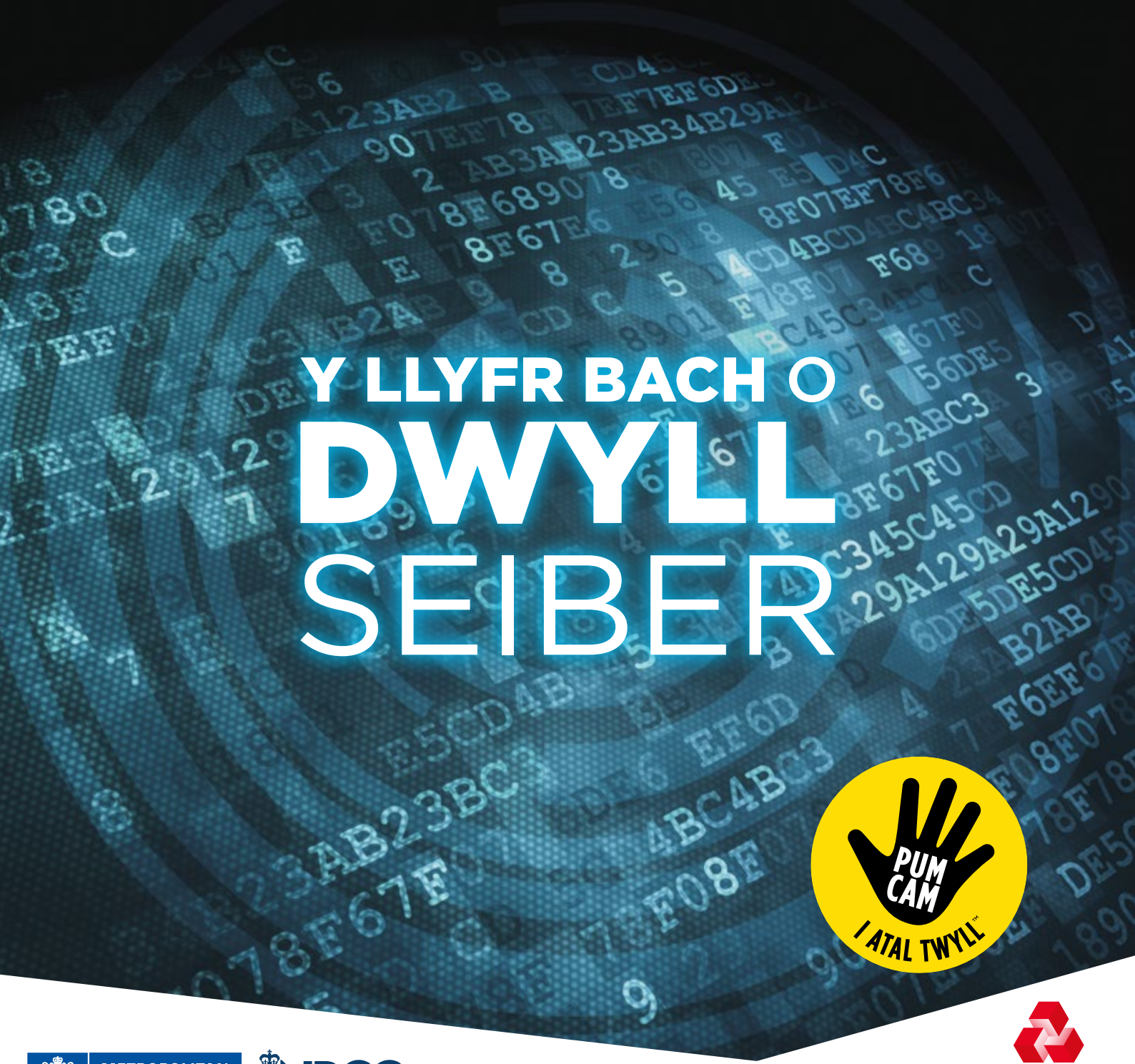
Y LLYFR BACH O DWYLL SEIBER



METROPOLITAN POLICE

NPCC National Police Chiefs' Council

NatWest Cymru

Annwyl Gwsmeriaid,

Yn NatWest rydym wedi ymrwymo i gynorthwyo ein cwsmeriaid a'n cymunedau i'w diogelu eu hunain rhag twyll ac ofn twyll.

Rydym yn credu mai addysg yw'r allwedd ar gyfer atal hyn ac felly rydym yn falch iawn o fod yn gweithio gyda Heddlu Llundain i gyflwyno'r canllaw addysgiadol hwn i chi.

Gobeithio y bydd y llyfr hwn o gymorth i chi amddiffyn eich busnes a'ch cwsmeriaid rhag Trosedd Seiber.

Yn NatWest, byddwn yn monitro cyfrifon 24/7 gan ddefnyddio technegau soffistigedig i adnabod twyll, sylwi ar weithgarwch amheus a helpu i ddiogelu ein cwsmeriaid.

Boed chi'n bancio ar lein neu'n defnyddio ein ap Bancio Symudol, gallwch fod yn dawel eich meddwl fod ein Haddewid Bancio Diogel yn eich amddiffyn. Ar ein gwefan **natwest.com** mae gwybodaeth ychwanegol am yr addewid hwn. Byddwch hefyd yn gallu lawrlwytho meddalwedd sy'n helpu i'ch amddiffyn ar y we.

Mae ein staff wedi'u hyfforddi'n drwyadl i gefnogi cwsmeriaid a ddioddefodd dwyll, neu sy'n meddwl iddyn nhw ddioddef twyll. Felly ni waeth pa mor ddibwys rydych yn meddwl yw eich ymholiad neu bryder, ddylech chi fyth fod ofn gofyn – rydym yma i helpu.

Marcelino Castrillo
Rheolwr-Gyfarwyddwr, Bancio Busnes

FALCON
FRAUD AND LINKED CRIME ONLINE

Pleser mawr i mi yw cyflwyno'r Llyfr Bach o Dwyll Seiber, yr ychwanegiad diweddaraf at frand y Llyfr Bach o Dwyll Mawr.

Mae technoleg yn datblygu'n gyflym ac er ei bod yn rhoi cyfleoedd gwych i wella prosesau busnes, cyfathrebu'n fwy effeithiol ac arwain at fwy o ffyniant, y mae hefyd yn rhywbeth y gall troseddwyr ei gamddefnyddio.

Fe gafodd y llyfryn hwn ei ddatblygu i'ch cynorthwyo i gymryd y camau angenrheidiol i amddiffyn eich busnes a'ch cwsmeriaid rhag trosedd seiber.

Mae Gwasanaeth Heddlu Llundain (MPS) wedi cydnabod y ffordd newidiol y mae busnesau yn gweithredu, ac yn union fel mae angen diogelwch rhag ymyrraeth ar swyddfa neu warws, y mae'r un peth yn wir ar gyfer eich presenoldeb ar lein.

Ar ôl ffurfio FALCON, uned sy'n ymroi i ymchwilio i dwyll a throsedd seiber, mae'r MPS wedi ymrwymo i fynd i'r afael â throseddu ar lein, a thrwy greu tîm Amddiffyn Seiber mae'n gallu cynnig cyngor a chefnogaeth i fusnesau sy'n awyddus i fod yn fwy diogel ar lein.

Gobeithio y bydd y llyfryn yn ddefnyddiol ac addysgiadol ac y bydd yn eich annog i adolygu eich prosesau a'ch trefniadau diogelwch ar lein, gan eich galluogi i amddiffyn eich busnes yn y byd ar lein.

Neil Ballard
Ditectif Uwcharolygydd
Heddlu Llundain

CYNNWYS

TWYLL SEIBER

CYFLWYNIAD

Mae tîm FALCON (Twyll a Throsedd Cyswllt Ar Lein) Gwasanaeth Heddlu Llundain yn falch o gyflwyno'r Llyfr Bach o Dwyll Seiber.

Fe gafodd y llyfryn hwn ei gynllunio'n benodol i gynnig cyngor i fusnesau bach a chanolig am aros yn ddiogel yn y byd seiber. Mae busnesau bach a chanolig i'w cael ym mhobman: ar y stryd fawr, ar stadau diwydiannol, ar lein neu gartref ac maen nhw'n hanfodol ar gyfer llwyddiant economi Prydain yn gyffredinol.

Gyda hyn a hyn o adnoddau ar gael ac amodau economaidd cythryblus mae'n bosib y bydd busnesau bach a chanolig yn rhoi blaenoriaeth i arloesi a thwf dros ddiogelwch ar lein a lleihau risg. Yn aml, bydd y materion hyn yn cael eu hystyried yn gostus, yn feichus ac yn bethau a fydd yn cymryd llawer o amser. Fodd bynnag, mae'n bwysig fod y meysydd hyn yn cael eu cydnabod a'u hasesu a bod cwmnïau yn ymwybodol o'r risgiau o du troseddwyr seiber.

Ni waeth ym mha fusnes ydym ni, mae pob un ohonom yn dibynnu ar y rhyngrwyd. Rydym yn ei ddefnyddio i brynu a gwerthu, cysylltu â'n cwsmeriaid a'i ddefnyddio i gael cefnogaeth logistaidd. Ond gyda'r holl gyfleoedd sy'n gysylltiedig â'r rhyngrwyd, mae'n bwysig cofio'r risgiau.

Bob dydd mae ymosodiadau'n digwydd yn erbyn miloedd o systemau cyfrifiadurol leled y byd. Mae yna droseddwyr sy'n manteisio ar eu gallu i fod yn anhysbys yn y byd ar lein i dwyllo, hacio a dwyn os bydd cyfle i wneud hynny.

Os bydd ymosodiad yn llwyddo, fe allai gael effaith ysgubol ar fusnes.

Fe all niwed i enw da a cholled ariannol arwain at gwmni yn mynd i'r wal. Fe all dwyn neu golli data gael cryn effaith ar enw da cwmni, gan gynnwys cwsmeriaid yn colli hyder, a gall arwain at ddirwyon sylweddol gan Swyddfa'r Comisiynydd Gwybodaeth.

DIOGELU EICH HUN

Dyw hyn ddim yn golygu na ddylai eich busnes ddefnyddio'r rhyngrwyd. Trwy weithredu ychydig o brosesau diogelwch syml a gwneud staff yn ymwybodol o'r bygythiadau, gallwch wneud gwahaniaeth sylweddol i'ch siawns o ddioddef yn sgil troseddwr seiber.

Mae'r llyfryn hwn yn anelu at dynnu sylw at fathau cyffredin o drosedd seiber a'r ffyrdd y gallwch eich amddiffyn eich hun. Nid yw hon yn rhestr hollgynhwysfawr, gan fod pethau'n newid drwy'r adeg, ond trwy ddilyn y cyngor fe allwch amddiffyn eich systemau yn well a gwella gwybodaeth eich staff sy'n eu defnyddio.

BYDDAI TUA 80% O YMOSODIADAU HYSBYS YN METHU TRWY SEFYDLU ARFERION SYLFAENOL AM DDIOGELWCH AR GYFER EICH POBL, PROSESAU A THECHNOLEG

Syr Iain Lobban
Cyfarwyddwr GCHQ, 2014

TWYLL SEIBER

TUEDDIADAU PRESENNOL O RAN TWYLL SEIBER

Yn 2014 fe wnaeth Swyddfa'r Maer dros Blismona a Throsedd (MOPAC) lunio ei Strategaeth ar gyfer Troseddau Busnesau. Nodwyd yn yr adroddiad bod trosedd seiber yn broblem sylweddol oedd ar gynnydd ym mhob sector o'r gymdeithas, gan gynnwys busnes. Nodwyd hefyd bod y rhyngrwyd wedi'i gwneud yn haws cyflawni twyll, gydag amcangyfrifon yn awgrymu bod 57% o adroddiadau am dwyll yn 2012/13 yn digwydd ar y we.

