National Cyber Security Centre
a part of GCHQ

NEN
The Education Network

# Seiberddiogelwch mewn ysgolion:
# Awgrymiadau ymarferol i bob un sy'n gweithio ym maes addysg

## Seiberddiogelwch Ysgolion

Mae angen i bob ysgol ofalu am ei data yn ogystal â rheoli'r risgiau sy'n gysylltiedig â defnyddio cyfrifiaduron a gwasanaethau ar rwydweithiau, felly **mae angen i bawb ddilyn rhai egwyddorion sylfaenol seiberddiogelwch da fel yr amlinellir yn y cardiau hyn.**

Mae angen i uwch arweinwyr a llywodraethwyr fod yn ymwybodol bod seiberddiogelwch yn fater rheolaeth a sicrwydd. Wedi'r cyfan, gallai seiberlendid gwael effeithio ar allu ysgol i weithredu, ei henw da a'i rhwymedigaethau cyfreithiol i gadw data personol yn ddiogel.

*Mae seiberddiogelwch yn ymwneud â diogelu'r* ***dyfeisiau*** *rydyn ni i gyd yn eu defnyddio a'r* ***gwasanaethau*** *rydyn ni'n eu cyrchu ar-lein - yn y cartref ac yn yr ysgol - rhag cael eu dwyn neu eu difrodi.*

*Mae'n ymwneud hefyd ag atal mynediad anawdurdodedig i'r symiau anferthol o* ***wybodaeth bersonol*** *rydyn ni'n ei chadw ar y dyfeisiau hyn ac ar-lein.*

## Pam mae seiberddiogelwch o bwys i ysgolion

Mae nifer cynyddol o ysgolion a cholegau'n cael eu heffeithio'n ddifrifol gan seiberddigwyddiadau: o bosibl oherwydd cais gwe-rwydo i ddwyn arian a chyfrineiriau, neu ymosodiad meddalwedd wystlo sy'n amgryptio ffeiliau gan atal mynediad iddynt. Ond pam?

- **Mae llawer o seiberddigwyddiadau yn rhai sydd heb gael eu targedu -** gallan nhw effeithio ar unrhyw ysgol nad oes ganddi lefelau diogelwch sylfaenol.

- **Mae ysgolion yn meddu ar lu o wybodaeth sensitif -** er enghraifft, manylion banc staff a rhieni, gwybodaeth feddygol am fyfyrwyr, cofnodion diogelu. Mae'n rhaid i hyn oll gael ei gadw'n ddiogel ac yn gyfrinachol.

- **Gwneud arian yw nod seiberdroseddwyr.** Maen nhw'n deall bod gwybodaeth sefydliad yn aml yn ddigon pwysig fel y gallai'r sefydliad hwnnw fod yn fodlon talu arianswm i'w chael yn ôl.

## Pwy sy'n gyfrifol am seiberymosodiadau?

### Troseddwyr ar-lein

Mae'r rhain yn dda iawn am adnabod yr hyn sy'n gallu creu gwerth ariannol, er enghraifft dwyn a gwerthu data sensitif, neu ariansymu systemau a gwybodaeth.

### Hacwyr

Unigolion yw'r rhain sy'n meddu ar arbenigedd i amrywiol raddau, sy'n aml yn gweithredu mewn ffordd heb ei thargedu - o bosibl i roi cynnig ar eu sgiliau eu hunain neu darfu ar rywbeth er mwyn diawlineb.

### Mewnwyr maleisus

Mae'r rhain yn defnyddio'u mynediad i ddata neu rwydweithiau sefydliad i gyflawni gweithgarwch maleisus fel dwyn gwybodaeth sensitif i'w rhannu gyda chystadleuwyr.

### Camgymeriadau gonest

Weithiau mae staff, er eu dymuniadau da, yn gwneud camgymeriad, er enghraifft drwy e-bostio rhywbeth sensitif i'r cyfeiriad e-bost anghywir.

### Disgyblion ysgol

Mae rhai myfyrwyr yn mwynhau'r her o roi cynnig ar eu seibersgiliau.

## Cyfrineiriau Cadarn

O'u gweithredu'n gywir, mae cyfrineiriau'n ffordd hawdd, effeithiol, a rhad ac am ddim o helpu i atal defnyddwyr anawdurdodedig rhag cyrchu dyfeisiau neu rwydweithiau. Dyma sut i'w defnyddio'n dda:

- Defnyddiwch gyfrinair gwahanol ar gyfer pob cyfrif / gwasanaeth. Os nad yw hyn yn bosibl yna sicrhewch fod gan eich cyfrifon mwyaf sensitif (e.e. cofnodion myfyrwyr) gyfrinair unigryw.
- Os oes **rhaid** i chi wneud nodyn o'ch cyfrineiriau, dylech eu storio'n ddiogel ac i ffwrdd o'ch dyfais.
- Dylech ystyried defnyddio rheolwr cyfrineiriau - neu ofyn i'ch tîm TG a yw hyn yn opsiwn.
- Defnyddiwch ddull awthentigeiddio dau ffactor (2FA) ar gyfrifon sensitif. Mae hyn yn darparu ffordd o wirio eilwaith mai chi yw'r person rydych chi'n dweud ydych chi.
- Dylech allgofnodi o'ch cyfrif bob tro byddwch yn camu i ffwrdd neu'n stopio defnyddio eich dyfais, hyd yn oed os mai am funud mae hyn. Mae hyn yn berthnasol yn yr ysgol neu tra'n gweithio o gartref.

