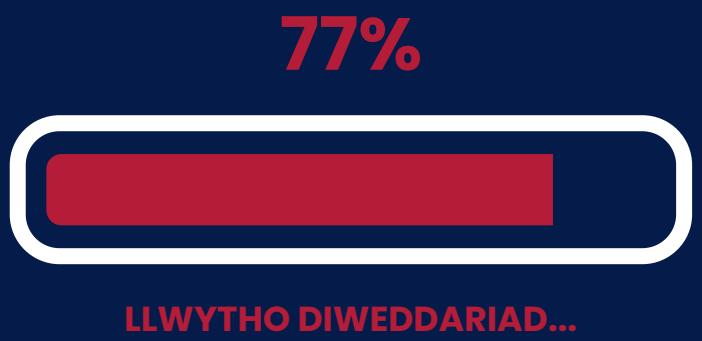
## Diweddaru'ch dyfeisiau

Fel unrhyw beiriant arall, mae angen cynnal a chadw cyfrifiaduron a ffonau symudol a'u gwasanaethau'n rheolaidd er mwyn sicrhau eu bod yn gweithio'n effeithiol ac yn ddiogel.

Gellir gwneud y rhan fwyaf o'r gwaith cynnal a chadw hwn drwy sicrhau bod y system weithredu a'r feddalwedd sydd wedi'i gosod ar eich dyfeisiau yn cael eu diweddaru'n rheolaidd.

Gelwir y broses hon yn 'patsio'.

Y ffordd hawsaf o sicrhau bod eich dyfais a'ch apiau yn cael eu diweddaru yw trwy drefnu bod diweddariadau'n digwydd yn awtomatig. Mae hyn wastad yn wir gyda'r systemau gweithredu mawr: Windows, macOS, iOS ac Android. Fodd bynnag, hwyrach y bydd yn ofynnol i chi wneud y diweddariadau eich hun gydag ambell feddalwedd.



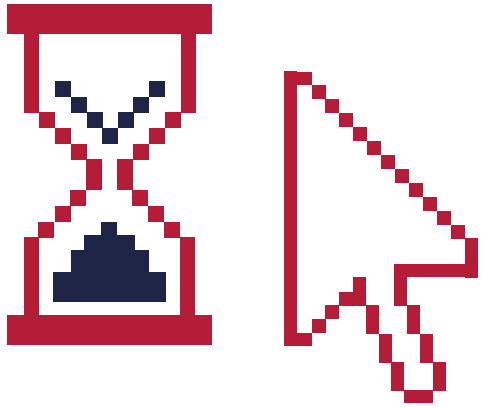

## Hen beiriannau

Os yw'ch cyfarpar cyfrifiadurol yn hen, bydd yn fwy agored i ymosodiad gan feirysau a maleiswedd. Bydd hefyd yn fwy tebygol o ddatblygu namau a allai arwain at golli data.

Yn y pen draw, bydd eich system weithredu (h.y. Microsoft Windows, Apple, macOS ac iOS, Google Chrome OS ac Android) yn darfod ac ni fydd yn derbyn diweddariadau mwyach.

Er enghraifft, ni fydd cyfrifiadur sy'n rhedeg Windows XP yn derbyn diweddariadau mwyach.

