Enw: _____ Dyddiad: _____ Sgôr: _____

Ymosodiadau Gwe-rwydo a Pheirianneg Gymdeithasol

Gwe-rwydo gwaywffon, sgamiau morfila, protocolau SPF/DKIM/DMARC, ffugio anfonwyr, a hyfforddiant diogelwch i weithwyr.

TROSOLWG DYSGU YMOSODIADAU GWE-RWYDO

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 ymosodiadau gwe-rwydo a pheirianneg gymdeithasol. Byddwch yn archwilio gwe-rwydo wedi'i dargedu, morfila, ffugio parthau, protocolau SPF/DKIM/DMARC, diogelwch dolenni a hyfforddiant ymwybyddiaeth i weithwyr.

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/ymosodiadau-gwe-pysgota/

Eich Map Llwybr Dysgu Lliniaru Gwe-rwydo

- Nodwch sgamiau gwe-rwydo, gwe-rwydo llais (vishing) a ffenestri naid cymorth cyffredin.
- Rhowch weithdrefnau dilysu trafodion y tu allan i'r band ar waith.
- Ffurfweddwch reolau SPF, DKIM a DMARC i rwystro parthau ffug.

CYFARWYDDIADAU'R CANLLAW YMOSODIADAU GWE-RWYDO

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 ddilysu e-bost. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

YMOSODIADAU GWE-RWYDO A PHEIRIANNEG GYMDEITHASOL (CYFLWYNIAD)

Mae ymosodiadau gwe-rwydo yn defnyddio negeseuon wedi'u targedu, sgamiau whaling a ffugio parthau i gasglu manylion mewngofnodi defnyddwyr. Mae diogelu systemau corfforaethol yn gofyn am roi rheolau SPF, DKIM a DMARC ar waith wrth y porth ochr yn ochr â chamau cymeradwyo y tu allan i'r sianel.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw gwe-rwydo gwaywffon?**
   - A. E-bost gwe-rwydo wedi'i dargedu ac wedi'i deilwra i unigolyn neu sefydliad penodol
   - B. Neges e-bost swmp eang a anfonir at filiynau o gyfeiriadau ar hap
   - C. Ymosodiad rhwydwaith sy'n gorlifo gweinyddion gwe â thraffig
   - D. Techneg echdynnu cronfa ddata sy'n targedu cofnodion defnyddwyr

2. **2. Pa brotocol sy'n gadael i barth restru ei gyfeiriadau IP anfon awdurdodedig yn y DNS i frwydro yn erbyn ffugio?**
   - A. SPF
   - B. DKIM
   - C. DMARC
   - D. HTTPS

3. **3. Beth yw ymosodiad morfila?**
   - A. Ymgyrch we-rwydo wedi'i thargedu'n benodol at uwch-swyddogion gweithredol corfforaethol amlwg
   - B. Ymosodiad chwistrellu SQL sy'n targedu copïau wrth gefn o gronfeydd data
   - C. Dwyn offer llwybrydd rhwydwaith ardal leol yn ffisegol
   - D. Sgan grym llwyr awtomataidd sy'n stwffio manylion mewngofnodi

4. **4. Beth mae DKIM yn ei wneud?**
   - A. Yn ychwanegu llofnod cryptograffig at e-byst i ddilysu dilysrwydd yr anfonwr
   - B. Rhwystro traffig pecynnau rhwydwaith sy'n dod i mewn wrth y wal dân
   - C. Yn amgryptio cyfeintiau storio cronfeydd data wrth orffwys
   - D. Mae'n sganio atodiadau e-bost am faleiswedd ar sail llofnodion

5. **5. Beth yw rôl DMARC?**
   - A. Cyfarwyddo gweinyddion e-bost sy'n derbyn ar sut i drin gwiriadau SPF/DKIM sydd wedi methu
   - B. Dadgryptio cyfrineiriau system gan ddefnyddio tablau enfys wedi'u rhag-gyfrifo
   - C. Cywasgu atodiadau e-bost cyn eu danfon
   - D. Ffurfweddu breintiau mynediad llwybro rhwydwaith

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae gwe-rwydo gwaywffon yn dibynnu ar negeseuon e-bost swmp generig a anfonir at filiynau o gyfeiriadau ar hap.

