Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Επιθέσεις ηλεκτρονικού ψαρέματος και κοινωνική μηχανική

Spear phishing, απάτες whaling, πρωτόκολλα SPF/DKIM/DMARC, πλαστογράφηση αποστολέα και εκπαίδευση υπαλλήλων στην ασφάλεια.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΕΠΙΘΕΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στις επιθέσεις phishing και την κοινωνική μηχανική. Θα εξερευνήσεις spear phishing, whaling, πλαστογράφηση domain, πρωτόκολλα SPF/DKIM/DMARC, ασφάλεια συνδέσμων και εκπαίδευση ευαισθητοποίησης των εργαζομένων.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- [ ] **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- [ ] **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- [ ] **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- [ ] **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- [ ] **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/epithesei-phishing/

Η πορεία μάθησής σου: περιορισμός του ηλεκτρονικού ψαρέματος (phishing)

- Αναγνώρισε τις συνήθεις απάτες ηλεκτρονικού ψαρέματος (phishing), φωνητικού ψαρέματος (vishing) και αναδυόμενων παραθύρων υποστήριξης.
- Εφάρμοσε διαδικασίες επαλήθευσης συναλλαγών εκτός ζώνης (out-of-band).
- Ρύθμισε κανόνες SPF, DKIM και DMARC για να αποκλείεις πλαστά domain.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΕΠΙΘΕΣΕΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στην πιστοποίηση αυθεντικότητας email. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΕΠΙΘΕΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ (ΕΙΣΑΓΩΓΗ)

Οι επιθέσεις ηλεκτρονικού ψαρέματος χρησιμοποιούν στοχευμένα μηνύματα, απάτες whaling και πλαστοπροσωπία τομέα για να συλλέξουν διαπιστευτήρια σύνδεσης χρηστών. Η ασφάλιση των εταιρικών συστημάτων απαιτεί την εφαρμογή κανόνων SPF, DKIM και DMARC στην πύλη, παράλληλα με βήματα έγκρισης εκτός καναλιού.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1 **1. Τι είναι το spear phishing;**

- A. Ένα στοχευμένο email phishing προσαρμοσμένο σε ένα συγκεκριμένο άτομο ή οργανισμό
- B. Ένα ευρύ μαζικό email που αποστέλλεται σε εκατομμύρια τυχαίες διευθύνσεις
- C. Μια επίθεση δικτύου που κατακλύζει τους διακομιστές ιστού με κίνηση
- D. Μια τεχνική εξαγωγής βάσης δεδομένων που στοχεύει εγγραφές χρηστών

2 **2. Ποιο πρωτόκολλο επιτρέπει σε ένα domain να καταχωρίζει στο DNS τις εξουσιοδοτημένες διευθύνσεις IP αποστολής του για την καταπολέμηση της πλαστοπροσωπίας (spoofing);**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. Τι είναι μια επίθεση whaling;**

- A. Μια εκστρατεία phishing που στοχεύει ειδικά εταιρικά στελέχη υψηλού προφίλ
- B. Μια επίθεση SQL injection που στοχεύει αντίγραφα ασφαλείας βάσεων δεδομένων
- C. Μια φυσική κλοπή εξοπλισμού δρομολογητή τοπικού δικτύου
- D. Μια αυτοματοποιημένη σάρωση brute-force με credential stuffing

4 **4. Τι κάνει το DKIM;**

- A. Προσθέτει κρυπτογραφική υπογραφή στα email για να επαληθεύεται η αυθεντικότητα του αποστολέα
- B. Αποκλείει στο τείχος προστασίας την εισερχόμενη κίνηση πακέτων δικτύου
- C. Κρυπτογραφεί τους τόμους αποθήκευσης βάσεων δεδομένων σε κατάσταση ηρεμίας (at rest)
- D. Σαρώνει τα συνημμένα email για κακόβουλο λογισμικό βάσει υπογραφών