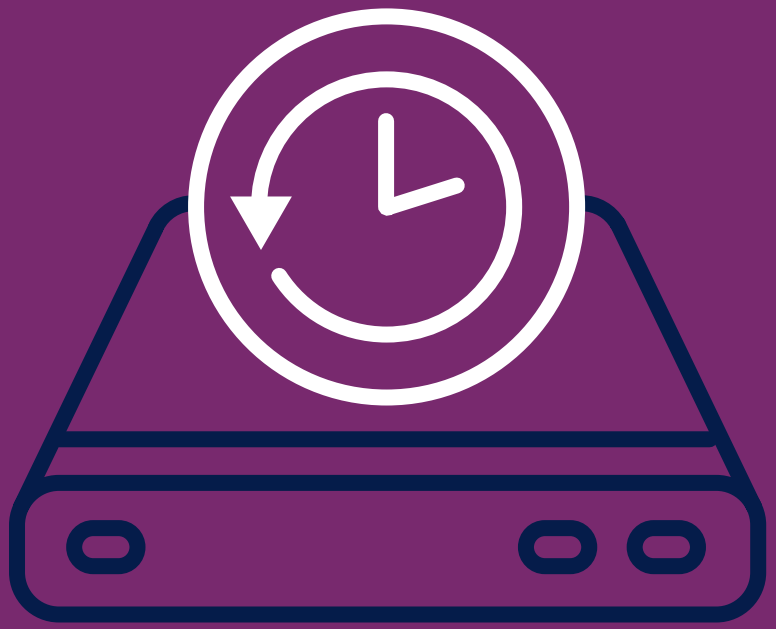
Os yw hyn yn digwydd, dylech ddiweddaru'ch system weithredu neu gael dyfais newydd yn lle'r un dan sylw.



## Cadwch gopi wrth gefn o'ch data

Mae'n debyg eich bod yn dibynnu ar lawer o ddata: e-byst, anfonebau, cysylltiadau, archebion, dyfynbrisiau.

Bydd cadw copïau wrth gefn o ddata pwysig a chadw'r rhain yn ffisegol ar wahân yn eich arbed rhag effeithiau gwaethaf maleiswedd neu ymosodiad meddalwedd wystlo.



## Sut mae cadw copi wrth gefn o'ch data

1

**Nodwch pa ddata sydd angen ei gopïo.**
Dyma'r wybodaeth na fyddech chi na'ch fferm a'ch busnes yn gallu gweithredu hebddi.

2

**Cadwch gopi wrth gefn diogel o'ch ffeiliau pwysig.**
Crëwch gopi wrth gefn yn rheolaidd o'r data sydd bwysicaf i chi, ac efallai ychwanegwch apwyntiad cylchol at eich calendr i'ch atgoffa. Cadwch y copi ar wahân o'ch cyfrifiadur, ar ddyfais storio USB o bosibl, ar yriant caled ar wahân, neu ar gyfrifiadur arall. Gallech hefyd ddefnyddio gwasanaethau cwmwl i gadw copi wrth gefn o'ch ffeiliau, fel na fyddwch yn colli pob copi os oes tân neu os oes lladrad ar y safle.

## Cadwch eich dyfeisiau'n ddiogel

Ffôn, gliniadur, PC a llechen - mae'n debyg y byddwch yn defnyddio mwy nag un ddyfais o ddydd i ddydd.

Dylech gymryd camau i gadw'r rhain i gyd yn ddiogel, yn enwedig os ydych chi'n defnyddio'r un dyfeisiau at ddefnydd busnes a gwaith personol.

**Galluogwch 'password protection**
'Galluogwch gyfrinair sgrin-gloi, PIN, dull adnabod ôl bys/wyneb, neu ddull dilysu arall ar gyfer pob un o'ch dyfeisiau symudol. Cofiwch ddiogelu eich cyfrifiadur cartref a/neu swyddfa hefyd.

**Defnyddiwch gynnyrch amgryptio.**
Mae hyn yn golygu BitLocker ar gyfer Windows, neu FileVault ar gyfer macOS.
Mae'r rhain wedi'u hadeiladu fel rhan o'ch system weithredu a'r cwbl sydd angen i chi ei wneud yw gofalu eu bod ymlaen. Bydd amgryptio'ch data yn atal mynediad heb awdurdod at eich gwybodaeth.

## Dyfeisiau coll neu wedi'u dwyn

Mae'r rhan fwyaf o ddyfeisiau yn cynnwys adnoddau am ddim ar y we y gallwch eu galluogi i wneud y canlynol.....