Mae Arolwg Torri Diogelwch Gwybodaeth y PWC a ryddhawyd ym mis Mehefin 2015 yn adrodd bod 90% o sefydiadau mawr a 74% o fusnesau bach a chanolig wedi wynebu achosion o danseilio diogelwch, i fyny o 81% a 60% y flwyddyn flaenorol. Mae amcangyfrifon o gostau'r tanseilio hwn rhwng £1.46m a £3.14m ar gyfer sefydliadau mawr a £75k - £311k ar gyfer busnesau bach a chanolig.

Mae enghreifftiau o ymosodiadau seiber hefyd wedi cynyddu o flwyddyn i flwyddyn. Yn ôl Swyddfa Genedlaethol Cudd-wybodaeth Twyll (NFIB), rhan o Action Fraud, canolfan riportio twyll a throsedd seiber, cafwyd cadarnhad bod tua 109,000 o achosion o droseddau seiber wedi'u riportio iddynt yn 2015. Roedd hyn yn gynnydd o 95,000 yn y flwyddyn flaenorol.

Mae data'r NFIB ar gyfer blwyddyn ariannol 2015 - 2016 yn cadarnhau bod bron i 19,000 o ddioddefwyr trosedd seiber yn Llundain gyda chyfanswm eu colledion yn £402 miliwn. Roedd nifer sylweddol o'r troseddau hyn yn erbyn busnesau.

CAFODD 48% O FUSNESAU BACH PRYDAIN EU TARGEDU GAN DROSEDDWYR SEIBER YN Y 12 MIS DIWETHAF, 10% O'R RHAIN FWY NAG UNWAITH

Arolwg SME Barclaycard 2016

TWYLL SEIBER

RISGIAU I FUSNESAU

Beth sydd yn y fantol?

Mae eich arian, eich enw da, eich data, eich eiddo deallusol, eich cyfarpar technoleg gwybodaeth (TG) a gwasanaethau ar sail TG fel gwefannau a systemau talu – mae'r rhain oll mewn perygl yn sgil troseddwyr seiber.

Mae data yn gallu bod yn amrywiol iawn a gall gynnwys manylion am gleientiaid neu wybodaeth bersonol, gwybodaeth am daliadau, manylion am gynnyrch a gwybodaeth gyfrinachol am gwmnïau. Gall data fod yn y fantol hefyd pryd bynnag y caiff ei storio, boed hyn ar systemau TG a dyfeisiau cwmni neu yn y cwmwl.

Mae tanseilio TG yn gallu bod yn gostus o ran ei drwsio a hefyd o ran niwed i enw da. Gallai tanseilio fel hyn arwain at arian yn cael ei ddwyn neu ei drosglwyddo'n dwyllodrus o gyfrifon banc cwmni. Mae colli data yn gallu arwain at ddirwy fawr hefyd oddi wrth Swyddfa'r Comisiynydd Gwybodaeth.

Pwy allai beri bygythiad?

- Troseddwyr sy'n ceisio dwyn oddi wrthych – boed hyn yn ddata neu'n arian. Mae'n bosib hefyd eu bod eisiau amharu ar eich systemau fel na all eich busnes weithredu yn ôl ei arfer.
- Cystadleuwyr sydd eisiau cael gafael ar ddata cyfrinachol eich cwmni neu sydd eisiau tarfu ar eich gwaith.
- Eich staff eich hun. Gall eich gweithwyr cyflogedig fod â mynediad at lawer iawn o ddata a gwybodaeth gyfrinachol sy'n cael ei dal gan eich cwmni. Gall gweithwyr anfodlon ddwyn hyn gyda'r bwriad o'i drosglwyddo i gystadleuwyr neu i'r cynigydd uchaf. Fe all staff gael eu twyllo hefyd neu eu 'teilwra'n gymdeithasol' i roi gwybodaeth gyfrinachol i droseddwyr seiber.
- Hacwyr sy'n awyddus i ddangos eu sgiliau a phrofi i eraill eu bod yn gallu tanseilio eich diogelwch.

ATAL TROSEDD SEIBER

Trosedd seiber – adnabod eich busnes a sut i'w amddiffyn

Mae busnesau bach a chanolig yn wynebu anhawster arbennig wrth ddod o hyd i gydbwysedd rhwng eu gweithgareddau i atal trosedd seiber a'r adnoddau sydd ganddynt ar gael.

Rydym yn cydnabod na all busnesau bach a chanolig beryglu eu helw trwy weithredu systemau rheoli safonol sy'n ddiangen a chostus i ymdrin â throsedd seiber. Nid yw gwneud dim yn opsiwn. Yn hytrach, rydym yn awgrymu cymryd camau sylfaenol, pragmatig ac ymarferol.

Yn gyntaf, mae'n bwysig deall beth yw eich data gwerthfawr a sicrhau ei fod yn ddiogel.

Os daeth materion diogelwch newydd i'r amlwg, dylid gweithredu trefniadau a rheolaethau newydd neu well i leihau'r problemau hyn.

Dylech greu diwylliant o atal trosedd seiber o fewn eich busnes. Ewch ati i hyfforddi staff i sylwi ar achosion o drosedd seiber a'r hyn y dylen nhw ei wneud os byddant yn dod ar draws achosion. Ni ddylai hyfforddiant ar drosedd seiber fod yn weithgaredd unigol a dylai staff gael eu diweddaru'n rheolaidd yn y maes hwn. Dylai pob aelod o staff newydd fod yn ymwybodol o bolisïau a threfniadau atal trosedd seiber unrhyw gwmni.

Mae achos o drosedd seiber yn gallu arwain at gyfres o ddigwyddiadau sy'n gallu bod yn anhygoel o drafferthus, niweidiol a chostus i'ch busnes. Os bydd rhywbeth yn digwydd, mae'n bwysig hefyd bod â mesurau yn eu lle a fydd yn helpu eich busnes i ddod ato'i hun mor gyflym â phosib.

Os nad oes gennych staff TG o fewn eich busnes mae'n bosib y bydd arnoch angen cymorth allanol i adolygu a diweddaru eich systemau, polisïau a threfniadau. Mae yna nifer o adnoddau ar gael i gynorthwyo gyda hyn gan gynnwys cwmnïau a gwefannau diogelwch TG sy'n cynnig cyfoeth o wybodaeth ynghylch atal trosedd seiber. Mae rhai o'r rhain yn cael eu rhestru ar dudalennau 29 i 32 yn y llyfryn hwn.

Bod yn gymesur sy'n bwysig. Gwnewch yn siwr fod y systemau a'r prosesau rydych yn eu gweithredu yn briodol ar gyfer eich busnes chi a maint eich busnes.

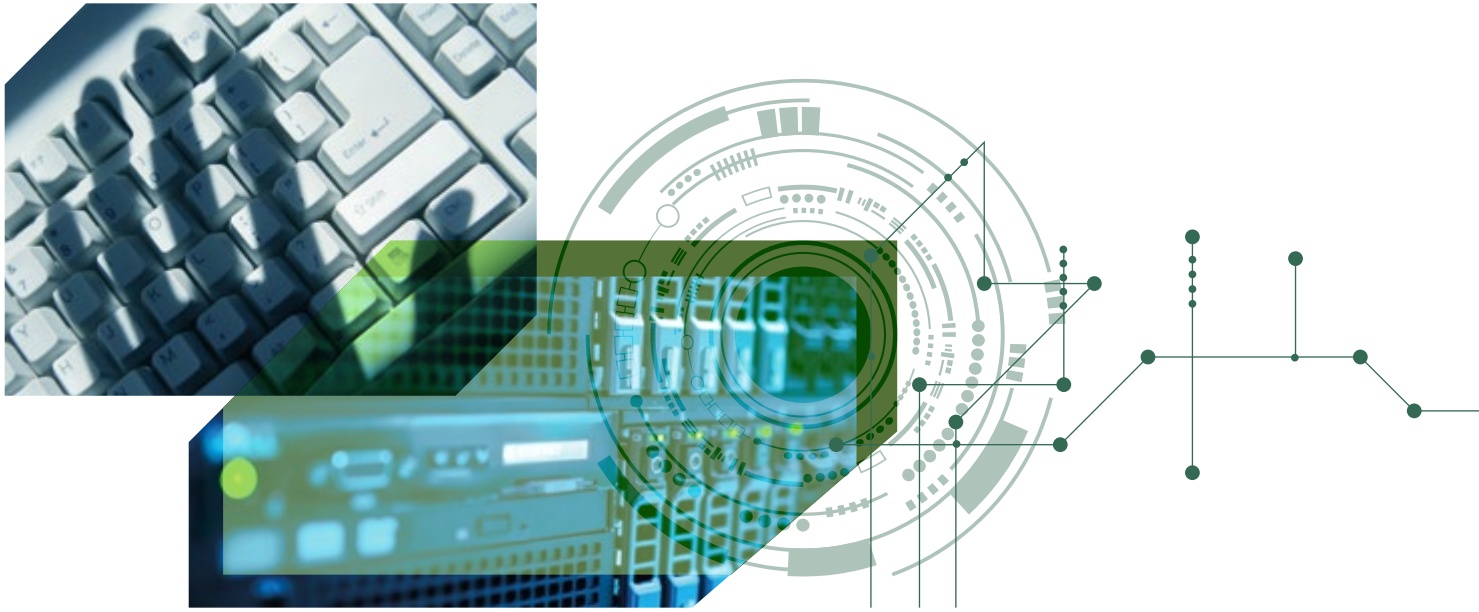
Mathau o drosedd seiber

Mae'n ddefnyddiol gwahaniaethu rhwng y ddau gategori o drosedd seiber:

Seiber-ddibynnol
Mae troseddau seiber-ddibynnol yn droseddau sy'n cael eu cyflawni yn erbyn cyfrifiaduron, rhwydweithiau cyfrifiadurol, dyfeisiau storio data neu ddyfeisiau eraill yn groes i'r Ddeddf Camddefnyddio Cyfrifiaduron. Mae'r troseddau hyn yn ymwneud â mynediad anghyfreithlon at system gyfrifiadurol neu fel na ellir defnyddio system.

Troseddau trwy gyfrwng seiber
Mae troseddau trwy gyfrwng seiber yn droseddau traddodiadol y gellir eu cynyddu o ran maint neu raddfa trwy ddefnyddio cyfrifiaduron, rhwydweithiau cyfrifiadurol neu ddyfeisiau eraill fel ffonau symudol a thabledi.

Gallai hyn ddigwydd wrth i fanylion cerdyn credyd ffug neu wedi'i ddwyn gael eu defnyddio i brynu eitem ar lein neu os bydd unigolyn yn anfon arian at droseddwr ar ôl derbyn e-bost twyllodrus.

