National Cyber Security Centre
a part of GCHQ

# Seiberddiogelwch:
# Awgrymiadau Ymarferol ar gyfer Amddiffyn Eich Sefydliad Ar-lein

## Seiberddiogelwch Sefydliadol

Mae angen i bob sefydliad edrych ar ôl ei ddata yn ogystal â rheoli'r risgiau o ddefnyddio gwasanaethau ar-lein, ac felly **mae angen i bawb ddilyn rhai egwyddorion sylfaenol seiberddiogelwch da fel yr amlinellir yn y cardiau.**

Rhaid i berchnogion a gweithwyr sefydliadau fod yn ymwybodol bod seiberddiogelwch yn fater rheoli a sicrhau. Wedi'r cyfan, gallai hylendid seiber gwael effeithio ar allu sefydliad i weithredu, ei enw da a'i rwymedigaethau cyfreithiol i gadw data personol yn ddiogel.

*Mae seiberddiogelwch yn ymwneud â diogelu'r **dyfeisiau** rydyn ni i gyd yn eu defnyddio a'r gwasanaeth rydyn ni'n ei gyrchu ar-lein – gartref ac yn y gwaith – rhag dwyn a difrod.*

*Mae hefyd yn ymwneud ag atal mynediad heb awdurdod i'r llawer iawn o **wybodaeth bersonol** rydyn ni'n ei storio ar y dyfeisiau hyn ac ar-lein.*

## Pam Mae Seiberddiogelwch yn Bwysig

Mae nifer cynyddol o sefydliadau yn cael eu heffeithio'n ddifrifol gan ddigwyddiadau seiber: efallai ymgais gwe-rwydo i ddwyn arian a chyfrineiriau, neu ymosodiad meddalwedd wystlo sy'n amgryptio ffeiliau sy'n atal mynediad. Ond pam?

- **Mae llawer o ddigwyddiadau seiber heb darged penodol.**
  Gallant effeithio ar unrhyw sefydliad nad oes ganddo lefelau sylfaenol o ddiogelwch.

- **Mae gan sefydliadau ddigon o wybodaeth sensitif.**
  Er enghraifft, cofnodion sefydliad, gwybodaeth taliadau cwsmeriaid, manylion personol a chyfrineiriau. Rhaid cadw hyn i gyd yn ddiogel ac yn gyfrinachol.

- **Mae troseddwyr seiber eisiau gwneud arian.**
  Maent yn deall bod gwybodaeth sefydliad yn aml yn ddigon pwysig i'r sefydliad hwnnw ac y gallent fod yn barod i dalu pridwerth i'w chael yn ôl.

## Pwy sydd y tu ôl i ymosodiadau seiber?

### Troseddwyr ar-lein

Maent yn dda iawn am nodi'r hyn y gellir pennu gwerth arno, er enghraifft dwyn a gwerthu data sensitif, neu ddal systemau a gwybodaeth i bridwerth.

### Hacwyr

Unigolion sydd â graddau amrywiol o arbenigedd, yn aml yn gweithredu mewn ffordd heb dargedau penodol – efallai i brofi eu sgiliau eu hunain neu achosi aflonyddwch er ei fwyn.

### Mewnwyr maleisus

Maent yn defnyddio eu mynediad at ddata neu rwydweithiau sefydliad i gynnal gweithgaredd maleisus, megis dwyn gwybodaeth sensitif i'w rhannu â chystadleuwyr.

### Camgymeriadau Gonest

Weithiau mae staff, gyda'r bwriadau gorau, yn gwneud camgymeriad yn unig, er enghraifft trwy e-bostio rhywbeth sy'n sensitif i'r cyfeiriad e-bost anghywir.

## Beth yw'r prif fygythiadau i sefydliadau?

### Meddalwedd Wystlo

Meddalwedd maleisus sy'n golygu na ellir defnyddio data neu systemau nes bod y dioddefwr yn gwneud taliad.