**Tracio lleoliad y ddyfais**

**Ei gloi o bell**

**Dileu data o bell**

**Adfer copi wrth gefn o ddata sydd wedi'i storio ar y ddyfais.**

## Diogelu'ch fferm rhag maleiswedd

Mae'r gair 'maleiswedd' yn dod o uno dau air: meddal**wedd malei**sus. Dyma'r gair ychydig mwy technegol am feirws cyfrifiadur.

Fel arfer, nod maleiswedd yw dwyn neu gribddeilio arian gennych chi, yn aml drwy ddal eich data yn wystl am arian.

Gall maleiswedd ymosod ar eich gliniadur a'ch ffôn, ond gall hefyd dargedu 'dyfeisiau' llai amlwg. Mae unrhyw beth sy'n cysylltu â'r rhyngrwyd mewn perygl yn sgil bygythiad maleiswedd.

**Er enghraifft, gallai maleiswedd:**

- Gloi eich dyfais neu eich atal rhag ei defnyddio
- Eich atal rhag symud eich cerbydau fferm
- Dwyn, dileu neu amgryptio eich data
- Amharu gydag unrhyw systemau awtomataidd rydych chi'n eu defnyddio
- Defnyddio gwasanaethau sy'n costio arian i chi, fel galwadau ffôn premiwm
- Cyhoeddi eich data fferm cyfrinachol yn gyhoeddus

## Diogelu rhag maleiswedd

**Cadwch gopi wrth gefn diogel o'ch ffeiliau pwysig.**
Crëwch gopi wrth gefn rheolaidd o'r data sydd bwysicaf i chi. Cadwch y copi ar wahân o'ch cyfrifiadur, ac ystyriwch ddefnyddio gwasanaethau cwmwl i gadw copi wrth gefn o'ch ffeiliau.

**Diweddarwch eich system weithredu** a'r apiau rydych chi'n eu defnyddio.
Pan fydd eich meddalwedd yn eich atgoffa bod diweddariadau ar gael, cofiwch ymateb iddyn nhw neu gosodwch eich dyfeisiau i wneud hyn yn awtomatig.

**Gofalwch fod eich cynnyrch gwrthfeirws ymlaen, ac wedi'i ddiweddaru.**
Mae meddalwedd gwrthfeirws yn aml wedi'i gynnwys am ddim mewn systemau gweithredu poblogaidd. Dylid ei ddefnyddio ar bob cyfrifiadur, gliniadur, ac ar ffonau symudol os yw hynny'n bosibl. Er enghraifft, yn Windows, ewch i Gosodiadau/Settings, galluogwch Virus and Threat Protection, a byddwch yn fwy diogel ar unwaith.

**Trowch eich wal dân ymlaen** i greu parth byffer rhwng eich rhwydwaith a'r rhyngrwyd.
Dewch o hyd i'r gosodiadau diogelwch rhwydwaith ar eich dyfais a gwiriwch fod eich wal dân ymlaen.

## Defnyddiwch gyfrineiriau bob amser

Mae'r rhan fwyaf o systemau angen enwau defnyddwyr a chyfrineiriau. Mae troseddwyr yn dibynnu ar y ffaith bod llawer o bobl yn defnyddio'r un cyfrinair ar gyfer pob cyfrif, neu'n defnyddio cyfrineiriau syml fel "cyfrinair".

Mae troseddwyr seiber yn gwerthu cyfuniadau o enwau defnyddwyr a chyfrineiriau wedi'u dwyn y maen nhw'n rhoi cynnig arnyn nhw ar gyfrifon o gwmpas y rhyngrwyd. Maen nhw hefyd yn rhoi cynnig ar gyfrineiriau cyffredin sy'n hawdd eu dyfalu ar hap yn erbyn gwahanol gyfrifon, gan obeithio am y gorau.

Dyma pam y dylech chi ddefnyddio cyfrineiriau ar wahân ar gyfer pob dyfais a chyfrif ar-lein, yn enwedig cyfrifon e-bost.