Gwir Gau

7 Cwestiwn 7

7. Gall polisïau DMARC gyfarwyddo gweinyddion post i wrthod negeseuon ffug heb awdurdod.

Gwir Gau

8 Cwestiwn 8

8. Mae dilysu SPF yn gweithio drwy ddilysu llofnod cryptograffig corff yr e-bost.

Gwir Gau

9 Cwestiwn 9

9. Mae ymosodiadau morfila yn targedu gweinyddwyr corfforaethol lefel isel i gael mynediad at ffeiliau cronfa ddata.

Gwir Gau

10 Cwestiwn 10

10. Mae gwirio ceisiadau am daliad y tu allan i'r sianel wreiddiol yn helpu i atal sgamiau trosglwyddo arian gwifren.

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 dargedu gweithiwr penodol gyda gwybodaeth bersonol yw gwe-rwydo _____ .

2. Yr enw ar newid pennawd e-bost yn dwyllodrus i wneud i negeseuon edrych yn ddilys yw _____ anfonwr.

3. Y cofnod DNS sy'n rhestru IPau gweinyddion post awdurdodedig yw _____ .

4. Y safon llofnod e-bost sy'n dilysu'r anfonwr yw _____ .

5. Mae sefydlu polisïau i wrthod negeseuon sy'n methu gwiriadau SPF/DKIM yn defnyddio _____ .

6. Yr enw ar ymgyrch we-rwydo sy'n targedu uwch swyddogion gweithredol yw _____ .

BANC GEIRIAU GEIRFA

DKIM DMARC FFUGIO GWAYWFFON GWE-RWYDO MORFILA SPF VISHING

Ysgrifennwch eich atebion yma:

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

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

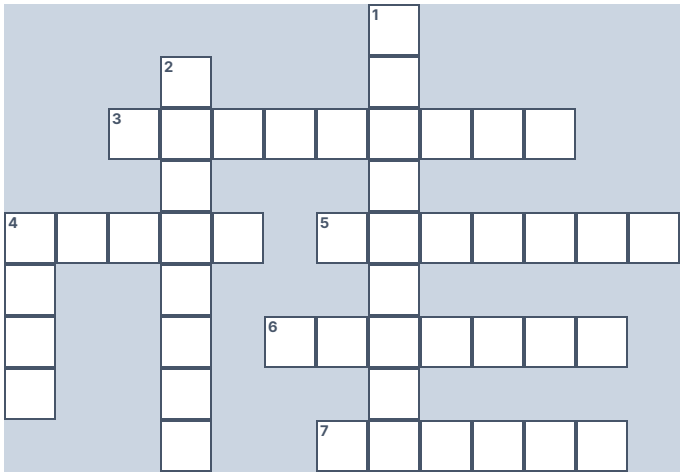
PARU DIFFINIADAU

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. GWAYWFFON	A	Galwadau sgam dros y llais.
☐	2. FFUGIO	B	Targedu uwch swyddogion gweithredol.
☐	3. SPF	C	Cyfarwyddiadau gwrthod polisi.
☐	4. DKIM	D	IPs anfonwyr awdurdodedig yn y DNS.
☐	5. DMARC	E	E-bost peirianneg gymdeithasol.
☐	6. MORFILA	F	E-bost wedi'i dargedu a'i bersonoli.
☐	7. GWE-RWYDO	G	Ffugio cyfeiriad e-bost yr anfonwr.
☐	8. GWE-RWYDO LLAIS	H	Llofnod cryptograffig mewn e-bost.

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

3. E-bost personol wedi'i dargedu. (9)

4. Cyfarwyddiadau polisi gwrthod. (5)

5. Targedu uwch swyddogion gweithredol. (7)

6. Galwadau sgam dros y llais. (7)

7. Creu cyfeiriad e-bost anfonwr ffug. (6)

CLIWIAU I LAWR

1. IPau anfonwyr awdurdodedig yn y DNS. (9)

2. E-bost peirianneg gymdeithasol. (8)

4. Llofnod cryptograffig mewn e-bost. (4)

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

3 ar draws: E-bost personol wedi'i dargedu. (9 llythyren):

4 ar draws: Cyfarwyddiadau polisi gwrthod. (5 llythyren):

5 ar draws: Targedu uwch swyddogion gweithredol. (7 llythyren):

6 ar draws: Galwadau sgam dros y llais. (7 llythyren):

7 ar draws: Creu cyfeiriad e-bost anfonwr ffug. (6 llythyren):

CLIWIAU I LAWR

1 i lawr: IPau anfonwyr awdurdodedig yn y DNS. (9 llythyren):

2 i lawr: E-bost peirianneg gymdeithasol. (8 llythyren):

4 i lawr: Llofnod cryptograffig mewn e-bost. (4 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.