### Gwe-rwydo

E-byst torfol heb dargedau penodol a anfonir at lawer o bobl yn gofyn am wybodaeth sensitif (megis manylion banc) neu'n eu hannog i ymweld â gwefan ffug.

### Feirws

Rhaglenni a all hunan-ddyblygu ac sydd wedi'u cynllunio i heintio rhaglenni neu systemau meddalwedd cyfreithlon. Math o ddrwgwedd.

### Peryglon Mewnol

Y potensial i ddifrod gael ei wneud yn faleisus neu'n anfwriadol gan ddefnyddiwr cyfreithlon sydd â mynediad breintiedig i systemau, rhwydweithiau neu ddata.

## Byddwch yn Seiber Ymwybodol

- **Crëwch gyfrinair ar wahân ar gyfer eich cyfrifon sy'n dra phwysig i'r sefydliad.**
  Mae eich cyfrifon yn cynnwys gwybodaeth sensitif am eich cwsmeriaid, eich sefydliad a gwybodaeth ariannol. Os nad yw'ch cyfrifon yn ddiogel, gallai eich sefydliad fod mewn perygl o ddigwyddiad seiber.

- **Crëwch gyfrineiriau cryf gan ddefnyddio tri o eiriau ar hap.**
  Gellir hacio cyfrineiriau gwan mewn eiliadau. Po hiraf a mwyaf anarferol yw eich cyfrinair, y cryfaf y daw a'r anoddaf yw ei hacio.

- **Cadwch eich cyfrineiriau yn eich porwr.**
  Mae'n arfer da defnyddio cyfrineiriau gwahanol ar gyfer y cyfrifon sy'n bwysicaf i chi. Wrth gwrs, gall cofio llawer o gyfrineiriau fod yn anodd, ond os ydych chi'n eu cadw yn eich porwr yna does dim rhaid i chi wneud hynny.

Seiber **Ymwybodol** cyberaware.gov.uk

Seiber Ymwobodol yw cyngor y llywodraeth ar sut i gadw'n ddiogel ar-lein.

- **Trowch Ddilysu Dwy Ffactor (2FA) ymlaen.**
  Mae 2FA yn lleihau'r risg o gael eich hacio trwy ofyn i chi ddarparu ail ffactor o wybodaeth, megis derbyn testun neu god wrth fewngofnodi, i wirio mai chi yw pwy ydych chi'n dweud ydych chi.

- **Cadwch eich dyfais sefydliad yn gyfredol**
  Sicrhewch fod gan eich holl ddyfeisiau'r diweddariadau meddalwedd diweddaraf i leihau'r risg o seiber-ddigwyddiadau. Bydd hyn yn sicrhau bod eich holl ddyfeisiau'n cynnwys y nodweddion diogelwch diweddaraf.

- **Gwnewch gopi wrth gefn o ddata sefydliadol pwysig a chysylltiadau allweddol**
  Trwy wneud copi wrth gefn o'ch data, gall eich sefydliad barhau i weithredu hyd yn oed os ydych chi'n dioddef digwyddiad seiber. Gall copïau wrth gefn gynnwys copïau papur, cyfryngau y gellir eu tynnu neu gopïau wrth gefn yn y cwmwl.**cyberaware.gov.uk**

## Paratoi ar gyfer digwyddiad seiber

Er bod gweithredu rheolaethau diogelwch da yn bwysig, nid oes y fath beth â diogelwch perffaith.

Mae pob sefydliad mewn perygl o ddigwyddiad seiber posib, felly mae'n hanfodol eich bod chi'n paratoi'ch ymateb ac yn cynllunio'ch adferiad pe bai digwyddiad seiber.

## Beth allwch chi ei wneud i baratoi ar gyfer digwyddiad?

- **Nodwch wybodaeth electronig tra phwysig**
  Megis manylion cyswllt, calendrau e-bost, a dogfennau hanfodol. Hefyd nodwch y systemau a'r adnoddau allweddol i gadw'ch sefydliad i redeg.

- **Gwnewch gopi wrth gefn rheolaidd o wybodaeth hanfodol**
  Gwiriwch yn rheolaidd bod y copi wrth gefn yn gweithio i sicrhau y gallwch adfer gwybodaeth ohono.