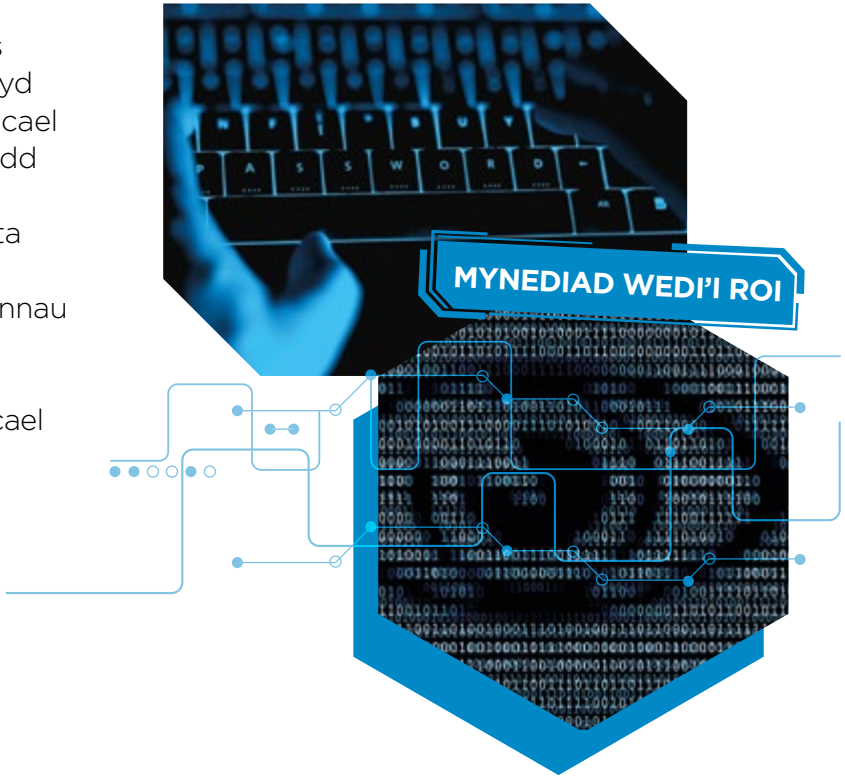


TWYLL SEIBER

TROSEDDAU SEIBER-DDIBYNNOL

Cyn dyfodiad y rhyngrwyd, roedd diogelwch cyfrifiaduron a rhwydweithiau yn gymharol syml gan mai'r cyfan oedd ei angen oedd diogelu eu systemau yn fewnol. Roedd cyfrifiaduron yn cael eu cysylltu ag eraill o fewn y cwmni ac yn gyffredinol nid oeddynt yn siarad â chyfrifiaduron eraill y tu hwnt i'w rhwydwaith eu hunain. Ers dyfodiad y rhyngrwyd mae'r her o ddiogelu cyfrifiaduron ar rwydwaith yn llawer anos.

Mae troseddau seiber-ddibynnol yn digwydd wrth i'r troseddwr gael mynediad heb awdurdod at system gyfrifiadurol neu weithredu fel na ellir defnyddio system. Os yw rhwydwaith wedi'i gysylltu â'r rhyngrwyd mae'n rhoi cyfle i droseddwr seiber geisio cael mynediad trwy ddilyn y llwybr hwn. Os bydd haciwr yn llwyddo i gael mynediad mae'n bosib y bydd yn gallu dwyn neu newid data ar rwydwaith, rheoli dyfeisiau sydd wedi'u cysylltu â rhwydwaith, fel CCTV neu beiriannau argraffu, neu weld beth mae defnyddiwr cyfrifiadur yn ei wneud trwy fonitro pob trawiad ar fysellfwrdd neu wylio beth sy'n cael ei ddangos ar y monitor neu'r we-gamera.



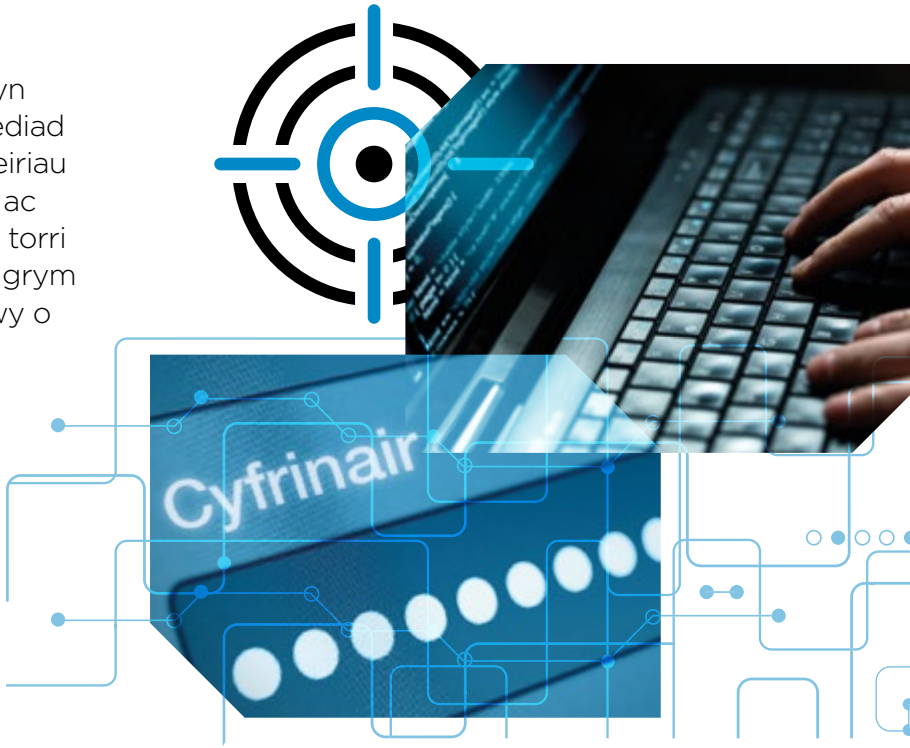
Hacio

Mae hacio yn digwydd pan fydd y sawl sy'n cael ei ddrwgdybio yn llwyddo i gael mynediad heb awdurdod i system gyfrifiadurol.

Mae yna nifer o ffyrdd o hacio systemau cyfrifiadurol.
Yn eu plith mae:

Ymosod ar gyfrineiriau
Bydd y sawl sy'n cael ei ddrwgdybio yn defnyddio rhaglenni cyfrifiadurol a fydd yn ceisio dyfalu cyfrinair er mwyn rhoi mynediad at system. Bydd y rhaglen yn creu cyfrineiriau ar sail termau wedi'u diffinio ymlaen llaw ac yna'n defnyddio'r cyfrineiriau hyn i geisio torri i mewn i'r system. Gyda digon o amser a grym cyfrifiadurol, mae'n bosib dyfalu'r rhan fwy o gyfrineiriau.

Ymosod ar raglenni
Mae hyn yn golygu targedu gwendidau yn rhaglenni'r system gyfrifiadurol.
Yn aml, bydd rhaglenni neu feddalwedd newydd yn cynnwys gwendidau y gellir eu camddefnyddio'n hawdd gan ganiatáu i ddiogelwch gael ei danseilio.



MYNEDIAD HEB AWDURDOD

TWYLL SEIBER

AMDDIFFYN RHAG HACIO

Defnyddio wal dân

Mae wal dân wedi'i chynllunio i amddiffyn un rhwydwaith cyfrifiadurol rhag un arall. Maen nhw'n cael eu defnyddio rhwng meysydd o ymddiriedaeth uchel ac isel, fel rhwydwaith preifat a'r rhyngrwyd. Mae waliau tân yn cynnig diogelwch trwy reoli traffig sy'n cyrraedd ac yn gadael rhwydwaith. Mae'r wal dân yn gwneud hyn trwy ddefnyddio set o hidlwyr neu reolau sy'n cael eu gosod gan y defnyddiwr i ganiatáu neu atal rhai mathau o draffig.

Mae wal dân yn gallu helpu i ddiogelu rhag hacwyr yn cael mynediad at eich systemau os cafodd ei sefydlu'n gywir.

Amgryptio data sensitif

Gwnewch yn siwr fod pob darn o ddata pwysig a sensitif wedi'i amgryptio felly, os caiff ei gyrchu neu ei ddwyn, ni fydd yn bosib ei ddarllen. Mae amgryptio yn gallu bod yn amrywiol iawn ac mae'n dibynnu ar ba fath o ddata sy'n cael ei amgryptio a sut mae'r data yn cael ei ddefnyddio, ei storio neu ei drosglwyddo.

Diweddaru meddalwedd

Mae'n bwysig sicrhau bod unrhyw feddalwedd ar eich cyfrifiaduron, systemau a dyfeisiau symudol yn cael ei ddiweddaru gan fod ei ddylunwyr yn mynd ati'n gyson i'w ddiweddaru i'w gadw'n ddiogel wrth i wendidau newydd gael eu darganfod.

Gwneir hyn drwy lawrlwytho diweddariadau neu gywiriadau gan ddatblygwr y meddalwedd pan ddaw cais. Yn aml iawn gellir gwneud hyn yn awtomatig, ond rhaid i chi ddewis yr opsiwn hwn o fewn offer y meddalwedd. Mae'n bwysig sicrhau hefyd fod y meddalwedd diweddaraf yn cael ei ddefnyddio oherwydd mae'n bosib y bydd hen feddalwedd yn hen ffasiwn ac nad oes modd ei ddiweddaru. Mae hyn yn golygu na fydd unrhyw wendidau newydd y bydd troseddwyr seiber yn eu darganfod yn cael eu datrys.

Bod â chyfrinair cryf

Yn aml, bydd diogelwch system TG yn cael ei danseilio oherwydd nad yw cyfrinair diofyn *(default)* ar feddalwedd neu galedwedd, fel llwybrydd *(router)*, yn cael ei newid. Mae'n bwysig bod pob cyfrinair diofyn yn cael ei newid cyn gynted â phosib.

Mae yna nifer o reolau cyffredinol ynghylch cyfrineiriau a fydd yn eu gwneud yn fwy diogel:

- Ceisiwch wneud cyfrinair mor hir â phosib, po fwyaf o nodau sydd ynddo, mwyaf anodd yw'r cyfrinair i'w ddyfalu.
- Defnyddiwch wahanol fathau o nodau gan gynnwys rhifau, symbolau ac atalnodau.
- Ceisiwch beidio â defnyddio geiriau o eiriadur yn eich cyfrinair oherwydd y bydd hyn yn eu gwneud yn haws eu dyfalu. Os ydych yn mynd i ddefnydd[illegible] sy'n hawdd eu cofio, beth am g[illegible] llythyren gyda symbol teby[illegible]newid 'a' gyda '@' neu 's' gyda '$'.
- Dylech ystyried defnyddio ymadrodd gyda thri gair ar hap fel 'cwchcwpanbuwch' neu eiriau o hoff gân fel 'henoynyranglesey'.
- Defnyddiwch wahanol gyfrineiriau ar gyfer cyfrifon gwahanol. Os bydd un cyfrinair yn cael ei ddyfalu, yna dim ond un cyfrif y gellir ei hacio.
- Ceisiwch osgoi defnyddio gwybodaeth bersonol fel pen-blwyddi, hoff dimau chwaraeon neu enwau plant/anifeiliaid anwes. Yn aml bydd troseddwyr seiber yn gallu darganfod y rhain gyda gwybodaeth rydych wedi'i rhoi ar lein, felly ddylech chi ddim eu defnyddio.