Lle bynnag y bo hynny'n bosibl, gofalwch fod eich cyfrineiriau yn rhai cryf. Ac ar gyfer eich cyfrifon pwysicaf, gwnewch nhw'n rhai unigryw. Mae canllawiau'r NCSC ar gyfrineiriau ar gael yn **https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0**

## Defnyddio cyfrineiriau yn dda

- **Newidiwch bob cyfrinair diofyn.** Ar gyfer pob dyfais newydd rydych chi'n dechrau ei defnyddio, cofiwch gynnwys eich rhwydwaith Wi-Fi a newidiwch gyfrinair diofyn y gwneuthurwr i gyfrinair newydd o'ch dewis chi.

- **Dewiswch gyfrineiriau cryf.** Cyfunwch dri gair ar hap i greu ymadrodd byr, cofiadwy.

- **Defnyddiwch gyfrinair gwahanol** ar gyfer pob cyfrif ar-lein os gallwch chi, yn enwedig eich prif gyfrif e-bost. Os yw troseddwyr yn gallu cael mynediad at eich e-bost a'i reoli, efallai y gallan nhw ailosod cyfrineiriau a chymryd rheolaeth o'ch cyfrifon eraill.

- **Os ydych chi'n nodi'ch cyfrineiriau ar bapur,** cadwch nhw'n ddiogel, i ffwrdd o'ch dyfais.

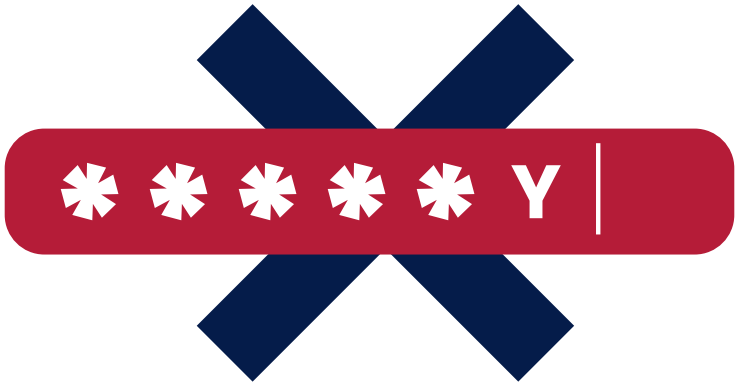
- **Meddyliwch am ddefnyddio rheolwr cyfrineiriau.**
  Er enghraifft, bydd y rhan fwyaf o borwyr gwefannau yn cynnig cadw eich cyfrineiriau ar eich rhan.

## Peidiwch â defnyddio cyfr1n€1r1au gwan

Wrth lunio cyfrinair, peidiwch â defnyddio gwybodaeth y gallai unrhyw un sy'n ceisio torri i mewn i'ch cyfrif ei chanfod amdanoch chi.

**Ni ddylai'ch cyfrineiriau gynnwys:**

- **Enwau teulu**
- **Enw eich anifail anwes**
- **Eich man geni**




- **Eich hoff wyliau**
- **Rhywbeth sy'n gysylltiedig â'ch hoff dîm chwaraeon**
- **Rhestr o rifau (e.e. 123456) neu eiriau fel 'cyfrinair' neu 'qwerty'.**

## Trowch dilysu dau gam ymlaen, 2FA

Mae dilysu dau gam (a elwir hefyd yn 2FA neu'n Dilysu Dau Ffactor) yn nodwedd ddiogelwch am ddim sy'n darparu lefel ychwanegol o ddiogelwch ar gyfer eich cyfrifon ar-lein.

Mae 2FA yn cadarnhau ddwywaith mai chi sydd wir yn ceisio mewngofnodi i'ch cyfrif. Gan olygu, os yw troseddwr yn gwybod eich cyfrinair, bydd yn methu cael mynediad at eich cyfrifon. Felly, os ydych chi'n cael yr opsiwn i droi 2FA ymlaen, ewch amdani.