- **Gwnewch restr o'r partneriaid allweddol rydych chi'n eu defnyddio i redeg eich sefydliad**
  Bydd hyn yn cynorthwyo'ch ymateb pe bai digwyddiad a bydd yn eich galluogi i gadw'ch sefydliad yn weithredol all-lein neu os na fydd systemau ar gael. e.e. rhifau cyswllt cyflenwyr, rhif cymorth TG.

- **Gwnewch gynllun digwyddiad** a'i gadw'n ddiogel fel y gallwch ei ddefnyddio os yw'ch offer yn cael ei ddwyn neu ei ddifrodi gan ddigwyddiad seiber.

**Gweler ein canllaw llawn i gael mwy o wybodaeth ar sut i baratoi a chynllunio.**
https://www.ncsc.gov.uk/collection/small-organisation-guidance--response and-recovery

## Riportio Digwyddiad

**Beth yw digwyddiad?**
Mae digwyddiad seiber yn fynediad heb awdurdod (neu ymgais i gael mynediad) i systemau TG sefydliad. Gall y rhain fod yn ymosodiadau maleisus (megis meddalwedd wystlo neu ymosodiadau gwe-rwydo), neu gallent fod yn ddigwyddiadau damweiniol (megis difrod gan dân/ llifogydd/lladrad).

**Riportio**
Os yw'ch sefydliad yn dioddef digwyddiad seiber neu os yw twyll yn effeithio arno (e.e. arian a gollwyd o ganlyniad i e-bost gwe-rwydo neu os yw'ch systemau TG yn cael eu peryglu), riportiwch ef i **Action Fraud** trwy ffonio 0300 123 2040 neu ewch i **www.actionfraud.police.uk** neu yn yr Alban trwy ganolfan alwadau 101 Police Scotland.

Os ydych wedi derbyn e-bost nad ydych yn hollol siŵr amdano, anfonwch ef ymlaen at y Gwasanaeth Riportio E-byst Amheus (SERS): **report@phishing.gov.uk**

## Symud eich sefydliad o'r corfforol i'r digidol.

Os ydych chi'n symud neu'n rhedeg eich sefydliad ar-lein ar hyn o bryd bydd hyn yn cyflwyno risgiau newydd, trwy roi mwy o ddibyniaeth ar dechnolegau digidol megis gwe-letya, prosesu cardiau credyd, ac offer cynhyrchiant megis e-bost, fideo a sgwrsio. Bydd cael perthynas dda â'ch darparwr/ darparwyr gwasanaeth TG yn help mawr gyda hyn.

Os ydych chi'n siarad yn uniongyrchol â'ch cyflenwr neu os ydych chi'n gyfrifol am eich TG eich hun, bydd y pwyntiau canlynol yn eich helpu i sicrhau bod diogelwch ar reng flaen unrhyw wasanaeth newydd rydych chi'n penderfynu ei ddefnyddio.

- **Clytiau a Diweddariadau**
  Gofynnwch i'ch darparwyr pa mor aml maen nhw'n clytio'r gwasanaethau rydych chi'n eu defnyddio, a gwiriwch unrhyw gontractau neu CLGau i sicrhau bod clytio yn cael ei gynnwys.

- **Copïau Wrth Gefn**
  Pa fath o drefniadau ar gyfer copïau wrth gefn sydd ar waith a pha mor aml y mae'r rhain yn cael eu profi? Dylech wybod pa mor aml y gwneir copi wrth gefn o'ch data, ble mae'n cael ei storio, a phwy sydd â mynediad iddo.

- **Mynediad:**
  A yw'ch data (a data eraill y mae gennych gyfrifoldeb amdanynt) yn cael eu diogelu'n iawn? A ydych chi'n gallu rhoi 2FA ar waith i gyfyngu mynediad i'ch data a'ch gwasanaethau?