5 **5. Ποιος είναι ο ρόλος του DMARC;**

- A. Οδηγίες προς τους διακομιστές email λήψης για το πώς να χειρίζονται αποτυχημένους ελέγχους SPF/DKIM
- B. Αποκρυπτογράφηση κωδικών πρόσβασης συστήματος με προϋπολογισμένους πίνακες rainbow
- C. Συμπίεση συνημμένων email πριν από την παράδοση
- D. Ρύθμιση προνομίων πρόσβασης δρομολόγησης δικτύου

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Το spear phishing βασίζεται σε γενικά μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνονται σε εκατομμύρια τυχαίες διευθύνσεις.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Οι πολιτικές DMARC μπορούν να δώσουν εντολή στους διακομιστές αλληλογραφίας να απορρίπτουν μη εξουσιοδοτημένα πλαστά μηνύματα.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Η επαλήθευση SPF λειτουργεί επικυρώνοντας την κρυπτογραφική υπογραφή του σώματος του email.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Οι επιθέσεις whaling στοχεύουν χαμηλόβαθμους εταιρικούς διαχειριστές για να αποκτήσουν πρόσβαση σε αρχεία βάσεων δεδομένων.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Η επαλήθευση αιτημάτων πληρωμής εκτός καναλιού (out-of-band) βοηθά στη διακοπή απατών με τραπεζικά εμβάσματα.

○ Σωστό ○ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Η στόχευση ενός συγκεκριμένου υπαλλήλου με εξατομικευμένες πληροφορίες είναι _____ ψάρεμα.

2. Η παραποίηση της κεφαλίδας ενός email ώστε το μήνυμα να φαίνεται νόμιμο ονομάζεται _____ αποστολέα.

3. Η λίστα με τις εξουσιοδοτημένες IP διακομιστών αλληλογραφίας στο DNS ονομάζεται εγγραφή _____ .

4. Το πρότυπο υπογραφής email που παρέχει επαλήθευση αποστολέα είναι το _____ .

5. Η θέσπιση πολιτικών απόρριψης αποτυχημένων ελέγχων SPF/DKIM γίνεται με το _____ .

6. Μια εκστρατεία ηλεκτρονικού ψαρέματος που στοχεύει ανώτατα στελέχη ονομάζεται _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΠΛΑΣΤΟΓΡΑΦΗΣΗ ΣΤΟΧΕΥΜΕΝΟ ΦΑΛΑΙΝΟΘΗΡΑ DKIM DMARC SMISHING SPF VISHING

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

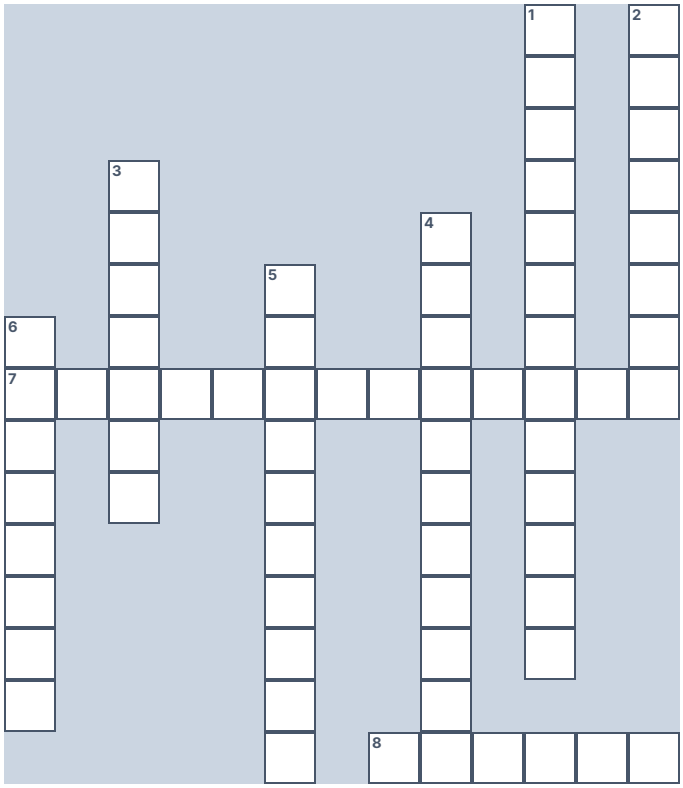
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. ΣΤΟΧΕΥΜΕΝΟ	A	Απατηλές κλήσεις μέσω φωνής.
☐	2. ΠΛΑΣΤΟΓΡΑΦΗΣΗ	B	Στοχεύουν στελέχη C-level.
☐	3. SPF	C	Οδηγίες απόρριψης πολιτικής.
☐	4. DKIM	D	IP εξουσιοδοτημένων αποστολέων DNS.
☐	5. DMARC	E	Μήνυμα ηλεκτρονικού ταχυδρομείου κοινωνικής μηχανικής.
☐	6. WHALING	F	Εξατομικευμένο στοχευμένο email.
☐	7. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	G	Πλαστογράφηση της διεύθυνσης email του αποστολέα.
☐	8. VISHING	H	Κρυπτογραφική υπογραφή στο email.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