**Ffordd dda o greu cyfrinair cadarn a chofiadwy yw defnyddio tri gair ar hap. Mynnwch olwg ar wefan NCSC i weld pam mae hyn mor effeithiol**

Dylai cyfrineiriau fod yn hawdd i **chi** eu cofio, ond yn anodd i **rywun arall** eu dyfalu. Rydyn ni'n awgrymu **nad ydych chi'n** cynnwys y canlynol:

- Enw eich partner
- Enw eich plentyn
- Enw eich anifail anwes
- Lle geni
- Hoff wyliau
- Rhywbeth sy'n gysylltiedig â'ch hoff dîm chwaraeon
- Restr o rifau (e.e. 123456) neu eiriau fel 'password' neu 'qwerty'.

## Beth mae pobl yn ei wybod amdanoch chi?

## Beth bydden nhw'n dyfalu y gallech ei ddefnyddio fel cyfrinair? Ceisiwch ofyn iddyn nhw. Gallech gael eich synnu.

## Gochelwch rhag gwe-rwydwyr!

Mewn ymosodiad gwe-rwydo nodweddiadol, mae sgamwyr yn anfon e-byst ffug at filoedd o bobl yn gofyn am wybodaeth sensitif (fel manylion banc) neu'n cynnwys dolenni i wefannau drwg. Maen nhw'n gwneud hyn i ddwyn eich manylion er mwyn eu gwerthu neu o bosibl i gyrchu gwybodaeth eich sefydliad

**Mae angen lleihau nifer yr e-byst gwe-rwydo ar wahanol lefelau - mae arweiniad gennym ar gyfer timau TG ar ein gwefan - ond dylai pob defnyddiwr ddilyn y canllawiau hyn:**

- **'Os yw'n ddrwgdybus, byddwch yn hysbys'.** Gofynnwch bob amser am gyngor os nad ydych yn sicr a yw'r ddolen neu'r e-bost yn ddilys.

- Peidiwch â theimlo'n hurt os ydych chi'n meddwl eich bod wedi cael eich dal allan: mae'n digwydd i ni i gyd o bryd i'w gilydd. Ond **cofiwch adrodd hyn** i'ch Pennaeth neu'ch tîm TG fel y gallent leiafu unrhyw niwed.

- Dysgwch am **dechnegau gwe-rwydo cyffredin** (gweler drosodd)

## Arwyddion bod gwe-rwydo ar waith

Mae rhai e-byst gwe-rwydo'n fwy soffistigedig nag eraill, ond mae'n helpu i fod yn ymwybodol o rai o'r cliwiau amlycaf. Mae'r rhain yn cynnwys:

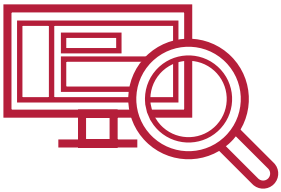
**A oes delweddau o logos o ansawdd gwael?**

**A oes gwallau sillafu neu ramadegol?**

**A yw'n eich annerch chi fel 'annwyl gyfaill' yn hytrach nag yn ôl eich enw?**

**A yw'n gofyn i chi weithredu ar frys?**

**A yw'n cyfeirio at neges flaenorol nad oes gennych gof o'i gweld?**



## Ffyn Cof neu Gofion Bach

Mae ffyn cof yn ffordd gynorthwyol o gludo data ond **maen nhw hefyd yn gallu lledu feirysau a maleiswedd o un cyfrifiadur neu rwydwaith i'r llall.**

Gallai fod yn syniad i chi feddwl am ffyrdd eraill o drosglwyddo data sy'n gallu cynnig mwy o ddiogelwch, e.e. arbed gwaith i ddarparwr storio ar-lein neu ei e-bostio atoch chi'ch hun.

## Ond os oes rhaid i chi ddefnyddio ffon gof, gwnewch hynny'n ofalus.

- Dim ond ffyn cof a ddarparwyd i chi gan eich ysgol y dylech eu defnyddio. Byddwch yn wyliadwrus a pheidiwch â defnyddio'ch rhai eich hun na rhai rydych wedi'u cael am ddim, h.y. rhai sydd wedi'u rhoi i chi.