- **Logiau**
  A yw logiau'n cael eu cadw at ddibenion diogelwch? Gall logio chwarae rhan hanfodol wrth ddiagnosio unrhyw broblemau. Bydd logiau hefyd yn amhrisiadwy wrth ymateb i ddigwyddiadau diogelwch ac adfer ohonynt.

- **Ymateb i Ddigwyddiad**
  Beth fydd yn digwydd os aiff pethau o chwith? Dylai darparwyr gwasanaeth weithredu ar y rhagdybiaeth y byddant yn cael eu hymosod arnynt. Dylai fod yn glir sut a phryd y byddant yn ymgysylltu â chi yn ystod digwyddiad diogelwch.

Darganfyddwch fwy:

https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital

## Fe welwch yr holl gyngor ac arweiniad hwn a mwy ar ein gwefan:

---

- **Canllaw Busnesau Bach**
  Sut i wella eich seiberddiogelwch; cyngor fforddiadwy, gweithredadwy i sefydliadau.
  https://www.ncsc.gov.uk/smallbusiness

- **Canllaw Elusennau Bach**
  Sut i wella seiberddiogelwch yn eich elusen - yn gyflym, yn hawdd ac am gost isel.
  https://www.ncsc.gov.uk/collection/charity

- **Canllaw Ymateb ac Adfer**
  Canllawiau sy'n helpu sefydliadau bach i ganolig i baratoi eu hymateb i ddigwyddiad seiber a chynllunio eu hadferiad.
  https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

- **Syniadau Da i Staff**
  Gellir cwblhau pecyn e-ddysgu NCSC 'Top Tips for Staff' ar-lein, neu ei ymgorffori yn eich platfform hyfforddi eich hun. Fe'i cynlluniwyd yn fwriadol ar gyfer cynulleidfa annhechnegol gydag awgrymiadau sy'n ategu unrhyw bolisïau a gweithdrefnau presennol
  https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

- **Ymarfer mewn Bocs**
  Offeryn ar-lein am ddim sy'n helpu sefydliadau i ddarganfod pa mor gydnerth ydyn nhw yn wyneb seiber-ymosodiadau ac ymarfer eu hymateb mewn amgylchedd diogel
  https://www.ncsc.gov.uk/information/exercise-in-a-box

- **Hanfodion Seiber**
  Mae cynllun ardystio a gefnogir gan y llywodraeth, Hanfodion Seiber, yn eich helpu i warchod eich sefydliad rhag y bygythiadau seiber mwyaf cyffredin a dangos eich ymrwymiad i seiberddiogelwch.
  https://www.ncsc.gov.uk/cyberessentials/overview

- **Gweithio gartref**
  Sut i sicrhau bod eich sefydliad yn barod ar gyfer cynnydd mewn gweithio gartref, a chyngor ar sylwi ar e-byst sgam coronafeirws (COVID-19)
  https://www.ncsc.gov.uk/guidance/home-working

- **Cynadledda Fideo**
  Canllawiau i'ch helpu chi i ddewis, ffurfweddu a defnyddio gwasanaethau cynadledda fideo megis Zoom a Skype yn eich sefydliad
  https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

- **Symud eich sefydliad o gorfforol i ddigidol**
  Cwestiynau diogelwch i'w gofyn i'ch darparwyr gwasanaeth TG wrth redeg eich sefydliad ar-lein
  https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital

- **Deg Cam i Seiberddiogelwch**
  Ewch â phethau ychydig ymhellach: rhannwch y dasg o amddiffyn rhwydweithiau yn ddeg cydran hanfodol.
  10 steps to cyber security - NCSC.GOV.UK

## Cylchlythyr Sefydliadau Bach

Os hoffech dderbyn cyngor a diweddariadau rheolaidd gennym ni gallwch ymuno â'n cylchlythyr misol a grëwyd yn benodol ar gyfer sefydliadau bach sy'n chwilio am y wybodaeth a'r cyngor diweddaraf ar seiberddiogelwch.

Gallwch danysgrifio yn:
**https://www.eventbrite.co.uk/e/ncsc-small-organisations-newsletter-registration tickets-142219336865**