7. Πλαστογράφηση της διεύθυνσης email του αποστολέα (13)

8. Email κοινωνικής μηχανικής (6)

ΚΑΘΕΤΑ

1. Απατηλές τηλεφωνικές κλήσεις με φωνή (13)

2. Οδηγίες για το τι θα γίνεται με τα email που αποτυγχάνουν στον έλεγχο του αποστολέα, όπως η απόρριψη (8)

3. Εγγραφή DNS με τις εξουσιοδοτημένες IP αποστολέων (SPF) (7)

4. Στόχευση ανώτατων στελεχών (C-level) (11)

5. Εξατομικευμένο στοχευμένο email (10)

6. Κρυπτογραφικός κωδικός πιστοποίησης που επισυνάπτεται σε κάθε email (8)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

7 οριζόντια: Πλαστογράφηση της διεύθυνσης email του αποστολέα (13 γράμματα):

8 οριζόντια: Email κοινωνικής μηχανικής (6 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Απατηλές τηλεφωνικές κλήσεις με φωνή (13 γράμματα):

2 κάθετα: Οδηγίες για το τι θα γίνεται με τα email που αποτυγχάνουν στον έλεγχο του αποστολέα, όπως η απόρριψη (8 γράμματα):

3 κάθετα: Εγγραφή DNS με τις εξουσιοδοτημένες IP αποστολέων (SPF) (7 γράμματα):

4 κάθετα: Στόχευση ανώτατων στελεχών (C-level) (11 γράμματα):

5 κάθετα: Εξατομικευμένο στοχευμένο email (10 γράμματα):

6 κάθετα: Κρυπτογραφικός κωδικός πιστοποίησης που επισυνάπτεται σε κάθε email (8 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Η Ψ Η Ξ Ψ Χ Σ Η Τ Χ Α Α Ο Υ Ν
Τ Ν Φ Ω Ξ Θ Ο Σ Θ Ο Ρ Υ Τ Ξ Υ
Α Τ Α Κ Α Ε Ξ Μ Η Λ Η Α Ν Υ Ζ
Π Η Ρ Ο Π Χ Ψ Κ Ι Κ Θ Υ Ι Ω Φ
Α Ψ Γ Ο Κ Θ Ι Ω Ι Ι Ο Ν Α Ε Θ
Η Α Ο Σ Α Τ Ι Ε Φ Ε Ν Κ Η Ω Κ
Κ Ε Π Κ Ι Π Ν Ι Α Ζ Ι Φ Ξ Κ Ν
Ι Γ Υ Λ Ν Γ Δ Η Θ Β Α Α Ξ Ρ Λ
Τ Ο Ο Φ Τ Θ Ψ Ζ Ω Ρ Λ Ρ Η Χ Φ
Η Π Θ Ε Π Τ Ν Τ Γ Κ Α Ρ Δ Τ Σ
Ν Π Λ Α Σ Τ Ο Γ Ρ Α Φ Η Σ Η Λ
Ω Ο Λ Ψ Α Ρ Ε Μ Α Μ Σ Θ Κ Ο Θ
Φ Ψ Σ Τ Ο Χ Ε Υ Μ Ε Ν Ο Ξ Λ Χ
Υ Ν Ψ Π Π Β Α Λ Ο Μ Β Λ Θ Ζ Ι
Ν Ψ Β Ω Ω Ψ Β Ν Υ Χ Μ Γ Ε Ξ Χ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΣΤΟΧΕΥΜΕΝΟ ΠΛΑΣΤΟΓΡΑΦΗΣΗ ΕΓΓΡΑΦΗ ΥΠΟΓΡΑΦΗ ΠΟΛΙΤΙΚΗ
ΦΑΛΑΙΝΟΘΗΡΑ ΨΑΡΕΜΑ ΦΩΝΗΤΙΚΗΑΠΑΤΗ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΣΤΟΧΕΥΜΕΝΟ

