Enw: _____ Dyddiad: _____ Sgôr: _____

Diogelwch ac Amgryptio Wi-Fi Cyhoeddus

Ymosodiadau dyn-yn-y-canol, pwyntiau mynediad twyllodrus, sniffian pecynnau, twneli VPN, ac amgryptio HTTPS.

TROSOLWG DYSGU DIOGELWCH WI-FI CYHOEDDUS

WEDI'I DDIOGELU

AMGRYPTIO DATA

Safon AES 256-did

YN CYDYMFFURFIO

SAFONAU BYD-EANG

Fframweithiau GDPR a CCPA

DIM YMDDIRIEDAETH

POLISI MYNEDIAD

Dilysu Aml-ffactor

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy ddiogelwch Wi-Fi cyhoeddus. Byddwch yn archwilio rhwydweithiau heb eu hamgryptio, ymosodiadau dyn-yn-y-canol (MitM), pwyntiau mynediad twyllodrus, sniffian pecynnau, twneli VPN, a diogelwch data wrth deithio gyda HTTPS.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli seiberddiogelwch ac atal bygythiadau.**
- [ ] **Rhan 5-7: Datrys posau croesair a chwilair.**
- [ ] **Rhan 8-9: Datrys astudiaethau achos a her y seiffr.**
- [ ] **Rhan 10: Adolygu tudalennau Cwestiynau Cyffredin sylfaenol ac uwch.**
- [ ] **Rhan 11: Archwilio 10 ffaith ddiddorol o'r byd go iawn.**
- [ ] **Bonws: her Meddwl yn Gyflym.**

Agorwch Ganllaw Seiberddiogelwch VPN.com

URL: https://www.vpn.com/cy/diogelwch-seiber/diogelwch-wifi-cyhoeddus/

Eich Map Llwybr Dysgu Diogelwch Wi-Fi Cyhoeddus

- Nodwch risgiau cyffredin Wi-Fi cyhoeddus, gan gynnwys sniffian pecynnau a phwyntiau mynediad twyllodrus.
- Rhowch dwneli amgryptio VPN ar waith i ddiogelu data wrth iddo deithio.
- Gorfodwch HTTPS a gosodiadau porwr gwe diogel ar gyfer gweithwyr o bell.

CYFARWYDDIADAU'R CANLLAW DIOGELWCH WI-FI CYHOEDDUS

Atebwch y cwestiynau amlddewis a gwir/gau, cwblhewch y brawddegau llenwi bylchau gan ddefnyddio'r banc geiriau, parwch y diffiniadau, a datryswch y posau croesair a chwilair. Cymhwyswch eich gwybodaeth i ddiogelwch mynediad o bell. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

DIOGELWCH WI-FI CYHOEDDUS AC AMDDIFFYN DATA WRTH DRAWSYRRU (CYFLWYNIAD)

Mae mannau problemus Wi-Fi cyhoeddus heb eu hamgryptio yn gadael traffig rhwydwaith yn agored i sniffian pecynnau a ffugio Evil Twin. Mae gorfodi traffig drwy dwneli amgryptio VPN diogel a gorfodi rheolau HSTS HTTPS-yn-unig yn amddiffyn sesiynau rhag rhyng-gipio ar y rhwydwaith lleol.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR YMATEB CYWIR.

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw ymosodiad Dyn-yn-y-Canol (MitM)?**
   - A. Rhyng-gipio a newid cyfathrebiadau rhwng dau barti ar rwydwaith a rennir
   - B. Techneg echdynnu cronfa ddata sy'n targedu cofnodion defnyddwyr
   - C. Llethu gweinyddion gwe â cheisiadau traffig rhwydwaith
   - D. Sychu cyfrolau storio'r gyriant caled lleol

2. **2. Beth yw pwynt mynediad twyllodrus (Gefell Drwg)?**
   - A. Man problemus Wi-Fi maleisus wedi'i ffurfweddu gyda'r un SSID â rhwydwaith dilys
   - B. Offeryn gweinyddol a ddefnyddir i fonitro copïau wrth gefn o gronfeydd data
   - C. Ffurfweddiad porth VPN diogel
   - D. Cofnod DNS sy'n mapio gweinyddion post awdurdodedig