C R I G N R M V P X Q O C U S

T E C L J B A I B C F P X L K

Y K R X T K D S Q M F J D I N

F N A K Q P G H M M U Q R S T

P T M G C G S I Q O G H S G B

S W D D S W Z N V C I Z W W F

D K H Z D A N G M D O Q X E P

O C U B A Y Z N O D K A D R O

N D F H I W D R R Q M E I W R

F Z S F Q F D V F F A A Q Y O

O N P T X F K Q I K R U S D D

C N Y B F O I S L X W J A O R

Z Y Y L G N M I A M R J M L T

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

B H L Z G J O P N W C M Z Y G

RHESTR GEIRIAU GEIRFA

GWAYWFFON FFUGIO COFNODSPF DKIM DMARC MORFILA GWERWYDO VISHING

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. GWAYWFFON
B. FFUGIO
C. COFNODSPF
D. DKIM
E. DMARC
F. MORFILA
G. GWERWYDO
H. VISHING

	DIFFINIADAU A MEYSYDD PARU
	1. Creu cyfeiriad e-bost anfonwr ffug.
	2. E-bost personol wedi'i dargedu.
	3. Galwadau sgam dros y llais.
	4. IPau anfonwyr awdurdodedig yn y DNS.
	5. E-bost peirianneg gymdeithasol.
	6. Cyfarwyddiadau polisi gwrthod.
	7. Llofnod cryptograffig mewn e-bost.
	8. Targedu uwch swyddogion gweithredol.

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. **FWYWGFONA** _____
2. **FCPNODSOF** _____
3. **ADCRM** _____
4. **RDOYWGWE** _____
5. **GUOFIF** _____
6. **IMDK** _____
7. **MLIAOFR** _____
8. **IHGVNIS** _____

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Dyfeisiau y gellir eu hacio			
2	Arwyddion o e-bost gwe-rwydo			
3	Arwyddion bod cyfrifiadur wedi'i heintio			
4	Geiriau sy'n creu brys ffug			
5	Ffyrdd o wirio anfonwr			
6	Pobl y gallwch ofyn iddynt am help TG			
7	Pethau rydych chi'n gwneud copi wrth gefn ohonynt			
8	Pysgod neu greaduriaid y môr rydych chi'n eu hadnabod			
9	Cwmnïau y mae sgamwyr yn esgus bod			
10	Arferion diogel y gallwch eu dechrau heddiw			
11	Pethau i'w gwneud ar ôl clicio ar ddolen ffug			
12	Pethau i'w gwneud ar ôl gollyngiad data			
13	Sianeli lle mae gwe-rwydo'n digwydd			
14	Pethau nad ydych chi byth yn eu hanfon drwy e-bost			
15	Ffyrdd o ddiogelu eich cyfrifon			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

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

ASTUDIAETH ACHOS 1: UNIONI YMOSODIAD MORFILA AR UWCH-SWYDDOGION

👨‍💼

Senario: Mae Prif Swyddog Ariannol yn derbyn e-bost hynod bersonol sy'n honni ei fod gan y Prif Weithredwr, yn gofyn am drosglwyddiad gwifren cyflym o $50,000 i gwblhau pryniant parth cyfrinachol.

Cwestiwn Trafod: Dadansoddwch y risgiau o ffugio brand, a disgrifiwch yn fanwl SPF/DKIM/DMARC a rheolaethau dilysu.

ASTUDIAETH ACHOS 2: GWEITHREDU POLISÏAU PORTH SPF/DKIM/DMARC

👨‍💼

Senario: Mae menter yn methu archwiliadau diogelwch oherwydd bod negeseuon e-bost marchnata sy'n mynd allan yn aml yn cael eu nodi fel sbam, ac mae hacwyr wrthi'n ffugio parth brand y cwmni.

Cwestiwn Trafod: Sefydlwch reolaethau technegol a gweinyddol i wirio dilysrwydd e-byst.

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

4 1 20 7 5 12 23 3 8 2 5 9 18 9 1 14 14 5 7

7 25 13 4 5 9 20 8 1 19 15 12 13 5 23 14

5 2 15 19 20

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: Beth yw gwe-rwydo?