DDoS

Mae ymosodiad Atal Gwasanaeth Gwasgaredig (DDoS) yn ymgais i danseilio gwasanaeth ar y rhyngrwyd, fel gwefan, trwy ei orlwytho â thaffig data. Fel arfer bydd hyn yn cael ei gyflawni trwy anfon llif o geisiadau ar yr un pryd at weinydd gan achosi i'r gweinydd chwalu wrth geisio ymateb i fwy o geisiadau nag sy'n ymarferol ymdrin â nhw. Bydd y mathau hyn o ymosodiadau yn aml yn cael eu cynnal yn erbyn gwefannau gan ddefnyddio rhwydwaith o gyfrifiaduron wedi'u rheoli o bell o'r enw botrwyd *(botnet)*. Fel arfer bydd cyfrifiaduron sy'n rhan o'r botrwyd wedi'u heintio â meddalwedd maleisus, *(gweler tudalen 13)*, sy'n caniatáu i droseddwyr seiber eu rheoli a gallu cyfeirio traffig at weinydd y dioddefwr.

Ni fydd ymosodiadau DDoS ynddynt eu hunain yn achosi difrod i'ch systemau. Pan fydd yr ymosodiad yn dod i ben, fe ddylai eich gweinydd a'ch gwasanaethau ddod yn ôl i drefn. Serch hynny, fe all colli systemau, am ba hyd bynnag, arwain at golli gwerthiant neu wneud niwed i enw da.

Gellir defnyddio ymosodiadau DDoS hefyd fel llen fwg i guddio neu dynnu sylw oddi wrth weithgarwch anghyfreithlon arall y gallai ymosodwr fod yn ei gyflawni yn erbyn systemau cwmni, fel dwyn data o'r rhwydwaith.

Mae'r rhan fwyaf sy'n dioddef ymosodiadau DDoS yn sefydliadau amlwg fel cwmnïau rhyngwladol, asiantaethau'r llywodraeth, banciau a sefydliadau ariannol eraill.

Fodd bynnag, nid yw unrhyw sefydliad yn ddiogel ac mae'n bwysig bod yn ymwybodol y gall y math hwn o ymosodiad ddigwydd.

Bygythiadau DDoS

Mae bygythiadau DDoS yn digwydd wrth i droseddwr seiber gysylltu â busnes a bygwth ymosodiad DDoS os na fydd yn talu swm o arian. Fel arfer bydd y bygythiadau hyn yn dod trwy e-bost gan ofyn i'r arian gael ei dalu gan y cwmni trwy gyfrwng Bitcoin, sy'n anodd ei olrhain.

TROSEDDWR SEIBER

TWYLL SEIBER

AMDDIFFYN RHAG YMOSODIADAU DDOS

Adnabod arwyddion ymosodiad gweithredol

Wrth wybod bod ymosodiad DDoS yn digwydd, gallwch weithredu ar y cyfle cynharaf. Fe allai'r symptomau canlynol fod yn arwydd o ymosodiad DDoS ar eich rhwydwaith:

- Rhwydwaith yn perfformio'n anarferol o araf (agor ffeiliau neu gyrchu gwefannau)
- Gwefan benodol heb fod ar gael
- Methu cael mynediad at unrhyw wefan
- Cynnydd sylweddol yn nifer yr e-byst sbam rydych yn eu derbyn

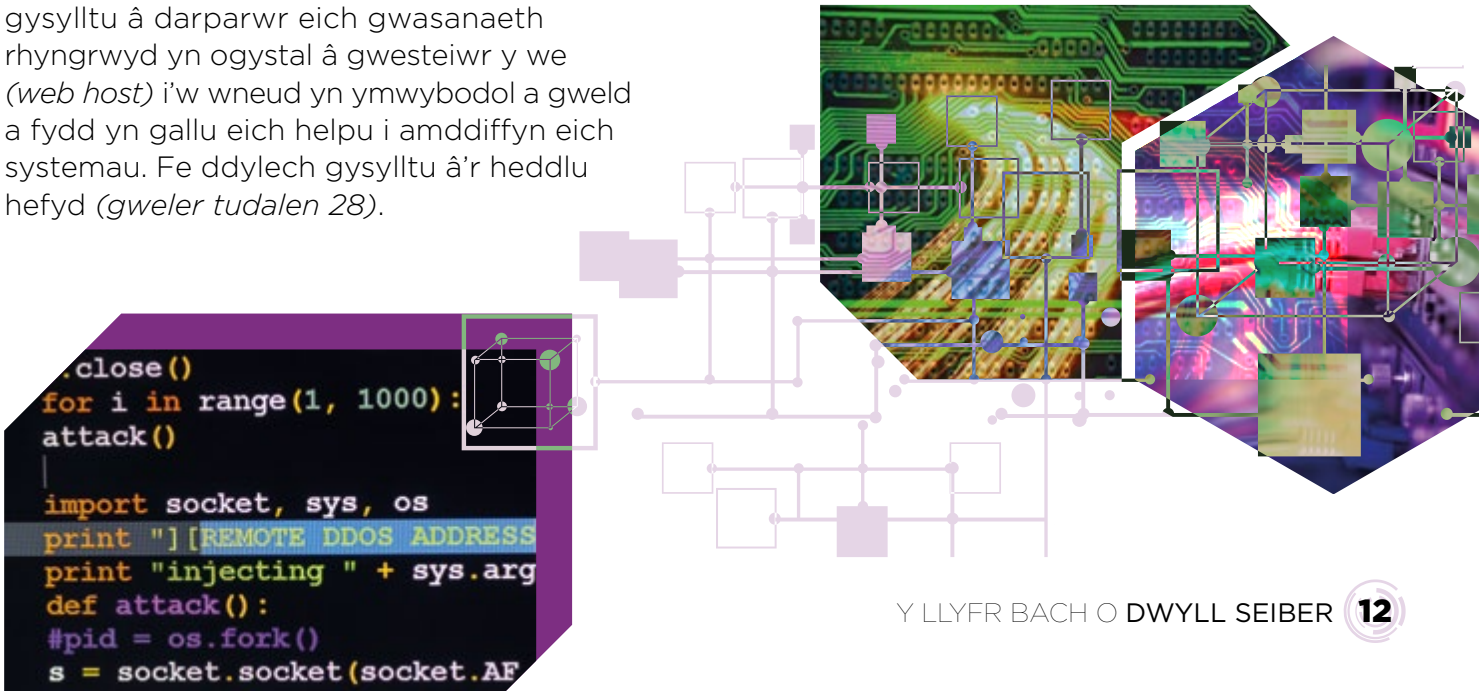
Os bydd ymosodiad yn digwydd fe ddylech gysylltu â darparwr eich gwasanaeth rhyngrwyd yn ogystal â gwesteiwr y we *(web host)* i'w wneud yn ymwybodol a gweld a fydd yn gallu eich helpu i amddiffyn eich systemau. Fe ddylech gysylltu â'r heddlu hefyd *(gweler tudalen 28)*.

Buddsoddi i leihau DDoS

Mae yna nifer o wahanol ffyrdd o leihau achosion o DDoS sydd ar gael gan amryw o gyflenwyr. Mae'r rhain yn gweithio trwy ddadansoddi'r traffig data ac adnabod traffig twyllodrus, gan ei rwystro rhag cyrraedd gweinydd y dioddefwr.

Bygythiadau DDoS

Os ydych yn wynebu bygythiadau DDoS peidiwch â thalu unrhyw arian. Cadwch unrhyw e-byst oddi wrth y troseddwr seiber a rhowch wybod i'r heddlu am y digwyddiad ar unwaith *(gweler tudalen 28)*.



TWYLL SEIBER

MALEISWEDD *(MALWARE)*

Mae'r term maleiswedd yn cyfeirio at feddalwedd maleisus. Mae hwn yn feddalwedd sy'n ceisio cael mynediad heb awdurdod at gyfrifiaduron neu ddyfeisiau eraill sydd wedi'u cysylltu, gan darfu ar eu gwaith arferol neu gasglu gwybodaeth oddi wrthynt.

Mae maleiswedd yn gallu heintio cyfrifiadur neu rwydwaith o nifer o ffynonellau gan gynnwys:

- Atodiadau e-bost sydd wedi'u heintio.
- Gwefannau wedi'u heintio, boed hynny drwy ymweld yn uniongyrchol neu drwy ddilyn dolenni ar e-byst neu negeseuon ar gyfryngau cymdeithasol.
- O ffeiliau llygredig wedi'u storio ar ddyfeisiau allanol fel gliniaduron, ffonau symudol neu gofion bach, sydd wedi'u cysylltu â'r rhwydwaith.

Mathau cyffredin o faleiswedd

Ysbïwedd *(Spyware)*

Mae ysbïwedd wedi'i gynllunio i ddwyn gwybodaeth am eich gweithgarwch ar gyfrifiadur neu ddyfais arall. Mae ysbïwedd yn gallu cyflawni nifer o swyddogaethau gan gynnwys recordio lluniau o'r sgrîn neu wneud cofnod o bob trawiad ar fysellfwrdd. Trwy wneud hyn bydd y troseddwr yn gallu cael gwybodaeth bersonol a gafodd ei rhoi ar gyfrifiadur a mynd ati i ddefnyddio'r wybodaeth honno, fel cyfrineiriau bancio ar y rhyngrwyd. Mae *Remote Access Trojans* (RATs) yn fath o ysbïwedd sy'n caniatáu i droseddwr seiber gysylltu o bell i heintio dyfeisiau a'u rheoli fel petaen nhw'n ddefnyddiwr ag awdurdod.

MAE MALEISWEDD YN GALLU HEINTIO CYFRIFIADUR NEU RWYDWAITH O NIFER O FFYNONELLAU

Meddalwedd wystlo *(Ransomware)*
Mae meddalwedd wystlo yn fath o faleiswedd sy'n golygu y gall troseddwyr seiber fynd ati o bell i gloi ffeiliau ar gyfrifiadur neu ddyfais arall sydd wedi'i chysylltu. Mae hyn yn golygu na fydd y gweithredwr yn gallu cael at y ffeiliau sydd wedi cloi ar y cyfrifiadur ac na all eu defnyddio. Unwaith y bydd y ffeiliau wedi'u cloi bydd y troseddwr yn cysylltu â'r dioddefwr ac yn cynnig eu datgloi am ffi, sef pridwerth. Fel arfer bydd y taliad dan sylw ar ffurf sy'n anodd ei olrhain, fel Bitcoin.

Feirws/Mwydyn *(Virus/worm)*
Mae feirysau a mwydod yn heintio systemau gwesteiwr ac yna'n lledaenu i heintio systemau eraill. Unwaith y byddant ar system, bydd feirysau a mwydod yn gosod copïau ohonynt eu hunain mewn rhaglenni, ffeiliau, a gyriannau. Mae mwydyn hefyd yn gallu lledaenu i gyfrifiaduron eraill gan ddefnyddio'r rhwydwaith y mae wedi'i gysylltu iddo. Mae mwydod a feirysau hefyd yn cario llwythi ychwanegol sy'n mynd ati i gyflawni gweithgarwch niweidiol ar eu gwesteiwyr.

Fe all y math hwn o faleiswedd achosi difrod sy'n lledaenu'n gyflym. Er enghraifft mae mwydod yn gallu gwneud i ymosodwyr greu rhwydwaith o beiriannau o'r enw botrwyd y gellir eu defnyddio mewn ymosodiad Atal Gwasanaeth Gwasgaredig (DDoS), *(gweler tudalen 11)*.