3. **3. Sut mae VPN yn diogelu traffig Wi-Fi cyhoeddus?**
   - A. Mae'n lapio pob pecyn rhwydwaith mewn twnnel wedi'i amgryptio, gan eu gwneud yn annarllenadwy i sniffwyr
   - B. Mae'n rhwystro pob cais cysylltu sy'n dod i mewn yn awtomatig
   - C. Mae'n newid cyfeiriad MAC y cerdyn rhwydwaith ffisegol
   - D. Mae'n dileu cwcis sydd wedi'u storio yn y porwr gwe

4. **4. Beth yw sniffian pecynnau?**
   - A. Defnyddio offer caledwedd neu feddalwedd i gipio a chofnodi pecynnau rhwydwaith
   - B. Sganio cyfeiriaduron lleol am ffeiliau dyblyg
   - C. Cyfyngu breintiau darllen cronfa ddata yn ôl rolau defnyddwyr
   - D. Amgryptio gyriannau storio gan ddefnyddio allweddi AES-256

5. **5. Beth yw rôl HTTPS?**
   - A. Amgryptio traffig y sesiwn rhwng y porwr a'r gweinydd gwe
   - B. Hidlo negeseuon e-bost sy'n dod i mewn wrth y porth
   - C. Cywasgu delweddau i lwytho tudalennau'n gyflymach
   - D. Rheoli strwythurau ffeiliau mewn storfa sydd ynghlwm wrth y rhwydwaith

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Gall defnyddwyr cysylltiedig ddal data testun plaen yn hawdd ar rwydweithiau Wi-Fi cyhoeddus agored.

Gwir Gau

7 Cwestiwn 7

7. Mae pwyntiau mynediad twyllodrus (Evil Twins) bob amser wedi'u hawdurdodi gan weinyddwyr rhwydwaith.

Gwir Gau

8 Cwestiwn 8

8. Mae VPN yn aneffeithiol wrth ddiogelu traffig rhag sniffio pecynnau ar rwydweithiau cyhoeddus.

Gwir Gau

9 Cwestiwn 9

9. Dim ond llwybr yr URL y mae HTTPS yn ei amgryptio, gan adael llwyth tâl y pecyn mewn testun plaen.

Gwir Gau

10 Cwestiwn 10

10. Mae mannau problemus Wi-Fi sy'n defnyddio diogelwch WPA3 yn cynnig amddiffyniad cryfach na rhwydweithiau agored heb gyfrinair.

Gwir Gau

Pwynt Gwirio 3: Mewnosod Termau Allweddol

Darllenwch bob brawddeg isod a llenwch y bwlch gyda'r term cywir o'r Banc Geiriau.

1. Yr enw ar gipio cyfrineiriau preifat ar Wi-Fi cyhoeddus yw _____ cyfathrebu.
2. Mae dadansoddi pecynnau crai ar rwydwaith lleol yn defnyddio _____ pecynnau.
3. Enw man Wi-Fi twyllodrus sy'n dynwared Wi-Fi gwesty yw _____ .
4. Mae diogelu traffig gwe wrth deithio yn gofyn am amgryptio gyda _____ .
5. Mae amgryptio pob allbwn rhwydwaith yn defnyddio _____ .
6. Llwybr cyfathrebu wedi'i amgryptio drwy rwydweithiau cyhoeddus yw _____ .

BANC GEIRIAU GEIRFA

CLEIENT VPN | GEFAILL DRWG | HTTPS | RHYNGIPIO | SAFON WPA | SNIFFIO | TWNNEL | WAL DÂN

Ysgrifennwch eich atebion yma:

1.
2.
3.
4.
5.
6.