B. ΠΛΑΣΤΟΓΡΑΦΗΣΗ

C. ΕΓΓΡΑΦΗ

D. ΥΠΟΓΡΑΦΗ

E. ΠΟΛΙΤΙΚΗ

F. ΦΑΛΑΙΝΟΘΗΡΑ

G. ΨΑΡΕΜΑ

H. ΦΩΝΗΤΙΚΗΑΠΑΤΗ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Πλαστογράφηση της διεύθυνσης email του αποστολέα.
2. Εξατομικευμένο στοχευμένο email.
3. Απατηλές τηλεφωνικές κλήσεις με φωνή.
4. Εγγραφή DNS με τις εξουσιοδοτημένες IP αποστολέων (SPF).
5. Email κοινωνικής μηχανικής.
6. Οδηγίες για το τι θα γίνεται με τα email που αποτυγχάνουν στον έλεγχο του αποστολέα, όπως η απόρριψη.
7. Κρυπτογραφικός κωδικός πιστοποίησης που επισυνάπτεται σε κάθε email.
8. Στόχευση ανώτατων στελεχών (C-level).

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της κυβερνοασφάλειας. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. **ΝΜΥΕΤΣΕΟΧΟ**

2. **ΕΓΗΦΑΡΓ**

3. **ΙΟΠΤΙΗΚΛ**

4. **ΑΕΡΜΨΑ**

5. **ΑΗΛΑΡΤΗΟΦΓΠΣΣ**

6. **ΦΗΓΑΥΡΠΟ**

7. **ΘΙΦΑΟΑΗΡΛΝΑ**

8. **ΑΝΤΙΑΗΗΦΚΩΤΠΗ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	Συσκευές που μπορούν να παραβιαστούν			
2	Ενδείξεις ενός email ηλεκτρονικού ψαρέματος			
3	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
4	Λέξεις που δημιουργούν ψεύτικη επείγουσα ανάγκη			
5	Τρόποι να ελέγξεις έναν αποστολέα			
6	Άνθρωποι που μπορείς να ρωτήσεις για βοήθεια στην πληροφορική			
7	Πράγματα που παίρνεις αντίγραφο ασφαλείας			
8	Ψάρια ή θαλασσινά πλάσματα που γνωρίζεις			
9	Εταιρείες που μιμούνται οι απατεώνες			
10	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
11	Πράγματα που κάνεις αφού πατήσεις σε έναν ψεύτικο σύνδεσμο			
12	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			
13	Κανάλια όπου συμβαίνει το ηλεκτρονικό ψάρεμα			
14	Πράγματα που δεν στέλνεις ποτέ με email			
15	Τρόποι να προστατεύσεις τους λογαριασμούς σου			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΑΠΟΚΑΤΑΣΤΑΣΗ ΕΠΙΘΕΣΗΣ WHALING ΣΕ ΑΝΩΤΑΤΑ ΣΤΕΛΕΧΗ

👷

Σενάριο: Ένας Οικονομικός Διευθυντής (CFO) λαμβάνει ένα εξαιρετικά εξατομικευμένο email που ισχυρίζεται ότι προέρχεται από τον CEO και ζητά ένα γρήγορο έμβασμα 50.000 $ για να κλείσει μια εμπιστευτική αγορά domain.