Ymosodiad peirianneg gymdeithasol yw gwe-rwydo lle mae troseddwyr yn anfon negeseuon twyllodrus i dwyllo defnyddwyr i rannu data sensitif.

Q2: Beth yw'r gwahaniaeth rhwng gwe-rwydo a gwe-rwydo wedi'i dargedu (spear phishing)?

Mae gwe-rwydo yn targedu grwpiau eang gyda chynnwys generig, tra bod gwe-rwydo wedi'i dargedu (spear phishing) yn targedu dioddefwyr penodol gan ddefnyddio manylion wedi'u teilwra.

Q3: Beth yw morfila (whaling)?

Mae morfila yn ymosodiad gwe-rwydo wedi'i dargedu'n fanwl at swyddogion gweithredol proffil uchel sydd â phŵer gweinyddol.

Q4: Beth yw ffugio e-bost?

Ffugio e-bost yw creu negeseuon e-bost gyda chyfeiriad anfonwr ffug i dwyllo'r derbynnydd i ymddiried yn y ffynhonnell.

Q5: Sut mae SPF yn atal ffugio?

Mae'n cyhoeddi rhestr o gyfeiriadau IP anfon awdurdodedig yn DNS, gan alluogi gweinyddion sy'n derbyn i ddilysu ffynhonnell y post. [1]

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

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

Q6: Beth yw DKIM?

Mae DomainKeys Identified Mail yn ychwanegu llofnod cryptograffig at benawdau e-bost, gan brofi bod parth wedi cymryd cyfrifoldeb ac nad yw'r neges wedi'i newid.

Q7: Beth yw ystyr DMARC?

Dilysu, Adrodd a Chydymffurfio Negeseuon yn seiliedig ar Barth (Domain-based Message Authentication, Reporting, and Conformance). [2]

Q8: Beth yw polisi DMARC?

Polisi sy'n dweud wrth weinyddion post sut i drin negeseuon sy'n methu SPF/DKIM (none, quarantine neu reject). [2]

Q9: Beth yw gwe-rwydo llais (vishing)?

Gwe-rwydo llais, lle mae ymosodwyr yn defnyddio galwadau ffôn twyllodrus i gael data gweinyddol neu ariannol.

Q10: Sut mae sganwyr dolenni'n helpu?

Maent yn sganio ac yn ailysgrifennu dolenni mewn e-byst sy'n dod i mewn i wirio diogelwch y tudalennau gwe cyrchfan ar adeg y clic.

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 homograff yn gweithio?

Mae ymosodwyr yn cofrestru enwau parth gan ddefnyddio nodau Unicode nad ydynt yn ASCII sy'n edrych yn debyg er mwyn dynwared enw parth dilys yn weledol.

Q2: Beth yw cynrychioliad punycode?

Amgodiad sy'n trosi enwau parth Unicode yn llinynnau sy'n gydnaws ag ASCII ac sy'n dechrau gydag 'xn--' fel y gall DNS eu trin.

Q3: Pam mai 'p=reject' yw'r cyflwr DMARC mwyaf diogel?

Mae'n gofyn i weinyddion sy'n derbyn wrthod post sy'n methu DMARC (SPF/DKIM wedi'u halinio) yn ystod y sesiwn SMTP, gan rwystro ffugio uniongyrchol. [2]

Q4: Sut mae ymosodwyr yn osgoi rheolau SPF?

Drwy fanteisio ar barthau sy'n edrych yn debyg (typosquatting) neu ddefnyddio cyfrifon sydd wedi'u cyfaddawdu ar wasanaethau e-bost trydydd parti dilys.

Q5: Beth yw cyfaddawdu e-bost busnes (BEC)?

Sgam corfforaethol lle mae ymosodwyr yn herwgipio neu'n dynwared cyfrifon e-bost busnes i awdurdodi taliadau twyllodrus.

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

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

Q6: Sut mae dilysu aml-ffactor yn atal gwe-rwydo?

Mae'n gofyn am docynnau eilaidd (fel allweddi caledwedd) na ellir eu dwyn drwy dudalennau glanio ffug yn unig.

Q7: Beth yw tudalen lanio cynaeafu manylion mewngofnodi?

Porth mewngofnodi ffug sy'n edrych yn debyg ac sydd wedi'i gynllunio i gipio enwau defnyddwyr, cyfrineiriau a thocynnau MFA a roddir mewn amser real.

Q8: Beth yw herwgipio is-barthau?