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

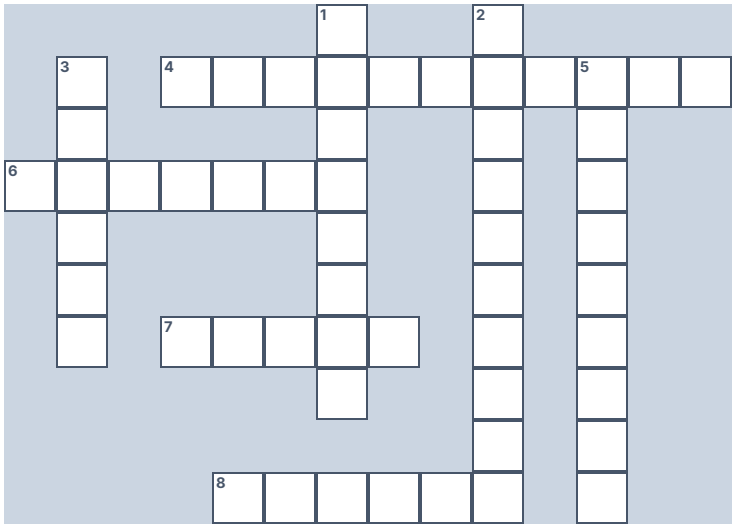
PARU DIFFINIADAU

Parwch bob term geirfa ar y chwith â'i ddiffiniad cywir ar y dde drwy ysgrifennu'r llythyren gyfatebol (A-H) yn y blwch mewnbwn y gellir ei lenwi.

☐	1. RHYNG-GIPIO	A	Safon diogelwch Wi-Fi fodern.
☐	2. CLUSTFEINIO	B	Llwybr data diogel wrth drosglwyddo.
☐	3. GEFELL DRWG	C	Hidlo traffig sy'n dod i mewn.
☐	4. HTTPS	D	Man problemus twyllodrus sy'n dynwared Wi-Fi.
☐	5. VPN	E	Darllen traffig wrth iddo gael ei drosglwyddo.
☐	6. TWNNEL	F	Dal pecynnau data rhwydwaith.
☐	7. WPA3	G	Rhwydwaith preifat rhithwir wedi'i amgryptio.
☐	8. WAL DÂN	H	Trosglwyddo diogel ar y we.

Pwynt Gwirio 5: Pos Croesair

Datryswch y croesair drwy deipio llythrennau yn y blychau gwyn gweithredol. Mae'r rhifau'n cyfateb i'r cliwiau isod.



CLIWIAU AR DRAWS

4. Man Wi-Fi twyllodrus sy'n dynwared rhwydwaith Wi-Fi. (11)

6. Cipio pecynnau data rhwydwaith. (7)

7. Trosglwyddo gwe diogel. (5)

8. Hidlo traffig sy'n dod i mewn. (6)

CLIWIAU I LAWR

1. Diogelwch Wi-Fi modern (WPA3). (8)

2. Rhwydwaith preifat rhithwir wedi'i amgryptio. (10)

3. Llwybr data diogel wrth deithio. (6)

5. Darllen traffig wrth iddo deithio. (9)

Pwynt Gwirio 5, dewis arall: Cliwiau Croesair Hygyrch

Gall defnyddwyr darllenwyr sgrin a bysellfwrdd deipio atebion y croesair yn uniongyrchol yn y meysydd testun isod.

CLIWIAU AR DRAWS

4 ar draws: Man Wi-Fi twyllodrus sy'n dynwared rhwydwaith Wi-Fi. (11 llythyren):

6 ar draws: Cipio pecynnau data rhwydwaith. (7 llythyren):

7 ar draws: Trosglwyddo gwe diogel. (5 llythyren):

8 ar draws: Hidlo traffig sy'n dod i mewn. (6 llythyren):

CLIWIAU I LAWR

1 i lawr: Diogelwch Wi-Fi modern (WPA3). (8 llythyren):

2 i lawr: Rhwydwaith preifat rhithwir wedi'i amgryptio. (10 llythyren):

3 i lawr: Llwybr data diogel wrth deithio. (6 llythyren):

5 i lawr: Darllen traffig wrth iddo deithio. (9 llythyren):

Pwynt Gwirio 6: Chwilair Geiriau Cudd

Dewch o hyd i'r 8 term geirfa allweddol sydd wedi'u cuddio yn y grid isod. Gall geiriau fod yn llorweddol, yn fertigol neu'n groeslinol.