Ερώτηση συζήτησης: Ανάλυσε τους κινδύνους πλαστοπροσωπίας brand και περίγραψε αναλυτικά τους ελέγχους SPF/DKIM/DMARC και ταυτοποίησης.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΕΦΑΡΜΟΓΗ ΠΟΛΙΤΙΚΩΝ ΠΥΛΗΣ SPF/DKIM/DMARC

👷

Σενάριο: Μια επιχείρηση αποτυγχάνει σε ελέγχους ασφαλείας επειδή τα εξερχόμενα email μάρκετινγκ επισημαίνονται συχνά ως ανεπιθύμητα, και χάκερ πλαστογραφούν ενεργά το domain του brand της εταιρείας.

Ερώτηση συζήτησης: Καθιέρωσε τεχνικούς και διοικητικούς ελέγχους για την επαλήθευση της γνησιότητας των email.

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

5	13	19	15	16	9	18	5		19	7	13

10	15	9	13	24	13	9	10	7		12	7	22	1	13	9	10	7		12	5

5	11	5	3	22	15	20	18

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Τι είναι το ηλεκτρονικό ψάρεμα;

Το ηλεκτρονικό ψάρεμα είναι μια επίθεση κοινωνικής μηχανικής όπου οι εγκληματίες στέλνουν δόλια μηνύματα για να εξαπατήσουν τους χρήστες ώστε να μοιραστούν ευαίσθητα δεδομένα.

Q2: Ποια είναι η διαφορά μεταξύ ηλεκτρονικού ψαρέματος και spear phishing;

Το ηλεκτρονικό ψάρεμα στοχεύει ευρείες ομάδες με γενικό περιεχόμενο, ενώ το spear phishing στοχεύει συγκεκριμένα θύματα με προσαρμοσμένες λεπτομέρειες.

Q3: Τι είναι το whaling;

Το whaling είναι μια εξαιρετικά στοχευμένη επίθεση ηλεκτρονικού ψαρέματος κατά υψηλόβαθμων στελεχών που έχουν διοικητική εξουσία.

Q4: Τι είναι η πλαστογράφηση email (email spoofing);

Η πλαστογράφηση email (email spoofing) είναι η δημιουργία μηνυμάτων email με πλαστή διεύθυνση αποστολέα, ώστε ο παραλήπτης να εμπιστευτεί την πηγή.

Q5: Πώς αποτρέπει το SPF την πλαστογράφηση;

Δημοσιεύει στο DNS μια λίστα εξουσιοδοτημένων διευθύνσεων IP αποστολής, επιτρέποντας στους διακομιστές παραλαβής να επαληθεύουν την πηγή της αλληλογραφίας. [1]

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Τι είναι το DKIM;

Το DomainKeys Identified Mail προσθέτει κρυπτογραφική υπογραφή στις κεφαλίδες των email, αποδεικνύοντας ότι ένα domain ανέλαβε την ευθύνη και ότι το μήνυμα δεν τροποποιήθηκε.

Q7: Τι σημαίνει DMARC;

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: Τι είναι μια πολιτική DMARC;

Μια πολιτική που λέει στους διακομιστές αλληλογραφίας πώς να χειρίζονται μηνύματα που αποτυγχάνουν στους ελέγχους SPF/DKIM (none, quarantine ή reject). [2]

Q9: Τι είναι το vishing;

Φωνητικό ηλεκτρονικό ψάρεμα (vishing), όπου οι επιτιθέμενοι χρησιμοποιούν δόλιες τηλεφωνικές κλήσεις για να αποσπάσουν διοικητικά ή οικονομικά δεδομένα.

