Cadw'n Ddiogel Ar-lein

Mae technoleg yn rhan ganolog o'n bywydau a thra rydym yn gwybod y gall roi'r arfau a'r cyfleoedd i bobl sy'n cam-drin i reoli, olrhain a cham-drin, fe all hefyd fod yn ffynhonnell bwysig o gefnogaeth a gwybodaeth ar ddiogelwch i ddioddefwyr camdriniaeth.

Yn y gorffennol, roedd cynllunio diogelwch o amgylch technoleg yn canolbwyntio ar ddioddefwyr camdriniaeth gan leihau eu defnydd o dechnoleg a dileu eu cyfrifon cyfryngau cymdeithasol a chael gwared ar eu ffonau clyfar. Mae hyn nid yn unig yn afrealistig ond mae'n cosbi dioddefwr y gamdriniaeth ac yn eu torri oddi wrth eu rhwydweithiau cymdeithasol a chefnogol, gan eu gadael yn ynysig. Yn hytrach, rydym ni'n argymell siarad gyda'ch cleient ynglŷn â defnyddio technoleg yn ddiogel a chymryd rhai camau syml i fynd i'r afael â diamddiffynedd. Dyma ein hawgrymiadau gwych:

Meddyliwch am eich ôl troed digidol cyfan

Edrychwch ar yr holl feysydd lle rydych yn defnyddio technoleg yn eich bywyd ac ystyriwch a oes yna unrhyw feysydd lle'r hoffech wella eich dealltwriaeth, diweddaru pa mor ddiogel rydych neu gyfyngu ar ba mor amlwg ydych chi.

Byddwch yn ddoeth o ran eich cyfrinair

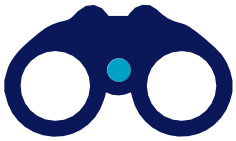
Mae cyfrineiriau cryf yn hanfodol i ddiogelu eich cyfrifon. Newidiwch enw defnyddwyr a chyfrineiriau hyd yn oed os nad ydych yn credu fod y cyfrifon wedi eu peryglu. Fe allwch ddefnyddio rheolwr cyfrineiriau i'ch helpu gyda hyn. Fe allwch hefyd ystyried defnyddio gwiriad dau gam er mwyn bod yn fwy diogel.

Gwiriwch y gosodiadau diogelwch

Diweddarwch osodiadau diogelwch ar gyfrifon cyfryngau cymdeithasol fel mai dim ond y bobl yr ydych eisiau cysylltu â nhw all weld eich negeseuon, lluniau a gwybodaeth.

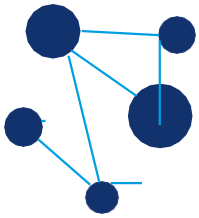
Byddwch yn ymwybodol o osodiadau lleoliad

Mae llawer o apiau a meddalwedd yn cofnodi gwybodaeth ynglŷn â'ch lleoliad daearyddol, a gall y wybodaeth hon gael ei chamddefnyddio gan rywun gyda mynediad i'ch cyfrifon/dyfeisiau. Gwiriwch pa apiau sy'n defnyddio gosodiadau lleoliad ac yna diffoddwch unrhyw rai nad ydych eu hangen.



Ystyriwch sut y gallech gael eich olrhain

Mae yna sawl ffordd y gall technoleg alluogi unigolyn i ddilyn eich symudiadau. Y dull mwyaf cyffredin yw drwy apiau yr ydych wedi eu gosod eich hun, y gall unigolyn arall wedyn gael gwybodaeth ohonynt. Er mwyn lleihau'r risg o ran hyn, ystyriwch ddiffodd apiau olrhain pan nad ydych yn eu defnyddio e.e. 'darganfod fy ffrindiau/ffôn/llechen', tracwyr ffitrwydd GPS, llywio lloeren.



Torrwch y cysylltiadau

Ystyriwch unrhyw gyfrifon wedi eu cysylltu neu ar y cyd a allai fod wedi eu gosod ar fwy nag un ddyfais ac a allai roi mynediad i rywun i'ch gwybodaeth neu ddyfeisiau. Gallai hyn gynnwys cyfrifon ar gyfer iTunes, y storfa apiau, storfa Google Play, eBay, Amazon, Kindle ac eraill.

Meddyliwch am dechnoleg yn y cartref tu hwnt i ffonau, llechi a chyfrifiaduron

Mae yna ddyfeisiau cartref clyfar e.e. Amazon Echo (Alexa), Google Home, thermostat clyfar, system larwm cartref neu reolyddion eraill y gellir cael mynediad iddynt o bell ac a allai gael eu defnyddio i fonitro neu i effeithio arnoch. Newidiwch y cyfrineiriau ar y rhain, i sicrhau mai dim ond pobl y gallwch ymddiried ynddynt all gael mynediad iddynt.

Diogelwch rwydwaith WiFi eich cartref

Fe all unigolyn gael mynediad i'ch dyfeisiau drwy'r rhwydwaith WiFi, a fydd yn hygyrch heb fod angen bod y tu mewn i'ch cartref. Newidiwch y manylion mewngofnodi a'r cyfrinair fel na ellir cael mynediad i'ch rhwydwaith heb yn wybod i chi.

Byddwch yn ymwybodol o gamerâu

Gellir cael mynediad i gamerâu a dyfeisiau o bell neu gellir eu gweithredu gan apiau. Gorchuddiwch y gwe-gamera ar eich cyfrifiadur/llechen pan nad yw'n cael ei ddefnyddio.