K X M Y P X F T O P L C R I G

N R S M P X Q W I O W C U S T

N E P L J B A N F B A C P X L

P K T Y K X T N F K L D Q M J

V D T I N G N E I K D Q P R G

T M H M Q E R L N S A T T H G

N C S Q O F H S S B N W D Y S

E Z V C Z A W F A K H Z D N N

I D Q X P I C U F B A Z N G D

E K A D O L D F O H I D R I Q

L M E I R L Z S N F Q V F P A

C A Q O N D P T W X Q K R I U

S D N Y B R F S P X W J A O R

Z Y Y L G W I M A R J M L T O

H Q Q H Z G A O V G U B Y R Y

RHESTR GEIRIAU GEIRFA

RHYNGIPIO, SNIFFIO, GEFAILLDRWG, HTTPS, CLEIENTVPN, TWNNEL, SAFONWPA, WALDAN

Pwynt Gwirio 6, dewis arall: Paru Geirfa Hygyrch

Parwch bob un o'r 8 term geirfa o'r Chwilair â'i ddiffiniad cywir drwy ysgrifennu'r llythyren (A-H) yn y bwlch.

TERMAU GEIRFA

A. RHYNGIPIO

B. SNIFFIO

C. GEFAILLDRWG

D. HTTPS

E. CLEIENTVPN

F. TWNNEL

G. SAFONWPA

H. WALDAN

DIFFINIADAU A MEYSYDD PARU

1. Diogelwch Wi-Fi modern (WPA3).
2. Man Wi-Fi twyllodrus sy'n dynwared rhwydwaith Wi-Fi.
3. Cipio pecynnau data rhwydwaith.
4. Llwybr data diogel wrth deithio.
5. Hidlo traffig sy'n dod i mewn.
6. Darllen traffig wrth iddo deithio.
7. Rhwydwaith preifat rhithwir wedi'i amgryptio.
8. Trosglwyddo gwe diogel.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol seiberddiogelwch. Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. **IGNHRPIOY**
2. **IGEGWLFRDLA**
3. **CNPTLENIVE**
4. **OPAWNSAF**
5. **FOFISIN**
6. **PHTST**
7. **ETNLNW**
8. **LNWADA**

Gweithgaredd Bonws: Meddwl yn Gyflym

3 ATEB YM MHOB CATEGORI. Y PERSON CYNTAF I GWBLHAU'R RHESTR SY'N ENNILL.

1	Rhesymau dros ddiweddaru meddalwedd			
2	Dyfeisiau sy'n cysylltu â Wi-Fi yn awtomatig			
3	Gwybodaeth na ddylech byth ei rhannu			
4	Arferion diogel y gallwch eu dechrau heddiw			
5	Ffyrdd o gadw'n ddiogel mewn caffi			
6	Dyfeisiau y gellir eu hacio			
7	Pethau y gall haciwr eu gweld ar Wi-Fi agored			
8	Arwyddion o rwydwaith Wi-Fi ffug			
9	Dewisiadau eraill yn lle Wi-Fi cyhoeddus			
10	Arwyddion rhybudd mewn e-bost			
11	Pethau nad ydych chi'n eu gwneud ar Wi-Fi cyhoeddus			
12	Mannau â Wi-Fi am ddim			
13	Ffyrdd o ddiogelu eich cyfrifon			
14	Arwyddion bod cyfrifiadur wedi'i heintio			
15	Enwau Wi-Fi sy'n ymddangos yn amheus			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

Cymhwyswch y cysyniadau rydych wedi'u dysgu i ddatrys y senarios go iawn isod.

ASTUDIAETH ACHOS 1: CYFYNGU AR SNIFFIAN PECYNNAU AR WI-FI CYHOEDDUS



Senario: Mae swyddog gwerthu o bell sydd wedi'i gysylltu â rhwydwaith Wi-Fi cyhoeddus mewn maes awyr yn sylwi bod sawl e-bost busnes sensitif wedi gollwng yn fuan ar ôl eu hanfon fel testun plaen.

Cwestiwn Trafod: Dadansoddwch risgiau rhwydweithiau cyhoeddus, ac amlinellwch ateb i amgryptio traffig.

ASTUDIAETH ACHOS 2: AMDDIFFYN RHAG MANNAU PROBLEMUS TWYLLODRUS EVIL TWIN



Senario: Mae ymosodwyr yn gosod pwynt mynediad diwifr twyllodrus o'r enw 'CoffeeShop_Guest' sy'n dynwared man cyswllt caffi dilys, gan gipio traffig rhwydwaith gan westeion diarwybod.

Cwestiwn Trafod: Disgrifiwch yn fanwl y camau gwirio i ganfod a rhwystro pwyntiau mynediad twyllodrus.