TWYLL SEIBER

EICH AMDDIFFYN EICH HUN RHAG MALEISWEDD

Defnyddio meddalwedd gwrth-feirws

Byddwch yn gosod y meddalwedd hwn ar bob cyfrifiadur, dyfais symudol a gweinydd. Bydd yn monitro ar gyfer maleiswedd o fewn cof, prosesau a gallu storio'r ddyfais a rhoi gwybod i'r defnyddiwr os daw o hyd i feirws. Mae'r rhan fwyaf o feddalwedd gwrth-feirws yn gallu tynnu meddalwedd maleisus y daeth ar ei draws a thrwsio'r difrod a achoswyd.

Mae'n bwysig diweddaru unrhyw feddalwedd gwrth-feirws gan fod ei ddylunwyr yn mynd ati'n gyson i'w wella wrth i raglenni maleiswedd newydd gael eu darganfod. Gwneir hyn drwy lawrlwytho diweddariadau neu gywiriadau gan ddylunwyr y meddalwedd. Mae'n bosib gwneud i'r rhan fwyaf o feddalwedd gwrth-feirws ddiweddaru'n awtomatig.

Defnyddio wal dân

Gweler tudalen 9 am ragor o wybodaeth am waliau tân.

Creu copi wrth gefn o'ch data yn rheolaidd

Gwnewch gopïau wrth gefn o waith a data pwysig a'u rhoi ar ddyfais ar wahân, fel gyriant caled symudol, a gwnewch yn siwr bod y copïau wedi llwyddo. Dylai'r copïau wrth gefn gael eu hamgryptio a'u cadw mewn lle diogel, fel sêff gwrthdan. Os yw eich cyfrifiadur wedi'i heintio gan faleiswedd, fel meddalwedd wystlo, gellir ei adfer gan ddefnyddio'r copi wrth gefn a dychwelyd unrhyw ddata sydd wedi'i gloi neu wedi'i golli.

Rheoli dyfeisiau

Dylech atal maleiswedd rhag heintio cyfrifiaduron trwy gyfyngu ar y dyfeisiau y gellir eu cysylltu iddynt, fel ffonau clyfar a gyriannau USB. Mae'r rhain yn gallu cario maleiswedd sy'n gallu trosglwyddo i gyfrifiadur y gwesteiwr pan fydd wedi cysylltu iddo. Cyn cysylltu unrhyw ddyfais, gwnewch yn siwr ei bod yn rhydd rhag maleiswedd.

Peidiwch â dilyn dolenni nac agor atodiadau mewn e-byst oni bai eu bod yn dod gan rywun rydych yn ymddiried ynddo

Wrth agor dolenni ac atodiadau mewn e-byst fe allech ganiatáu i feddalwedd maleisus gael ei lawrlwytho ar eich system neu ddyfais. Mae maleiswedd yn gallu cuddio mewn atodiadau e-byst, gan gynnwys ffeiliau .pdf neu ddogfennau Word, neu gael eu lawrlwytho o dudalen gwe faleisus wrth i chi gysylltu.

ASTUDIAETH ACHOS

MEDDALWEDD WYSTLO

Fe wnaeth cwmni teithio annibynnol bach wynebu achos o feddalwedd wystlo ar ôl i aelod o staff agor atodiad mewn e-bost. Roedd y meddalwedd maleisus wedi'i osod yn yr atodiad ac fe gafodd ei lansio pan gafodd yr e-bost ei agor. Fe wnaeth y maleiswedd amgryptio nifer o ffeiliau pwysig ar weinydd y cwmni gan olygu na allai weithredu'n effeithiol am nifer o ddiwrnodau, gan arwain at golli refeniw.

TWYLL SEIBER

TROSEDDAU TRWY GYFRWNG SEIBER
TEILWRA CYMDEITHASOL
(SOCIAL ENGINEERING)

Mae teilwra cymdeithasol yn cynnwys twyllwr yn mynd ati'n fedrus i gymryd mantais ar unigolyn i gynorthwyo ei weithgaredd troseddol. Gall fod yn haws twyllo gweithiwr cyflogedig i agor e-bost wedi'i heintio sy'n gosod maleiswedd ar system nag ydyw i hacio'r system ei hun yn uniongyrchol. Oherwydd hyn, mae teilwra cymdeithasol wedi tyfu'n fwy amlwg ac mae troseddwyr seiber yn dod o hyd i ffyrdd mwy beiddgar o gael pobl i gyflawni tasgau, darparu gwybodaeth neu roi arian gan ddefnyddio'r rhyngrwyd.

Mathau o deilwra cymdeithasol

Gwe-rwydo *(Phishing)*
Yn aml bydd troseddwyr seiber yn anfon e-byst gan honni eu bod yn rhywun arall at nifer o dderbynwyr ar yr un pryd. Gall yr e-bost honni ei fod yn dod oddi wrth fanc, safle ocsiwn ar lein neu adran y llywodraeth. Nod yr e-bost yw cael y derbynnydd i wneud rhywbeth na fydden nhw'n ei wneud fel arfer, neu ddatgelu gwybodaeth gyfrinachol i'r anfonwr.

Trwy wneud iddi ymddangos bod yr e-bost yn dod o ffynhonnell gyfreithlon, mae'r derbynnydd yn fwy tebygol o ateb neu weithredu'n unol â'r e-bost.

Mae meddalwedd ar gael sy'n gallu dangos neu 'dwyllo' cyfeiriad e-bost yn llinell anfonwr yr e-bost, felly mae'n ymddangos bod e-bost yn dod oddi wrth rywun arall.

Gall yr e-bost ddod o gyfeiriad e-bost sy'n debyg i'r un go iawn h.y. *@met.p0lice.uk* (mae'r 'o' wedi'i newid yn 'sero') yn hytrach na *@met.police.uk.*

Heb gymryd amser i weld a yw cyfeiriad y sawl sy'n anfon yn gywir, mae'n bosib y bydd y derbynnydd yn credu bod yr e-bost yn ddilys.

RHYBUDD

Bydd e-byst yn aml yn gofyn am fanylion mewngofnodi ar gyfer gwefannau bancio ar y rhyngrwyd. Gall hyn fod ar ffurf cwestiynau diogelwch i gadarnhau pwy yw'r derbynnydd. Unwaith y bydd yr atebion wedi'u rhoi, fe all y troseddwr seiber gywain yr holl fanylion a'u defnyddio i ddwyn o gyfrifon banc ar lein neu brynu pethau ar y we.

Mae'n bosib hefyd y bydd e-byst gwe-rwydo yn cynnwys maleiswedd mewn atodiadau a byddwch yn cael gorchymyn i'w hagor, *(gweler tudalen 13)*. Efallai y bydd yr e-bost yn gofyn i chi glicio ar ddolen sy'n mynd â chi i wefannau ffug neu faleisus sy'n gallu trosglwyddo maleiswedd i'ch dyfais neu gywain gwybodaeth y byddwch yn ei rhoi.

Spearphishing

Mae *spearphishing* yn ffurf fwy uniongyrchol ar we-rwydo. Eto, bydd y troseddwyr seiber yn anfon e-bost, ond y tro hwn bydd yn targedu unigolyn penodol a bydd yr 'anfonwr' yn rhywun sy'n gyfarwydd i'r derbynnydd. Gall fod yn gydweithiwr, gweithiwr hŷn neu rywun o adran TG y cwmni. Eto, bydd cyfeiriad e-bost yr anfonwr yn ymddangos fel petai oddi wrth anfonwr cyfarwydd.

Mae'n bosib hefyd y bydd yr e-bost yn cynnwys gwybodaeth arall i wneud iddo ymddangos yn fwy dilys. Gall hyn gynnwys manylion am ble mae'r anfonwr, er enghraifft mewn cynhadledd neu ar wyliau.

Mae'r wybodaeth hon i'w chael oddi ar safleoedd cyfryngau cymdeithasol. Gall hefyd ddangos gwybodaeth am y derbynnydd a ddaeth oddi ar y rhyngrwyd, fel prifysgolion a fynychwyd neu fwytai yr ymwelwyd â nhw.

GWALL DYNOL SY'N ACHOSI 95% O DRAMGWYDDAU MEWNOL

IBM 2015 Cyber Security Intelligence Index

Bydd e-byst *spearphishing* yn aml yn gofyn i'r derbynnydd gwblhau gweithred benodol, er enghraifft, darparu manylion cyfrif banc neu roi manylion mewngofnodi cyfrifiadur y gwaith. Gallant ofyn hefyd ar i ffeil sydd wedi'i hatodi gael ei hagor, neu glicio ar ddolen. Fe all agor atodiad neu glicio ar ddolen arwain at lawrlwytho maleiswedd ar eich cyfrifiadur.

Twyll gyda thaliadau

Mae twyll gyda thaliadau yn fath penodol o *spearphishing* sy'n targedu busnesau gyda'r bwriad o'u cael i drosglwyddo arian i gyfrif banc sy'n cael ei weithredu gan y troseddwr seiber.

Mae yna ddau brif fath o dwyll gyda thaliadau, twyll y Prif Weithredwr a thwyll mandad. Fel arfer mae'r ddau wedi'u targedu at staff o fewn adran gyfrifon y cwmni a defnyddio cyfeiriadau e-bost yr anfonwr ffug.

Mae twyll y Prif Weithredwr yn ymwneud ag e-bost sy'n honni ei fod yn dod oddi wrth uwch aelod o staff o fewn cwmni, fel Prif Weithredwr neu Gyfarwyddwr Cyllid. Bydd yr e-bost yn gofyn i'r derbynnydd wneud taliad neu drosglwyddo cyllid ar gyfer cyfle busnes neu fargen sy'n mynd ymlaen. Yn aml bydd y cais am daliad yn fater brys ac mae pwysau ar y derbynnydd i wneud taliad cyn gynted â phosib.

Mae twyll mandad fel arfer yn cynnwys e-bost sydd fel petai'n dod oddi wrth gyflenwr cyfarwydd. Bydd yr e-bost yn gofyn i daliadau am gynnyrch neu wasanaethau yn y dyfodol gael eu gwneud i gyfrif banc newydd, a rhoddir rheswm dros y newid. Bydd y cyfrif newydd yn cael ei weithredu gan y troseddwr seiber a bydd unrhyw arian a delir yn cael ei golli.

EICH AMDDIFFYN EICH HUN RHAG YMOSODIADAU TEILWRA CYMDEITHASOL

Y peth gorau i'w wneud gydag ymosodiadau teilwra cymdeithasol yw addysg a hyfforddiant ymwybyddiaeth i staff. Trwy wneud staff yn ymwybodol o'r mater fe fyddant mewn gwell sefyllfa i fynd i'r afael ag ef. Fe ddylai'r hyfforddiant hwn gynnwys y canlynol:

Sut i wirio cyfeiriad e-bost anfonwr mewn e-bost

Symudwch eich llygoden dros y cyfeiriad e-bost sy'n cael ei ddangos ym mocs yr anfonwr. Os yw'r cyfeiriad e-bost yn ffug fe ddylai hyn ddangos o ba gyfeiriad e-bost y daeth y neges mewn gwirionedd. Byddwch yn ymwybodol bod twyllwyr yn gallu tanseilio hyn felly efallai y bydd angen i chi edrych ar ddata pennawd yr e-bost i gadarnhau tarddiad y cyfeiriad e-bost. Mae'r ffordd rydych yn mynd ati i weld y data hwn yn wahanol gyda phob darparwr e-byst ac mae'n bosib y bydd angen i chi eu holi ynghylch sut i gyflawni hyn.