- Sicrhewch fod cyfrinair ar y ffon gof. Mae hyn yn golygu y caiff y data sydd wedi'i storio arni ei amgryptio fel nad oes modd ei gyrchu os caiff y ffon gof eich dwyn neu ei cholli.

- Os oes opsiwn i redeg rhaglenni o'r ffon gof yn awtomatig, sicrhewch fod hwn wedi'i ddiffodd fel bod yn rhaid gwirio ffeiliau'n gyntaf.

## Gweithio o gartref

Chi sy'n gyfrifol o hyd am gadw gwybodaeth gwaith yn ddiogel pan fyddwch chi'n ei chyrchu gartref. Gall yr awgrymiadau hyn helpu i leiafu'r posibilrwydd bod digwyddiad seiberddiogelwch yn trosglwyddo o ddyfeisiau'r cartref i rwydwaith yr ysgol neu'r ffordd arall.

- Defnyddiwch feddalwedd gwrth-feirws cyfoes ar eich dyfeisiau eich hun.
- Lawrlwythwch yr holl ddiweddariadau meddalwedd cyn gynted ag y maent ar gael.
- Sicrhewch fod cyfrineiriau ar eich **holl** ddyfeisiau. (Hyd yn oed os mai dim ond ar gyfer eich gwaith rydych yn defnyddio'ch gliniadur, gallai gael ei gydamseru i'ch ffôn neu'ch llechen).
- Newidiwch unrhyw gyfrineiriau diofyn ar ddyfeisiau neu feddalwedd - gan gynnwys system ddi-wifr (Wi-Fi) eich cartref.
- Gosodwch ddull awthentigeiddio dau ffactor (2FA) ar gyfer cyfrifon sensitif. Gofynnwch i'ch adran TG os yw'n ymddangos nad yw hyn yn opsiwn.

**Mae digon o gyngor pellach ar gael ar ein gwefan, gan gynnwys:**

**Top Tips for Staff (Saesneg yn unig)** - ein pecyn e-ddysgu i'ch helpu i ddysgu sut i gadw'n ddiogel ar-lein.

Mae **The Small Business Guide (Saesneg yn unig)** yn llawn camau syml y gellir eu rhoi ar waith i leihau'r posibilrwydd y cewch eich dal mewn seiberddigwyddiad yn y gwaith neu gartref.

Mae arweiniad penodol am **gyfrineiriau a gwe-rwydo** ar gael yn www.ncsc.gov.uk

**I'r sawl sy'n rheoli TG ysgol:**

**Cyber Essentials (Saesneg yn unig)** - pum cam allweddol i warchod yn erbyn seiberfygythiadau cyffredin.

**Ten Steps to Cyber Security (Saesneg yn unig)** - i symud pethau ymlaen ychydig ymhellach: mae'n rhannu'r dasg o warchod rhwydweithiau yn ddeg cam hanfodol.

**Exercise in a Box (Saesneg yn unig)** - teclyn byw sy'n cynnig ymarferion pen-bwrdd a rhai a efelychir i roi cynnig arnyn nhw a dysgu wrthyn nhw.

***Adrodd:***

*Os yw'ch ysgol yn dioddef digwyddiad seiberddiogelwch neu'n cael ei heffeithio gan dwyll (e.e. colli arian o ganlyniad i e-bost gwe-rwydo neu systemau TG yn cael eu cyfaddawdu), dylech adrodd hyn i* **Action Fraud** *drwy ffonio 0300 123 2040 neu fynd i www.actionfraud.police.uk*

## Symleiddio Seiberddiogelwch

Gall camau syml wneud y byd o wahaniaeth, felly cofiwch y canlynol:

- Peidiwch byth ag anwybyddu diweddariadau meddalwedd - maen nhw'n cynnwys patsys sy'n eich cadw chi a'ch ysgol yn ddiogel
- Cofiwch gloi eich dyfais bob amser pan nad ydych yn ei defnyddio
- Dim ond o fannau apiau swyddogol fel Google Play neu App Store Apple y dylech lawrlwytho apiau a meddalwedd
- Peidiwch â rhannu cyfrifon ag eraill
- Peidiwch ag ofni herio polisïau neu brosesau sy'n gwneud eich gwaith yn anodd. Nid yw diogelwch sy'n eich rhwystro rhag gwneud eich gwaith yn gweithio!
- Crëwch ddiwylliant o holi – os yw'n edrych yn rhyfedd, mynnwch farn arall

Mae'r holl gyngor wedi'i seilio ar arweiniad NCSC ym mis Awst 2019. I gael ffeiliau o'r cardiau hyn sy'n barod i'w hargraffu, ewch i www.ncsc.gov.uk/information/resources-for-schools

@ncsc

National Cyber Security Centre