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae gweithiwr proffesiynol seiberddiogelwch yn diogelu asedau rhwydwaith rhag actorion bygythiad ar-lein. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges drwy ysgrifennu'r llythrennau cyfatebol yn y bylchau gwag.

ALLWEDD AMGRYPTIO LLYTHRENNAU-I-RIFAU

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

1	13	7	18	25	16	20	9	23	3	8		20	18	1	6	6	9	7

23	9	6	9		3	25	8	15	5	4	4	21	19		7	25	4	1

22	16	14

Neges wedi'i datgodio:

AWGRYM: MAE POB RHIF YN CYNRYCHIOLI SAFLE'R LLYTHYREN HONNO YN YR WYDDOR (E.E. 1 = A, 2 = B, 26 = Z).

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan A)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q1: Pam mae Wi-Fi cyhoeddus yn anniogel?

Nid yw Wi-Fi cyhoeddus agored yn amgryptio traffig dros yr awyr, felly gall eraill gerllaw ddal unrhyw ddata heb ei ddiogelu. [2]

Q2: Beth yw sniffian pecynnau?

Mae sniffiwr pecynnau yn cipio data crai sy'n llifo dros ryngwyneb rhwydwaith, gan ddatgelu cyfrineiriau testun plaen a manylion traffig.

Q3: Beth yw Evil Twin?

Pwynt mynediad twyllodrus a sefydlwyd gan hacwyr sy'n dynwared enw a gosodiadau man problemus Wi-Fi lleol dibynadwy.

Q4: Sut mae VPN yn fy niogelu?

Mae'n llwybro eich traffig drwy dwnnel wedi'i amgryptio, gan guddio eich gweithgarwch pori rhag sniffwyr ar y rhwydwaith lleol.

Q5: A yw HTTPS yn fy niogelu ar Wi-Fi cyhoeddus?

Ie, mae'n amgryptio'r data a gyfnewidir rhwng eich porwr a'r wefan, ac mae VPN yn ychwanegu haen arall o ddiogelwch.

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan B)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q6: Beth yw WPA3?

Y safon Wi-Fi Protected Access fodern, sy'n cynnig amgryptio cryfach ac amddiffyniad rhag ymosodiadau geiriadur all-lein. [1]

Q7: A all Wi-Fi cyhoeddus ddarparu maleiswedd?

Gallant, gall ymosodwyr ryng-gipio traffig a chwistrellu ysgogiadau lawrlwytho maleisus (lawrlwythiadau wrth basio) i'ch sesiwn porwr.

Q8: Beth yw risg rhannu ffeiliau?

Os yw rhannu ffeiliau wedi'i alluogi, gall defnyddwyr eraill ar y rhwydwaith cyhoeddus ddarllen neu addasu cyfeiriadur eich ffolderi lleol.

Q9: Beth yw porth caeth (captive portal)?

Y dudalen fewngofnodi y mae rhwydweithiau gwestai neu gaffis yn ei defnyddio i roi mynediad i'r rhyngrwyd, y gall ymosodwyr ei ffugio weithiau.

Q10: A ddylwn i ddiffodd Wi-Fi pan nad wyf yn ei ddefnyddio?

Ydy, mae analluogi Wi-Fi yn atal eich dyfais rhag cysylltu'n awtomatig â rhwydweithiau nad oes modd ymddiried ynddynt.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan C)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q1: Sut mae ymosodiad Dyn-yn-y-Canol yn manteisio ar DNS?

Drwy ddefnyddio ffugio DNS ar lwybrydd twyllodrus i gyfeirio porwyr targed at dudalennau glanio gwe-rwydo sy'n edrych yn debyg yn hytrach na'r parthau targed.

Q2: Beth yw herwgipio sesiwn?

Ymosodwr sy'n sniffio cwci sesiwn heb ei amgryptio dros Wi-Fi cyhoeddus ac yn ei fewnforio i osgoi mewngofnodi â manylion.

Q3: Beth yw stripio SSL?

Ymosodiad MitM lle mae ymosodwr yn israddio cais HTTPS diogel defnyddiwr i HTTP heb ei amgryptio, gan gipio manylion mewngofnodi mewn testun plaen.

Q4: Sut mae HSTS yn diogelu rhag stripio SSL?

Mae HTTP Strict Transport Security yn gorfodi porwyr i gysylltu drwy HTTPS yn unig, gan wrthod disgyn yn ôl i HTTP heb ei amgryptio. [3]

Q5: Beth yw VPN twnnel hollt?