Gyda 2FA ar waith, mae'n rhaid i unrhyw un sy'n ceisio cael mynediad at eich cyfrif wybod eich cyfrinair yn ogystal â chael mynediad at eich ail dystiolaeth o bwy ydych chi hefyd.

Yn aml, mae'r ail ffynhonnell dystiolaeth hon yn cynnwys anfon cod i'ch ffôn clyfar, neu fod cod yn cael ei greu gan ap dilysu neu ddyfais.

Cymerwch olwg ar y Gosodiadau ar gyfer pob cyfrif pwysig sydd gennych chi i weld a yw 2FA wedi'i alluogi. Ewch i Cyber Aware (**https://www.ncsc.gov.uk/cyberaware/home**) am gyfarwyddiadau cam wrth gam ar sut i droi ymlaen eich 2FA ar gyfer eich e-bost, cyfryngau cymdeithasol a chyfrifon banc ar-lein.

## Diogelu eich presenoldeb ar-lein

Mae nifer o fanteision i gael presenoldeb ar-lein. Gall alluogi busnesau i rannu cynnwys digidol, meithrin cymunedau, cael mynediad at gynulleidfaoedd ehangach a chyfathrebu'n effeithiol gyda'i gilydd.

Mae'n bwysig cymryd camau i sicrhau nad yw'r wybodaeth sy'n cael ei rhannu ar-lein gennych chi na'ch gweithwyr yn gwneud eich busnes yn fwy agored i niwed.

Wrth ddefnyddio'r cyfryngau cymdeithasol, meddyliwch am beth rydych chi'n postio, a phwy all ei weld. Ydych chi wedi ffurfweddu'r opsiynau preifatrwydd fel ei fod ond yn hygyrch i'r bobl rydych chi am iddyn nhw ei weld? Dylech reoli pwy sydd â mynediad at y cyfrifon hyn, gan ofalu bod angen defnyddio cyfrineiriau unigryw a 2FA.

Ar eich gwefan neu gyfrif cyfryngau cymdeithasol, meddyliwch am yr hyn sydd angen i'ch dilynwyr a'ch ffrindiau ei wybod, a pha fanylion nad oes eu hangen (ond a allai fod yn ddefnyddiol i droseddwyr).

Gwnewch yn siŵr fod y cwmni sy'n lletya eich gwefan yn gwmni cyfreithlon gyda'r gosodiadau diogelwch cywir, mae canllawiau pellach gan NCSC a allai fod yn ddefnyddiol ar gael yn **https:// www.ncsc.gov.uk/guidance/moving-business-fromphysical-to-digital**. Meddyliwch hefyd am y diogelwch y gallech fod ei angen os oes gennych chi siop neu system archebu ar-lein.

## Delio gydag e-byst, negeseuon testun a galwadau ffôn sgâm

Bydd neges destun neu e-bost sgâm gyffredin yn ceisio eich argyhoeddi i glicio ar ddolen, gan eich anfon i wefan a allai lawrlwytho feirysau ar eich cyfrifiadur, neu ddwyn eich cyfrineiriau a'ch gwybodaeth bersonol.

Mae rhai sgamiau ar-lein yn hyrwyddo cyfleoedd buddsoddi ffug, yn hysbysebu peiriannau ffug i'w gwerthu drwy'r hyn a allai ymddangos fel gwerthwr cyfreithlon, neu'n honni eu bod o CThEM ac yn cynnig ad-daliadau treth.

Bydd rhai troseddwyr hyd yn oed yn ffonio a chogio eu bod o gwmnïau cyfreithlon mewn ymgais i'ch twyllo i rannu gwybodaeth, a fyddai'n eu galluogi i gymryd arian gennych chi neu gael mynediad at eich cyfrifon busnes.