Gwnewch yn siwr hefyd mai'r cyfeiriad e-bost a ddangosir yw cyfeiriad e-bost cywir y sefydliad ac nad yw wedi'i sillafu'n anghywir, fel *@met.p0lice.uk* (mae'r 'o' wedi'i newid i 'sero') yn hytrach na *@met.police.uk*. Yn aml, bydd e-byst gwe-rwydo yn cael eu hanfon o gyfrif e-bost tebyg i gyfeiriad e-bost cwmni dilys, er enghraifft *police@gmail.com* neu *police@yahoo.com*, yn hytrach na chyfrif corfforaethol dilys, fel @met.police.uk.

Mae hwn yn ymddangos fel bod yr e-bost wedi dod oddi wrth anfonwr dilys gan fod yr enw corfforaethol yn ymddangos yng nghyfeiriad e-bost yr anfonwr.

Beth ddylech chi ei wneud os cewch gais i ddarparu manylion banc, gwybodaeth bersonol neu fanylion mewngofnodi

Os byddwch yn cael cais ar gyfer y math hwn o wybodaeth, yna fe ddylech ei ddilysu trwy gysylltu â'r sefydliad neu'r unigolyn sy'n gwneud y cais gan ddefnyddio manylion cyswllt cadarn. Peidiwch â chysylltu trwy ateb e-bost o'r un a gawsoch a pheidiwch ag ateb gan ddefnyddio unrhyw rai o'r manylion cyswllt, fel rhifau ffôn, sydd i'w gweld yn yr e-bost. Os nad oes gennych fanylion cyswllt yn barod, cysylltwch â'r sefydliad gan ddefnyddio manylion a gawsoch wrth chwilio ar y rhyngrwyd.

Sut i ddilysu ceisiadau am newid i wybodaeth am gyfrif neu fanylion bancio cleient a cheisiadau am daliadau unigol

Os bydd e-bost yn cyrraedd yn gofyn am newid cyfrif banc ar gyfer taliad, manylion gwybodaeth gyswllt ar gyfrif neu daliad unigol, dylech ddilysu hyn drwy gysylltu'n uniongyrchol â'r sefydliad neu'r sawl sy'n gofyn am y newid gan ddefnyddio manylion cyswllt cadarn.

MEDDALWEDD MALEISUS

TWYLL SEIBER

ASTUDIAETH ACHOS

Fe wnaeth Cyfarwyddwr Cyllid cwmni adnoddau dynol bach dderbyn e-bost gan gredu ei fod yn dod oddi wrth Brif Weithredwr y cwmni gan fod eu cyfeiriad e-bost yn ymddangos ym mocs anfonwr yr e-bost. Roedd yr e-bost yn dweud wrth y Cyfarwyddwr Cyllid am wneud taliad i gyfrif banc oedd yn ymddangos yn yr e-bost. Gan gredu bod y cais yn ddilys, fe wnaeth y Cyfarwyddwr Cyllid drosglwyddo £30,000 i'r cyfrif.

Cysylltodd banc y cwmni â'r Cyfarwyddwr Cyllid mewn perthynas â hyn, i gadarnhau ei fod yn ddilys. Fe wnaeth y Cyfarwyddwr Cyllid gadarnhau wrth y banc fod popeth yn iawn. Sylweddolwyd wedyn fod y cais yn dwyllodrus ac nad oedd yn bosib cael yr arian yn ôl.

Fe wnaeth yr heddlu gadarnhau bod cyfeiriadau e-bost busnes y Prif Weithredwr a'r Cyfarwyddwr Cyllid yn ymddangos ar wefan y cwmni a bod hynny o gymorth mawr i'r troseddwr seiber wrth greu'r e-bost *spearphishing*. Darganfuwyd hefyd, wrth symud y llygoden dros y cyfeiriad e-bost ar yr e-bost a anfonwyd gan y troseddwr ei bod yn bosib gweld cyfeiriad e-bost go iawn yr anfonwr.

TWYLL SEIBER

COLLI DATA

Fe all y wybodaeth rydych yn ei rhoi ar lein fod yn werthfawr iawn i droseddwr seiber. Mae miliynau o bobl yn defnyddio safleoedd cyfryngau cymdeithasol bob dydd ac mae gan lawer o bobl broffiliau ar lein gyda llawer iawn o wybodaeth amdanyn nhw, eu gwaith, addysg a diddordebau personol.

Yn yr un ffordd y gall troseddwr weld ar neges cyfryngau cymdeithasol eich bod ar wyliau ac yna'n torri i mewn i'ch tŷ, gall troseddwr seiber ddefnyddio cyfeiriad e-bost eich gwaith neu rywbeth rydych wedi'i roi ar lein, fel digwyddiad y bydd yn ei fynychu, i gynorthwyo mewn ymosodiad seiber yn eich erbyn.

Mae'n hawdd iawn i droseddwr seiber greu e-bost *spearphishing* gyda gwybodaeth sydd i'w chael yn hawdd trwy chwilio'r rhyngrwyd.

Er enghraifft, fe allai trydariad syml am ymweliad â bwyty gael ei ddefnyddio i greu e-bost *spearphishing* sy'n ymddangos fel petai'n dod oddi wrth y bwyty. Gall yr e-bost hwn gynnig cyfle i chi gymryd rhan mewn cystadleuaeth neu hawlio gostyngiad ar eich ymweliad nesaf trwy gwblhau ffurflen sydd wedi'i hatodi gyda'r e-bost. Gallai'r ffurflen gynnwys meddalwedd maleisus ac wrth ei agor fe all y maleiswedd heintio eich cyfrifiadur.

SPEARPHISHING

TWYLL SEIBER

EICH AMDDIFFYN EICH HUN RHAG COLLI DATA

Byddwch yn ofalus gyda'r hyn rydych yn ei roi ar lein

A oes raid i'r wybodaeth fod yn gyhoeddus? Dylech fod yn arbennig o ofalus wrth roi cyfeiriadau e-bost busnesau yn uniongyrchol ar lein. Fe all troseddwyr seiber eu defnyddio i greu e-byst *spearphishing*. Ateb syml yn aml yw cyfeiriad e-bost contact@ neu info@.

Dylech wybod pa wybodaeth sydd i'w chael amdanoch ar lein

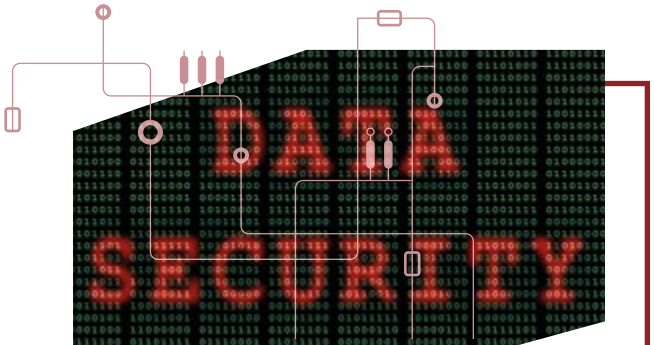
Chwiliwch y rhyngrwyd yn sydyn i weld pa ddata sydd ar gael amdanoch chi. Efallai y bydd gwybodaeth sydd wedi'i gosod gan bobl eraill nad ydych yn ymwybodol ohoni, neu wybodaeth nad oeddech yn gwybod oedd ar gael yn gyhoeddus. Os ydych yn gyfarwyddwr cwmni, mae pentwr o wybodaeth ar gael amdanoch chi a'ch busnes trwy wefan Tŷ'r Cwmnïau a gwefannau eraill tebyg. Os yw eich busnes wedi'i gofrestru yn eich cyfeiriad gartref, bydd y cyfeiriad hwn i'w weld ar lein.

Dylech wahanu gwybodaeth fusnes oddi wrth wybodaeth bersonol

Peidiwch â chynnwys manylion cyswllt personol ar wefannau busnes ac fel arall. Cadwch eich gwaith a'ch bywyd personol ar wahân.

Dylech gael gosodiadau preifatrwydd ar safleoedd cyfryngau cymdeithasol

Peidiwch â gadael i bawb weld popeth. Gwnewch yn siwr fod gwybodaeth a manylion personol sydd ond ar gael i ffrindiau a chydweithwyr yn cael eu cadw'n breifat. I wneud hyn, dylech gael gosodiadau preifatrwydd ar safleoedd cyfryngau cymdeithasol sy'n cyfyngu ar bwy sy'n cael gweld eich gwybodaeth. Hefyd, byddwch yn wyliadwrus o bobl sydd eisiau eich dilyn neu fod yn ffrind i chi. Ydych chi'n gwybod pwy ydyn nhw mewn gwirionedd? Meddyliwch pa ddiddordeb sy ganddyn nhw ynoch chi ac a yw'n addas iddyn nhw weld gwybodaeth bersonol amdanoch.



TWYLL SEIBER

LLECYNNAU Wi-Fi

Mae cysylltiadau neu lecynnau Wi-Fi yn gallu bod yn ddefnyddiol er mwyn mynd ar y rhyngrwyd pan nad ydych gartref neu yn eich gweithle. Nid yw pob cysylltiad Wi-Fi yn ddiogel fodd bynnag, ac mae yna ffyrdd y gall troseddwyr seiber eu defnyddio i godi eich data.

Sniffian

Mae sniffian yn dechneg lle bydd y troseddwr seiber yn dal eich data wrth i chi ei anfon dros y rhwydwaith Wi-Fi. Trwy wneud hyn maen nhw'n gallu dwyn cyfrineiriau, manylion mewngofnodi a gwybodaeth sensitif ac yna un ei ei ddefnyddio i gyflawni troseddau yn eich erbyn neu ei werthu i rywun arall. Hyd yn oed os na fyddwch yn teipio manylion mewngofnodi ar eich dyfais bob tro y byddwch yn agor ap ar ffôn, fel e-bost neu gyfryngau cymdeithasol, bydd manylion mewngofnodi yn cael eu hanfon ar draws y rhwydwaith a gellir eu rhyng-gipio.

Mannau Mynediad Drwg *(Evil Access Points)*

Mae troseddwyr seiber yn gallu sefydlu eu llecynnau cyhoeddus eu hunain mewn ymgais i'ch cael chi i gysylltu â nhw. Yn gyntaf byddant yn cysylltu eu cyfrifiadur â'r rhyngrwyd. Yna byddant yn darlledu eu signal fel cysylltiad Wi-Fi gan fynd ati'n aml i'w alw'n rhywbeth fel 'free_wifi' neu 'coffee_shop_wifi'.

Unwaith y byddwch yn cysylltu â'r llecyn Wi-Fi rydych yn cysylltu â chyfrifiadur y troseddwr mewn gwironedd ac maen nhw'n gallu dal unrhyw ddata rydych yn ei anfon.