Ffurfweddiad sy'n llwybro traffig corfforaethol yn unig drwy'r VPN gan anfon data'r rhyngrwyd cyhoeddus yn uniongyrchol, a all beryglu datgelu llwybrau gollwng.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan D)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q6: Pam mae WPA2 yn agored i KRACK?

Mae'r Key Reinstallation Attack yn manteisio ar ysgwyd llaw pedair ffordd WPA2 i ddadgryptio pecynnau heb gyfrinair y Wi-Fi.

Q7: Beth yw ynysu cleientiaid?

Gosodiad diogelwch llwybrydd sy'n atal dyfeisiau Wi-Fi cysylltiedig rhag cyfathrebu â'i gilydd yn uniongyrchol, gan flocio sniffio lleol.

Q8: Sut mae ymosodwyr yn defnyddio gweinyddion DNS ffug?

Maent yn ffurfweddu llwybryddion twyllodrus i neilltuo gweinyddion DNS ffug i gleientiaid, gan ganiatáu iddynt ryng-gipio ac ailysgrifennu pob chwiliad gwe.

Q9: A all VPN guddio fy nghyfeiriad MAC lleol?

Na. Dynodwyr haen-2 lleol yw cyfeiriadau MAC; defnyddiwch osodiad hapnodi MAC adeiledig (cyfeiriad preifat) eich dyfais yn lle hynny.

Q10: Beth yw ymosodiad ffugio porth caeth?

Ymosodwr sy'n cynnal porth dilysu ffug ar fan problemus twyllodrus i ddwyn manylion mewngofnodi dan gochl mynediad Wi-Fi am ddim.

Rhan 11: 10 Ffaith a Mewnwelediad Seiberddiogelwch o'r Byd Go Iawn

Adolygwch ffeithiau o'r byd go iawn am dor-diogelwch, mecanweithiau amddiffyn, a safonau cydymffurfio.

1. CIPOLWG AR DDIOGELWCH

Mae gweithwyr o bell yn aml yn defnyddio Wi-Fi mewn caffis, gwestai a meysydd awyr, lle na allant reoli diogelwch y rhwydwaith.

2. CIPOLWG AR DDIOGELWCH

Gall man problemus twyllodrus Evil Twin gopïo union enw a chyfeiriad MAC rhwydwaith dibynadwy, gan ddrysu dyfeisiau.

3. CIPOLWG AR DDIOGELWCH

Mae meddalwedd sniffian pecynnau fel Wireshark am ddim a gall ddangos cyfrineiriau HTTP heb eu hamgryptio fel testun clir.

4. CIPOLWG AR DDIOGELWCH

Mae diogelwch WPA3 yn defnyddio Simultaneous Authentication of Equals (SAE) i amddiffyn rhag ymosodiadau grym ysgrublaidd lleol.

5. CIPOLWG AR DDIOGELWCH

Mae ymosodiadau tynnu SSL yn osgoi diogelwch HTTPS sylfaenol drwy ryng-gipio ailgyfeiriadau HTTP cychwynnol yn y porth.

6. CIPOLWG AR DDIOGELWCH

Mae penawdau ymateb HTTP Strict Transport Security (HSTS) yn atal porwyr rhag disgyn yn ôl i gysylltiadau HTTP heb eu hamgryptio. [3]

7. MEWNWELEDIAD DIOGELWCH

Mae diffodd 'Auto-Connect' yn atal ffonau clyfar rhag cysylltu â rhwydweithiau twyllodrus sy'n edrych yn debyg mewn mannau cyhoeddus.

8. MEWNWELEDIAD DIOGELWCH

Mae ffurfweddiadau VPN 'always-on' menter yn gorfodi holl draffig rhwydwaith gweithwyr o bell drwy waliau tân corfforaethol.

9. MEWNWELEDIAD DIOGELWCH

Gall pwyntiau mynediad twyllodrus roi atebion DNS ffug, gan ailgyfeirio parthau targed i weinyddion gwe-rwydo.

10. CIPOLWG AR DDIOGELWCH

Heb VPN, gall defnyddwyr eraill ar fan problemus agored weld pa wefannau a gweinyddion y mae eich dyfais yn cysylltu â nhw.