Ymosodwr sy'n cymryd rheolaeth ar bwyntydd is-barth DNS nas defnyddir i gynnal tudalennau glanio gwe-rwydo maleisus o dan riant-barth dibynadwy.

Q9: Sut mae gwiriad aliniad DKIM yn gweithio?

Mae'n dilysu bod y parth ym mhennawd 'From' yn cyfateb i'r parth a lofnododd y neges yn gryptograffig ym mhennawd DKIM.

Q10: Beth yw rôl porth e-bost?

Hidlo e-bost sy'n dod i mewn, archwilio dolenni, rhoi atodiadau mewn blwch tywod, a dilysu cydymffurfiaeth SPF/DKIM/DMARC.

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

Gwe-rwydo a ffugio oedd y math o drosedd a adroddwyd amlaf i IC3 yr FBI yn 2025, gyda 191,561 o gwynion. [4]

2. CIPOLWG AR DDIOGELWCH

Achosodd cyfaddawdu e-bost busnes (BEC) golledion o dros $3 biliwn a adroddwyd i IC3 yr FBI yn 2025. [4]

3. CIPOLWG AR DDIOGELWCH

Mae ymosodiadau homograff yn defnyddio llythrennau Cyrilig tebyg i ddyblygu parthau brand union-gyfatebol yn weledol mewn porwyr.

4. CIPOLWG AR DDIOGELWCH

Gyda 'p=reject', mae parth yn gofyn i dderbynwyr wrthod post sy'n methu yn ystod y danfon, nid ei ffeilio fel sbam. [2]

5. CIPOLWG AR DDIOGELWCH

Mae ymosodiadau morfila sy'n targedu Prif Weithredwyr yn aml yn gofyn am daliadau brys ar gyfer uno cyfrinachol neu brynu parthau.

6. CIPOLWG AR DDIOGELWCH

Mae pyrth cynaeafu manylion mewngofnodi yn copïo tudalennau mewngofnodi go iawn fel bod dioddefwyr yn teipio cyfrineiriau'n syth i ffurflen yr ymosodwr.

7. MEWNWELEDIAD DIOGELWCH

Mae canllawiau gwe-rwydo ar y cyd CISA yn argymell hyfforddi defnyddwyr ochr yn ochr â DMARC, SPF, DKIM ac MFA sy'n gwrthsefyll gwe-rwydo. [3]

8. MEWNWELEDIAD DIOGELWCH

Mae gwerthuso SPF wedi'i gyfyngu i 10 term sy'n holi DNS; mae mynd dros y terfyn yn rhoi canlyniad 'permerror'. [1]

9. MEWNWELEDIAD DIOGELWCH

Mae allweddi diogelwch caledwedd FIDO2 yn darparu diogelwch a gefnogir yn gryptograffig rhag cynaeafu manylion mewngofnodi o bell.

10. CIPOLWG AR DDIOGELWCH

Gwe-rwydo yw un o'r ffyrdd mwyaf cyffredin y mae ymosodwyr yn cael mynediad i sefydliad am y tro cyntaf, a dyna pam mae hyfforddiant ymwybyddiaeth rheolaidd yn amddiffyniad effeithiol.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] 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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[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 gwe-rwydo gwaywffon? → E-bost gwe-rwydo wedi'i dargedu ac wedi'i deilwra i unigolyn neu sefydliad penodol

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae SPF yn cyhoeddi gwesteiwyr anfon awdurdodedig parth yn y DNS fel y gall derbynwyr wirio anfonwr yr amlen.

3 **Cwestiwn 3** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw ymosodiad morfila? → Ymgyrch we-rwydo wedi'i thargedu'n benodol at uwch-swyddogion gweithredol corfforaethol amlwg

4 **Cwestiwn 4** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth mae DKIM yn ei wneud? → Yn ychwanegu llofnod cryptograffig at e-byst i ddilysu dilysrwydd yr anfonwr

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw rôl DMARC? → Cyfarwyddo gweinyddion e-bost sy'n derbyn ar sut i drin gwiriadau SPF/DKIM sydd wedi methu

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae gwe-rwydo gwaywffon wedi'i deilwra i bobl benodol, yn wahanol i we-rwydo torfol generig.

7 **Cwestiwn 7** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gall polisïau DMARC gyfarwyddo gweinyddion post i wrthod negeseuon ffug heb awdurdod.

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

NODYN ADDYSGU

Gau: mae SPF yn gwirio'r IP anfon yn erbyn y DNS; DKIM yw'r un sy'n gwirio llofnod cryptograffig.