Diogelwch eich Hun

- Defnyddiwch Rwydwaith Preifat Rhithwir (VPN) wrth gael mynediad at gysylltiadau Wi-Fi cyhoeddus. Trwy ddefnyddio VPN bydd eich holl ddata yn cael ei amgryptio wrth iddo gael ei drosglwyddo dros y rhwydwaith, felly os caiff ei ryng-gipio gan unrhyw un, fyddan nhw ddim yn gallu ei ddarllen. Gallwch lawrlwytho VPN ar ffonau a chyfrifiaduron ar ffurf ap.
- Peidiwch â gwneud unrhyw beth ar Wi-Fi cyhoeddus na fyddech am i bobl eraill ei weld, fel bancio ar lein, cyrchu e-byst eich cwmni neu unrhyw beth sy'n gofyn i chi roi enw defnyddiwr neu gyfrinair.
- Os nad ydych yn siwr a yw cysylltiad llecyn Wi-Fi yn ddiogel, peidiwch â'i ddefnyddio, ond yn hytrach defnyddiwch eich cysylltiad data 3G neu 4G i gael mynediad at y rhyngrwyd. Mae data sy'n mynd dros 3G a 4G wedi'i amgryptio.

RHWYDWAITH PREIFAT RHITHWIR

TWYLL SEIBER Y DYFODOL

Mae'r rhyngrwyd wedi agor byd o gyfleoedd i fusnesau a defnyddwyr. Y mae wedi cyflymu trafodion, symleiddio prosesau a chreu rhyngwyneb mwy cyfleus rhwng busnesau a chwsmeriaid. Mae llawer o fusnesau bach bellach yn gallu cael eu rhedeg gan ddefnyddio dim ond gliniadur ar fwrdd y gegin. Bydd technoleg yn parhau i wella, ond beth fydd effaith hyn ar ddiogelwch?

Y rhyngrwyd pethau – IOT

Gyda chynnydd yn nifer y dyfeisiau wedi'u cysylltu â'r rhyngrwyd, fel ceir, setiau teledu ac oergelloedd, buan y daeth troseddwyr seiber i wybod sut i fanteisio arnynt a chyflawni trosedd seiber. Gwelwyd eisoes bod grwpiau o droseddwyr seiber wedi defnyddio lled band y rhyngrwyd wedi'i gysylltu â dyfeisiau IOT i gyflawni ymosodiadau DDoS ar raddfa fawr. Cafwyd adroddiadau hefyd fod meddalwedd cerbydau wedi'i hacio gydag ymosodwyr yn cymryd drosodd y pethau hanfodol fel arafu a llywio.

Cynnydd mewn bygythiadau seiber

Rydym yn disgwyl gweld mwy o feddalwedd wystlo a dioddefwyr yn gorfod talu pridwerthoedd uwch, yn enwedig pan fydd busnes mawr yn cael ei fygwth. Yn ogystal â defnyddio maleiswedd mwy cymhleth i amgrypio ffeiliau rydym hefyd yn disgwyl gweld cynnydd yn nifer y grwpiau bygythiadau seiber a dulliau ymosod. Mae troseddwyr seiber eisoes yn galw am bridwerthoedd i atal ymosodiadau DDoS, neu maent yn cysylltu â busnesau a gofyn am arian ar ôl dwyn data hanfodol o rwydweithiau'r cwmni.

Deddfwriaeth

Fe ddaeth Rheoliad Diogelu Data Cyffredinol (GDPR) Ewropeaidd i rym ar 25 Mai 2018 ac mae'n gweithredu cyfres o reolau y mae'n rhaid i unrhyw un sy'n prosesu data personol cwsmeriaid gadw atynt. Bydd cwsmeriaid yn cael mwy o lais o ran yr hyn y gallwch ei wneud gyda'u data a sut gellir ei ddefnyddio a bydd riportio mynediad diawdurdod at ddata yn orfodol. Bydd hefyd yn rhoi mwy o rym i reoleiddwyr osod dirwyon sylweddol os yw eich busnes yn gyfrifol am golli data, hyd at 5% o drosiant byd-eang neu €20m. Os bydd y Deyrnas Unedig yn gadael yr Undeb Ewropeaidd, mae'n debygol y bydd busnesau sy'n dal data dinasyddion yr Undeb Ewropeaidd yn gorfod cydymffurfio o hyd â'r gyfarwyddeb hon os ydynt yn dymuno cynnal busnes yn Ewrop.

TWYLL SEIBER

SUT I RIPORTIO

Mae riportio trosedd, gan gynnwys trosedd seiber, yn bwysig. Os na fyddwch yn rhoi gwybod i'r awdurdodau, sut byddan nhw'n gwybod ei fod wedi digwydd a sut gallant wneud unrhyw beth amdano? Cofiwch os ydych yn ddioddefwr, ni waeth pa mor ddibwys, mae'n bosib y bydd busnesau eraill mewn sefyllfa debyg. Gall eich gwybodaeth ffurfio rhan o un jig-so mawr a gall fod yn hanfodol ar gyfer cwblhau'r darlun a dal y troseddwyr.

Ble i riportio

Dylech riportio pob twyll a honiadau o drosedd seiber i Action Fraud un ai ar lein yn www.actionfraud.police.uk

Neu dros y ffôn ar 0300 123 2040

Oni bai:

- Fod trosedd wrthi'n digwydd neu ar fin cael ei chyflawni.
- Bod rhywun a ddrwgdybir yn hysbys yn lleol neu os yw'n hawdd adnabod y sawl a ddrwgdybir.
- Mae'r drosedd yn cynnwys dioddefwr agored i niwed.

Os felly, cysylltwch â'r heddlu yn uniongyrchol ar 999, neu 101 os nad yw'n argyfwng. Gallwch hefyd riportio yng ngorsaf leol yr heddlu.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Helpwch i darfu ar dwyllwyr trwy riportio e-byst twyll y byddwch yn eu derbyn

Mae gwefan Action Fraud yn gadael i chi riportio e-byst gwe-rwydo a gawsoch neu faleiswedd sydd wedi effeithio ar eich cyfrifiaduron, systemau neu ddyfeisiau. Bydd y rhain yn cael eu hanfon ymlaen at y National Fraud Intelligence Bureau sy'n cael ei redeg gan Heddlu Dinas Llundain i'w dosbarthu a'u dadansoddi. Mae hyn yn golygu y gellir casglu cudd-ymchwil hollbwysig a chymryd camau ataliol. Bydd hyn yn ceisio tarfu ar y twyllwyr a chau'r cysylltiadau rhyngddyn nhw a dioddefwyr.

TWYLL SEIBER

CYNGOR PELLACH

Isod mae rhestr o wefannau a allai fod yn ddefnyddiol:

www.actionfraud.police.uk

Action Fraud yw canolfan riportio genedlaethol y Deyrnas Unedig ar gyfer twyll a throsedd seiber. Os ydych wedi cael profiad o drosedd seiber fe ddylech riportio hynny'n uniongyrchol i Action Fraud dros y ffôn neu drwy eu gwefan, *(gweler tudalen 28 am fanylion cyswllt)*. Ar wefan Action Fraud hefyd mae'r wybodaeth ddiweddaraf am sawl math o dwyll a throsedd seiber a manylion am sut i'ch amddiffyn eich hun ar lein.

www.cyberaware.gov.uk

Mae Cyber Aware (Cyber Streetwise yn flaenorol) yn rhoi cyngor am ddiogelwch seiber i fusnesau bach ac unigolion, fel defnyddio cyfrineiriau cryf sy'n cynnwys 'tri gair ar hap' a mynd ati bob amser i lawrlwytho'r meddalwedd a'r ap diweddaraf, i'ch helpu i amddiffyn eich dyfeisiau rhag troseddwyr seiber. Mae'r canllawiau yn seiliedig ar gyngor arbenigol gan y National Cyber Security Centre, rhan o GCHQ.

I gael gwybod mwy, ewch i www.cyberaware.gov.uk

www.financialfraudaction.org.uk

Mae Financial Fraud Action UK Ltd (FFA UK) yn gyfrifol am arwain y frwydr gyffredinol yn erbyn twyll yn niwydiant taliadau'r Deyrnas Unedig. Gan weithio gyda'i aelodau – sy'n cynnwys y prif fanciau, cwmnïau cardiau credyd, debyd a thalu, a derbynwyr taliadau trwy gerdyn – mae FFA UK yn ceisio arwain brwydr y diwydiant yn erbyn twyll ariannol i leihau ei effaith ar unigolion a chwmnïau, ac ar y diwydiant yn gyffredinol. Ar wefan FFA UK mae cyfoeth o wybodaeth ynghylch sut i'ch amddiffyn eich hun a'ch busnes rhag twyll a throsedd seiber.

Mae FFA UK wedi lansio *Take Five to Stop Fraud* sy'n annog pobl i oedi ac ystyried a yw'r sefyllfa yn ddilys – stopio a meddwl a yw'r hyn sy'n cael ei ddweud yn gwneud synnwyr mewn gwirionedd.

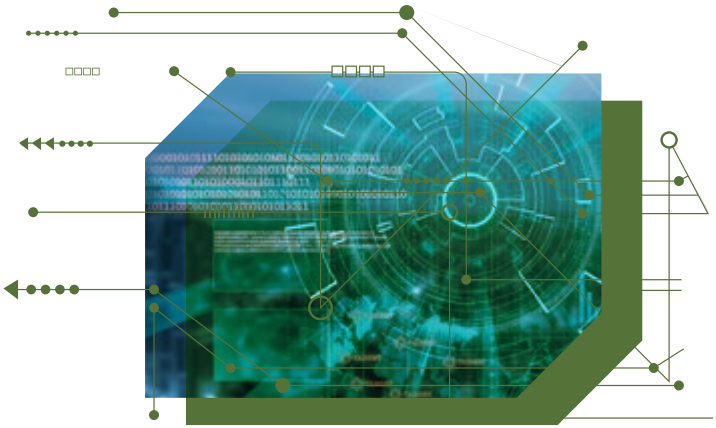
PUM CAM I ATAL TWYLL™

www.takefive-stopfraud.org.uk

DIOGELWCH EICH HUN

www.fsb.org.uk
Mae'r Ffederasiwn Busnesau Bach yn cynnig nifer o wasanaethau busnes hanfodol i'w aelodau gan gynnwys cyngor, arbenigedd ariannol, cefnogaeth a llais cryf wrth lobïo'r llywodraeth. Eu cenhadaeth yw cynorthwyo busnesau llai i gyflawni eu huchelgais.

www.getsafeonline.org
Get Safe Online yw'r ffynhonnell fwyaf poblogaidd ym Mhrydain o wybodaeth hawdd ei deall ynghylch diogelwch ar lein. Mae eu gwefan yn adnawdd unigryw sy'n darparu cyngor ymarferol am sut i'ch diogelu eich hun, eich busnes a'ch teulu rhag mathau cyffredin o drosedd seiber. Ar y wefan mae canllawiau ar lawer o bynciau cysylltiedig hefyd – gan gynnwys creu copïau wrth gefn a diogelu data.



www.gov.uk/government/policies/cyber-security
Mae'r wefan hon yn adnawdd ar lein sy'n manylu polisïau'r llywodraeth mewn perthynas â diogelwch seiber. Mae'n cynnwys nifer o adroddiadau a phapurau polisi gyda manylion am ymdrechion y llywodraeth i fynd i'r afael â throsedd seiber ynghyd â chopïau o ddatganiadau i'r wasg a chanllawiau ar ddiogelwch seiber i fusnesau.

www.londondsc.co.uk
Mae'r London Digital Security Centre (LDSC) yn ceisio helpu i ddiogelu ac amddiffyn busnesau micro a chanolig Llundain rhag peryglon a bygythiadau seiber. Sefydlwyd yr LDSC i gefnogi Busnesau Bach a Chanolig Llundain a'u cynorthwyo i fynd ati'n ddiogel i fanteisio ar gyfleoedd yn y byd digidol. Yn ogystal â chynghori sut i barhau'n ddiogel ar lein maent yn cynnig gwasanaethau noddedig i fusnesau, fel sganio am wendidau.

www.met.police.uk/fraud
Mae tudalennau rhybuddion twyll gwefan Heddlu Llundain yn rhoi gwybodaeth i gynorthwyo i fynd i'r afael â thwyll a throseddau economaidd eraill.

www.ico.org.uk
Swyddogaeth Swyddfa'r Comisiynydd Gwybodaeth yw cynnal hawliau gwybodaeth er budd y cyhoedd. Ar eu gwefan mae gwybodaeth ynghylch sut i gydymffurfio â deddfwriaeth berthnasol ynghylch rheoli data personol gan gynnwys diogelu gwybodaeth bersonol a darparu mynediad at wybodaeth swyddogol.

www.nationalcrimeagency.gov.uk
Yr Asiantaeth Troseddu Cenedlaethol (NCA) sy'n arwain brwydr heddlu'r Deyrnas Unedig i dorri troseddau difrifol a threfnedig. Mae eu gwefan yn cynnwys gwybodaeth am fygythiadau troseddol ar hyn o bryd a chanllawiau i fusnesau ar ddiogelwch ar lein.

www.ncsc.gov.uk
Mae'r Ganolfan Diogelwch Seiber Genedlaethol (NCSC) yn rhan o GCHQ a dyma brif awdurdod y Deyrnas Unedig ar ddiogelwch seiber.