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau byd-eang NIST, OWASP a chydymffurfio â phreifatrwydd data.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Cwestiwn 1** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw ymosodiad Dyn-yn-y-Canol (MitM)? → Rhyng-gipio a newid cyfathrebiadau rhwng dau barti ar rwydwaith a rennir

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw pwynt mynediad twyllodrus (Gefell Drwg)? → Man problemus Wi-Fi maleisus wedi'i ffurfweddu gyda'r un SSID â rhwydwaith dilys

3 **Cwestiwn 3** — **Ateb Cywir: A**

NODYN ADDYSGU

Sut mae VPN yn diogelu traffig Wi-Fi cyhoeddus? → Mae'n lapio pob pecyn rhwydwaith mewn twnnel wedi'i amgryptio, gan eu gwneud yn annarllenadwy i sniffwyr

4 **Cwestiwn 4** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw sniffian pecynnau? → Defnyddio offer caledwedd neu feddalwedd i gipio a chofnodi pecynnau rhwydwaith

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw rôl HTTPS? → Amgryptio traffig y sesiwn rhwng y porwr a'r gweinydd gwe

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gall defnyddwyr cysylltiedig ddal data testun plaen yn hawdd ar rwydweithiau Wi-Fi cyhoeddus agored.

7 **Cwestiwn 7** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: man cyswllt heb awdurdod a sefydlir gan ymosodwr i ddynwared un go iawn yw Evil Twin.

8 **Cwestiwn 8** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae VPN yn amgryptio traffig mewn twnnel, felly ni all sniffwyr lleol ei ddarllen.

9 **Cwestiwn 9** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae HTTPS yn amgryptio'r gyfnewidfa HTTP gyfan, gan gynnwys llwybr yr URL a chynnwys y dudalen.

10 **Cwestiwn 10** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae mannau problemus Wi-Fi sy'n defnyddio diogelwch WPA3 yn cynnig amddiffyniad cryfach na rhwydweithiau agored heb gyfrinair.

Allweddi Geirfa a Chyfarwyddyd Marcio

Cyfarwyddyd Marcio i Athrawon: Rhowch 1 pwynt am bob paru cywir (8 pwynt i gyd) a phob term cyd-destun (6 phwynt i gyd).

PWYNT GWIRIO 4: ALLWEDD PARU CYSYNIADAU

E 1. RHYNG-GIPIO	F 2. CLUSTFEINIO	D 3. GEFELL DRWG	H 4. HTTPS
G 5. VPN	B 6. TWNNEL	A 7. WPA3	C 8. WAL DÂN

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 RHYNGIPIO	2 SNIFFIO	3 GEFAILL DRWG	4 HTTPS
5 CLEIENT VPN	6 TWNNEL		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 G – SAFONWPA	2 C – GEFAILLDRWG	3 B – SNIFFIO	4 F – TWNNEL
5 H – WALDAN	6 A – RHYNGIPIO	7 E – CLEIENTVPN	8 D – HTTPS

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio RHYNG-GIPIO, CLUSTFEINIO a GEFELL DRWG yn eu geiriau eu hunain a rhoi enghraifft o bob un.

Astudiaethau Achos:
Gofynnwch i fyfyrwyr gefnogi eu hargymhellion â ffeithiau o'r daflen waith yn hytrach na thybiaethau.

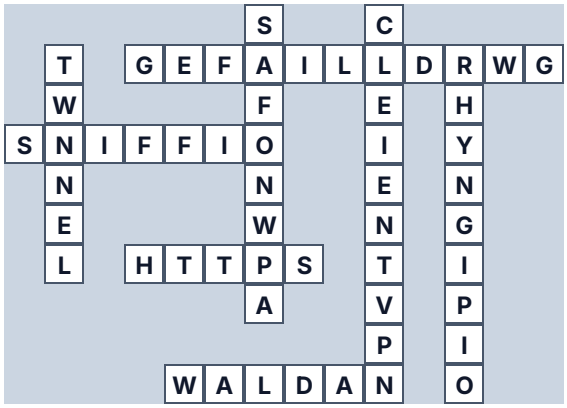
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