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

NODYN ADDYSGU

Gau: mae whaling yn targedu uwch swyddogion gweithredol, sy'n gallu cymeradwyo taliadau a chyrchu data sensitif.

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

NODYN ADDYSGU

Gwir: mae cadarnhau ceisiadau am daliad drwy sianel ar wahân a hysbys yn helpu i atal twyll gwifren.

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

F 1. GWAYWFFON	G 2. FFUGIO	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. MORFILA	E 7. GWE-RWYDO	A 8. GWE-RWYDO LLAIS

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 GWAYWFFON	2 FFUGIO	3 SPF	4 DKIM
5 DMARC	6 MORFILA		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 B – FFUGIO	2 A – GWAYWFFON	3 H – VISHING	4 C – COFNODSPF
5 G – GWERWYDO	6 E – DMARC	7 D – DKIM	8 F – MORFILA

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio GWAYWFFON, FFUGIO a SPF 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.

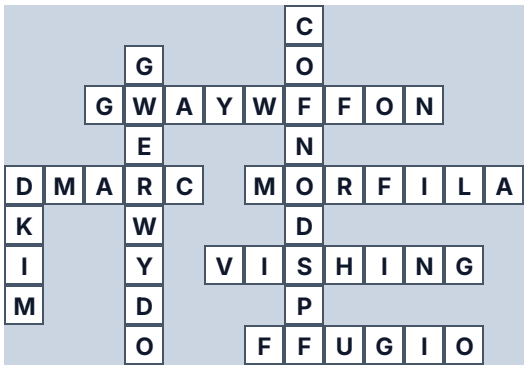
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

3 ar draws: GWAYWFFON E-bost personol wedi'i dargedu. (9 llythyren)

4 ar draws: DMARC Cyfarwyddiadau polisi gwrthod. (5 llythyren)

5 ar draws: MORFILA Targedu uwch swyddogion gweithredol. (7 llythyren)

6 ar draws: VISHING Galwadau sgam dros y llais. (7 llythyren)

7 ar draws: FFUGIO Creu cyfeiriad e-bost anfonwr ffug. (6 llythyren)

CLIWIAU I LAWR

1 i lawr: COFNODSPF IPau anfonwyr awdurdodedig yn y DNS. (9 llythyren)

2 i lawr: GWERWYDO E-bost peirianneg gymdeithasol. (8 llythyren)

4 i lawr: DKIM Llofnod cryptograffig mewn e-bost. (4 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.	FWYWGFONA	GWAYWFFON	5.	GUOFIF	FFUGIO
2.	FCPNODSOF	COFNODSPF	6.	IMDK	DKIM
3.	ADCRM	DMARC	7.	MLIAOFR	MORFILA
4.	RDOYWGWE	GWERWYDO	8.	IHGVNIS	VISHING

ALLWEDD HER Y SEIFFR CYFRINACHOL

"DATGELWCH BEIRIANNEG GYMDEITHASOL MEWN EBOST"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Unioni Ymosodiad Morfila ar Uwch-swyddogion

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae Prif Swyddog Ariannol yn derbyn e-bost personol iawn sy'n honni ei fod gan y Prif Weithredwr, yn gofyn am drosglwyddiad gwifren cyflym o $50,000 i gwblhau pryniant parth cyfrinachol.
- Strategaeth a Datrysiad a Argymhellir: Ffurfweddwch DMARC gyda pholisi 'p=reject' i rwystro parthau anfonwyr ffug. Ychwanegwch faneri rhybudd anfonwr allanol yn y porth, a mynnwch gadarnhad llafar y tu allan i'r band ar gyfer pob trafodiad ariannol.

B Astudiaeth Achos 2: Gweithredu Polisïau Porth SPF/DKIM/DMARC

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae menter yn methu archwiliadau diogelwch oherwydd bod negeseuon e-bost marchnata allanol yn aml yn cael eu nodi fel sbam, ac mae hacwyr wrthi'n ffugio parth brand y cwmni.
- Strategaeth ac Ateb a Argymhellir: Cyhoeddwch gofnod TXT ar gyfer SPF sy'n manylu ar IPs anfonwyr awdurdodedig. Ffurfweddwch allweddi llofnodi DKIM ar weinyddion post sy'n mynd allan, a dadansoddwch adroddiadau adborth XML DMARC sy'n dod i mewn i nodi camddefnydd.