Prif bwrpas yr NCSC yw lleihau risg diogelwch seiber i'r Deyrnas Unedig trwy wella ei diogelwch seiber a dycnwch seiber.

Bydd yn gweithio gyda sefydliadau, busnesau, ac unigolion yn y Deyrnas Unedig i roi cyngor awdurdodol a chyson am ddiogelwch seiber a rheoli digwyddiadau seiber, wedi'i ategu gydag ymchwil ac arloesedd gyda'r gorau yn y byd.

Mae NCSC hefyd yn ymateb i ddigwyddiadau er mwyn lleihau'r niwed i'r Deyrnas Unedig, cynorthwyo i adfer a dysgu gwersi ar gyfer y dyfodol.

I gael gwybod mwy, ewch i: www.ncsc.gov.uk

www.nomoreransom.org
Mae gwefan "No More Ransom" yn fenter gan Uned Genedlaethol Troseddau Technoleg Uwch heddlu'r Iseldiroedd, Canolfan Trosedd Seiber Ewrop Europol a chwmnïau diogelwch seiber preifat sy'n ceisio cynorthwyo dioddefwyr meddalwedd wystlo i adennill eu data sydd wedi'i amgryptio heb orfod talu i'r troseddwyr. Oherwydd ei bod yn llawer haws osgoi'r bygythiad nag ymladd yn ei erbyn unwaith y bydd y system wedi'i llygru, mae'r prosiect hefyd yn anelu at addysgu defnyddwyr ynghylch sut mae meddalwedd wystlo yn gweithio a pha wrthfesurau y gellir eu cymryd yn effeithiol i osgoi heintio.

CEFNOGAETH YCHWANEGOL

CiSP

Mae Partneriaeth Rhannu Gwybodaeth Seiber-ddiogelwch (CiSP) yn cael ei gweithredu gan yr NCSC ac mae'n caniatáu i aelodau ar draws gwahanol sectorau a sefydliadau gyfnewid gwybodaeth am fygythiadau seiber wrth i droseddu ddigwydd, mewn amgylchedd diogel a dynamig, gan weithredu o fewn fframwaith sy'n diogelu cyfrinachedd gwybodaeth sy'n cael ei rhannu.

Mae'r platfform yn cynnwys nifer o fforymau agored a chaeëdig sy'n caniatáu i ddefnyddwyr o feysydd busnes penodol neu gyda diddordebau neilltuol rannu gwybodaeth gyda defnyddwyr eraill o'r un natur.

I gael gwybod mwy ac ymuno â CiSP gweler:
www.ncsc.gov.uk/cisp

National Cyber Security Centre
a part of GCHQ

CiSP
Cyber-security Information Sharing Partnership

Cyber Essentials

Mae cynllun Cyber Essentials yn achredu busnesau mawr a bach i hysbysebu'r ffaith eu bod wedi bodloni safon diogelwch seiber a gymeradwyir gan y llywodraeth. Trwy ganolbwyntio ar lanweithdra seiber sylfaenol, bydd cwmnïau wedi'u diogelu'n well rhag y bygythiadau seiber mwyaf cyffredin.

Mae Cyber Essentials ar gyfer pob sefydliad, o bob maint, ac ym mhob sector. Nid yw hyn wedi'i gyfyngu i gwmnïau yn y sector preifat, eithr mae'n gymwys hefyd i brifysgolion, elusennau, a sefydliadau yn y sector cyhoeddus.

Mae Cyber Essentials yn orfodol ar gyfer contractau llywodraeth ganolog a hysbysebir ar ôl 1 Hydref 2014 sy'n cynnwys ymdrin â gwybodaeth bersonol a darparu rhai cynhyrchion a gwasanaethau TGCh.

Fe gafodd cynllun Cyber Essentials ei ddatblygu mewn ymgynghoriad agos â diwydiant fel rhan o Raglen Diogelwch Seiber Genedlaethol y Deyrnas Unedig.

I gael gwybod mwy ewch i:
www.cyberaware.gov.uk/cyberessentials/

CYBER ESSENTIALS

TWYLL SEIBER GEIRFA

Botrwyd *(botnet)*

Casgliad o gyfrifiaduron wedi'u heintio y gellir eu rheoli o bell gan droseddwr seiber.

Ymosodiad nerthol *(brute force attack)*

Defnyddio rhaglenni cyfrifiadurol i geisio adnabod y cyfrinair i ganiatáu mynediad heb awdurdod i system.

Cwcis

Ffeiliau sy'n cael eu dal ar eich cyfrifiadur sy'n cynnwys gwybodaeth am eich defnydd ar wefannau.

Colli data

Colli data yn ddamweiniol, nid rhywun yn dwyn data.

Dwyn data

Dwyn data yn fwriadol.

Colli data *(data leakage)*

Pan fydd gwybodaeth am unigolyn neu fusnes yn cael ei chyhoeddi ar lein. Gall y wybodaeth hon gael ei defnyddio i lunio e-byst *spearphishing*.

Ymosodiad Atal Gwasanaeth Gwasgaredig (DDoS)

Ymosodiad sy'n cael ei lansio ar system gan rwydwaith o gyfrifiaduron, o'r enw Botrwyd, sy'n tarfu ar gyfrifiadur neu wefan.

Dosbarthu maleiswedd trwy e-bost

Maleiswedd sy'n cael ei gyflwyno trwy atodiad mewn e-bost.

Ecsbloetio *(exploits)*

Mae'r rhain wedi'u cynllunio i gymryd mantais ar ddiffyg neu wendid mewn system gyfrifiadurol, yn nodweddiadol am resymau maleisus, fel gosod maleiswedd.

Hacktivism

Mae hyn yn hacio sy'n digwydd er dibenion gwleidyddol neu gymdeithasol.

MEDDALWEDD MALEISUS

Cipio gwybodaeth *(keylogging)*

Mae hyn yn cynnwys logio pob trawiad ar fysellfwrdd cyfrifiadur neu ddyfais dan fygythiad.

Maleiswedd *(malware)*

Mae hwn yn feddalwedd maleisus sy'n cynnwys ysbïwedd, ceffyl Troea, feirysau a mwydod.

Cywiriadau *(patches)*

Mae'r rhain yn trwsio gwendidau sydd i'w cael mewn meddalwedd, systemau gweithredu neu gymhwysiadau.

E-byst gwe-rwydo

Proses yw hon o dwyllo derbynwyr i ddadlennu gwybodaeth sensitif trwy anfon e-byst twyllodrus.

Meddalwedd wystlo *(ransomware)*

Mae hwn yn fath o faleiswedd sy'n gwrthod mynediad at eich ffeiliau neu gyfrifiadur hyd nes byddwch wedi talu pridwerth.

Teilwra cymdeithasol *(social engineering)*

Mae hyn yn cyfeirio at ddylanwadu ar ddioddefwyr i ddadlennu gwybodaeth neu gwblhau tasg na fydden nhw'n ei gwneud fel arfer.

Spearphishing

Gwe-rwydo wedi'i dargedu yw hwn sydd yn aml yn defnyddio cyfeiriadau e-bost twyllodrus ac sy'n cynnwys gwybodaeth a geir wrth 'golli data' *(data leakage)* er mwyn gwneud i'r cynnwys ymddangos yn ddilys.

Twyllo *(spoofing)*

Mae twyllo trwy e-bost yn digwydd wrth i gyfeiriad e-bost yr anfonwr gael ei ffugio er mwyn cynorthwyo gyda theilwra cymdeithasol. Bydd meddalwedd sydd ar gael ar lein yn cael ei ddefnyddio i guddio gwir anfonwr e-bost.

Ysbïwedd *(spyware)*

Meddalwedd maleisus yw hwn sy'n caniatáu i droseddwyr seiber gael gafael ar wybodaeth breifat heb yn wybod i ddefnyddiwr. Gall gofnodi trawiadau ar fysellfwrdd neu pa wefannau yr ymwelwyd â nhw a throsglwyddo'r wybodaeth hon i'r troseddwr seiber.

Ceffyl Troea *(Trojan)*

Mae ceffylau Troea yn rhaglenni maleisus sy'n ymddangos eu bod yn rhywbeth gwahanol i'r hyn ydynt mewn gwirionedd. Gallai hyn fod yn rhywbeth a lawrlwythir sy'n datgan ei fod yn chwaraewr fideo ag yntau mewn gwirionedd yn faleiswedd.

Feirws

Mae feirysau yn ddarnau o feddalwedd maleisus sy'n ymsefydlu mewn ffeil ac sy'n gallu lledaenu o un cyfrifiadur i un arall. Maent yn arbennig o niweidiol a gellir eu defnyddio i ddwyn data neu reoli cyfrifiadur – gweler Botrwyd.

Gwendidau *(vulnerabilities)*

Mae'r rhain yn ddiffygion o fewn rhaglenni y gellir eu hecsbloetio gan droseddwyr seiber i ymosod ar gyfrifiaduron, systemau a dyfeisiau symudol.

Mwydyn *(worm)*

Mae mwydyn yn fath o feirws sy'n ecsbloetio gwendid penodol o fewn system gan ddefnyddio hyn i ledu i systemau eraill.

Sombi

Sombi yw cyfrifiadur sy'n gallu cael ei reoli o bell gan droseddwr seiber. Fe fydd wedi'i heintio â maleiswedd a gall gael ei ddefnyddio fel rhan o Botrwyd.


MEDDALWEDD WYSTLO MALEISWEDD
cyfrinair
Inbox (6)
Starred

Cafodd y llyfryn hwn ei ysgrifennu a'i gynhyrchu gan dîm Diogelwch Seiber FALCON Heddlu Llundain.

I gysylltu â'r Tîm Diogelwch e-bostiwch cyberprotect@met.police.co.uk

FALCON
FRAUD AND LINKED CRIME ONLINE