K	X	M	Y	P	X	F	T	O	P	L	C	R	I	G
N	R	S	M	P	X	Q	W	I	O	W	C	U	S	T
N	E	P	L	J	B	A	N	F	B	A	C	P	X	L
P	K	T	Y	K	X	T	N	F	K	L	D	Q	M	J
V	D	T	I	N	G	N	E	I	K	D	Q	P	R	G
T	M	H	M	Q	E	R	L	N	S	A	T	T	H	G
N	C	S	Q	O	F	H	S	S	B	N	W	D	Y	S
E	Z	V	C	Z	A	W	F	A	K	H	Z	D	N	N
I	D	Q	X	P	I	C	U	F	B	A	Z	N	G	D
E	K	A	D	O	L	D	F	O	H	I	D	R	I	Q
L	M	E	I	R	L	Z	S	N	F	Q	V	F	P	A
C	A	Q	O	N	D	P	T	W	X	Q	K	R	I	U
S	D	N	Y	B	R	F	S	P	X	W	J	A	O	R
Z	Y	Y	L	G	W	I	M	A	R	J	M	L	T	O
H	Q	Q	H	Z	G	A	O	V	G	U	B	Y	R	Y

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

4 ar draws: GEFAILLDRWG Man Wi-Fi twyllodrus sy'n dynwared rhwydwaith Wi-Fi. (11 llythyren)

6 ar draws: SNIFFIO Cipio pecynnau data rhwydwaith. (7 llythyren)

7 ar draws: HTTPS Trosglwyddo gwe diogel. (5 llythyren)

8 ar draws: WALDAN Hidlo traffig sy'n dod i mewn. (6 llythyren)

CLIWIAU I LAWR

1 i lawr: SAFONWPA Diogelwch Wi-Fi modern (WPA3). (8 llythyren)

2 i lawr: CLEIENTVPN Rhwydwaith preifat rhithwir wedi'i amgryptio. (10 llythyren)

3 i lawr: TWNNEL Llwybr data diogel wrth deithio. (6 llythyren)

5 i lawr: RHYNGIPIO Darllen traffig wrth iddo deithio. (9 llythyren)

Allwedd Datrys Geiriau Cymysg a Seiffr

Allwedd marcio ar gyfer y gweithgaredd dad-sgramblo geirfa a'r Her Seiffr Gyfrinachol.

ALLWEDD DATRYS GEIRIAU CYMYSG

1.	IGNHRPIOY	RHYNGIPIO	5.	FOFISIN	SNIFFIO
2.	IGEGWLFRDLA	GEFAILLDRWG	6.	PHTST	HTTPS
3.	CNPTLENIVE	CLEIENTVPN	7.	ETNLNW	TWNNEL
4.	OPAWNSAF	SAFONWPA	8.	LNWADA	WALDAN

ALLWEDD HER Y SEIFFR CYFRINACHOL

"AMGRYPTIWCH TRAFFIG WIFI CYHOEDDUS GYDA VPN"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Cyfyngu ar Sniffian Pecynnau ar Wi-Fi Cyhoeddus

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae uwch-weithredwr gwerthu o bell sydd wedi'i gysylltu â rhwydwaith Wi-Fi cyhoeddus mewn maes awyr yn sylwi bod sawl e-bost busnes sensitif wedi'u gollwng yn fuan ar ôl iddo eu hanfon mewn testun plaen.
- Strategaeth ac Ateb a Argymhellir: Gwnewch hi'n orfodol defnyddio cleient VPN menter ar bob gweithfan o bell. Gorfodwch estyniadau porwr HTTPS-yn-unig, a rhwystrwch brotocolau heb eu hamgryptio (fel HTTP ac FTP) ar wal dân y cleient.

B Astudiaeth Achos 2: Amddiffyn rhag Mannau Problemus Twyllodrus Evil Twin

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae ymosodwyr yn gosod pwynt mynediad diwifr twyllodrus o'r enw 'CoffeeShop_Guest' sy'n dynwared man problemus caffi dilys, gan gipio traffig rhwydwaith gwesteion diarwybod.
- Strategaeth a Datrysiad a Argymhellir: Archwiliwch gyfeiriadau MAC BSSID pwyntiau mynediad i wirio dilysrwydd y rhwydwaith. Gorfodwch ddilysu ystum cleientiaid i rwystro cysylltu â rhwydweithiau agored, a mynnwch fannau problemus (hotspots) cellog ar gyfer gwaith sensitif.