## Sut i adnabod negeseuon neu alwadau amheus

Y peth cyntaf i'w ystyried wrth dderbyn galwad neu neges yw "ydw i'n disgwyl y neges neu'r alwad hon?" ac "ydy'r anfonwr neu'r galwr yn bwy bynnag y maen nhw'n honni ydyn nhw?". Os nad ydych chi'n siŵr, cadarnhewch drwy gysylltu â'r person neu'r busnes drwy'r manylion cyswllt sydd gennych chi ar eu cyfer mewn dogfen wreiddiol neu ar wefan y busnes. Peidiwch â defnyddio'r rhifau na'r cyfeiriadau sydd wedi'u cynnwys yn y negeseuon amheus.

Cofiwch na fydd yr Asiantaeth Taliadau Gwledig, eich banc nac unrhyw ffynhonnell swyddogol arall, yn gofyn i chi am wybodaeth bersonol mewn e-bost nac mewn neges destun.

## Sut i adnabod negeseuon a galwadau amheus

Mae'r rhan fwyaf o sgamiau yn defnyddio'r un dulliau. Dyma driciau i gadw llygad barcud amdanyn nhw:

**Awdurdod**
Ydy'r neges yn honni i fod gan rywun swyddogol?

**Brys**
Ydych chi'n clywed bod angen i chi ymateb 'ar unwaith' neu 'o fewn 24 awr'?

**Emosiwn**
Ydy'r neges yn gwneud i chi gyffroi, yn ofnus, yn obeithiol neu'n chwilfrydig?

**Prinder**
Ydy'r neges yn cynnig rhywbeth sy'n brin? Gall ofni colli cyfle wneud i chi ymateb yn gyflym.

**Digwyddiadau cyfoes**
Ydych chi'n disgwyl gweld neges fel hon? Yn aml mae troseddwyr yn manteisio ar straeon am bynciau llosg neu adegau penodol o'r flwyddyn: maen nhw'n gwybod dyddiadau ffenestr daliadau Cynllun y Taliad Sylfaenol.

Os ydych chi wedi derbyn e-bost nad ydych chi'n hollol sicr amdani, anfonwch y neges ymlaen at Wasanaeth Hysbysu am E-byst Amheus NSCS, SERS, yn **report@phishing.gov.u**

Dylid anfon negeseuon testun amheus ymlaen am ddim at **7726.**

## Ble i droi am help

**Os ydych chi'n chwilio am wybodaeth am broblemau diogelwch TG cyffredin,** fel e-byst neu wefannau twyllodrus, cyfrif wedi'i hacio neu wedi'i lygru gan faleiswedd, ewch i wefan NCSC yn **www.ncsc.gov.uk**

**Os ydych chi'n derbyn neges gwe-rwydo bosibl,** gallwch roi gwybod i'r NCSC drwy ddefnyddio ein Gwasanaeth Hysbysu am E-byst Amheus, SERS. Anfonwch y neges ymlaen at **report@phishing.gov.uk**. Os gwelir bod y neges yn cysylltu â chynnwys maleisus, bydd yn cael ei dileu neu ei rhwystro, gan helpu i atal eraill rhag dioddef y drosedd hon yn y dyfodol.

**Dylid anfon negeseuon testun amheus ymlaen at 7726.** Mae'r cod byr am ddim hwn yn galluogi eich darparwr i ymchwilio i darddiad y neges destun a gweithredu os yw'r neges yn un faleisus.

**Os ydych chi'n ddigon anlwcus i brofi trosedd seiber,** dylech roi gwybod i Action Fraud drwy ddefnyddio'u hadnodd hysbysu am dwyll yn **www.actionfraud.police.uk**, neu drwy ffonio **0300 123 2040.**

**Os ydych chi'n byw yn yr Alban** dylech roi gwybod i Police Scotland drwy ffonio **101.**

National Cyber Security Centre
a part of GCHQ

NFU

*Mae'r holl gyngor yn seiliedig ar ganllawiau NSCS ym mis Tachwedd 2020. Am ffeiliau parod i'w hargraffu o'r ddogfen hon, ewch i:*

https://www.ncsc.gov.uk/guidance/cyber-security-for-farmers

@ncsc

National Cyber Security Centre