Q10: Πώς βοηθούν οι σαρωτές συνδέσμων;

Σαρώνουν και ξαναγράφουν τους εισερχόμενους συνδέσμους email για να επαληθεύουν την ασφάλεια των ιστοσελίδων προορισμού τη στιγμή του κλικ.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς λειτουργεί μια επίθεση ομογραφίας (homograph);

Οι επιτιθέμενοι καταχωρίζουν ονόματα τομέα με χαρακτήρες Unicode εκτός ASCII που μοιάζουν οπτικά, ώστε να μιμούνται ένα νόμιμο όνομα τομέα.

Q2: Τι είναι μια αναπαράσταση punycode;

Μια κωδικοποίηση που μετατρέπει ονόματα τομέα Unicode σε συμβατές με ASCII συμβολοσειρές που ξεκινούν με 'xn--', ώστε το DNS να μπορεί να τα χειριστεί.

Q3: Γιατί το 'p=reject' είναι η ασφαλέστερη κατάσταση DMARC;

Ζητά από τους διακομιστές παραλαβής να απορρίπτουν αλληλογραφία που αποτυγχάνει στο DMARC (ευθυγραμμισμένα SPF/DKIM) κατά τη συνεδρία SMTP, αποκλείοντας την άμεση πλαστογράφηση. [2]

Q4: Πώς παρακάμπτουν οι επιτιθέμενοι τους κανόνες SPF;

Εκμεταλλευόμενοι ονόματα τομέα που μοιάζουν (typosquatting) ή χρησιμοποιώντας παραβιασμένους λογαριασμούς σε νόμιμες υπηρεσίες email τρίτων.

Q5: Τι είναι η παραβίαση επαγγελματικού email (BEC);

Μια εταιρική απάτη όπου οι επιτιθέμενοι υφαρπάζουν ή μιμούνται επιχειρηματικούς λογαριασμούς email για να εγκρίνουν δόλιες πληρωμές.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Πώς σταματά ο έλεγχος ταυτότητας πολλαπλών παραγόντων το ηλεκτρονικό ψάρεμα (phishing);

Απαιτεί δευτερεύοντα διακριτικά (όπως κλειδιά υλικού) που δεν μπορούν να κλαπούν μόνο μέσω παραπλανητικών σελίδων προσγείωσης.

Q7: Τι είναι μια σελίδα προορισμού συλλογής διαπιστευτηρίων;

Μια πύλη σύνδεσης-μίμηση που σχεδιάστηκε για να υποκλέπτει σε πραγματικό χρόνο ονόματα χρήστη, κωδικούς πρόσβασης και διακριτικά MFA που πληκτρολογούνται.

Q8: Τι είναι η υφαρπαγή υποτομέα (subdomain hijacking);

Ένας επιτιθέμενος αναλαμβάνει τον έλεγχο ενός αχρησιμοποίητου δείκτη υποτομέα DNS για να φιλοξενήσει κακόβουλες σελίδες phishing κάτω από ένα αξιόπιστο γονικό domain.

Q9: Πώς λειτουργεί ο έλεγχος ευθυγράμμισης DKIM;

Επαληθεύει ότι ο τομέας στην κεφαλίδα «From» ταιριάζει με τον τομέα που υπέγραψε κρυπτογραφικά το μήνυμα στην κεφαλίδα DKIM.

Q10: Ποιος είναι ο ρόλος μιας πύλης email;

Φιλτράρισμα εισερχόμενων email, έλεγχος συνδέσμων, sandboxing συνημμένων και επικύρωση της συμμόρφωσης SPF/DKIM/DMARC.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το ηλεκτρονικό ψάρεμα και η πλαστοπροσωπία (phishing και spoofing) ήταν ο πιο συχνά αναφερόμενος τύπος εγκλήματος στο IC3 του FBI το 2025, με 191.561 καταγγελίες. [4]

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η παραβίαση επιχειρηματικού email (BEC) προκάλεσε απώλειες άνω των $3 δισεκατομμυρίων που αναφέρθηκαν στο IC3 του FBI το 2025. [4]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιθέσεις ομόγλυφων χρησιμοποιούν κυριλλικά γράμματα που μοιάζουν με λατινικά για να αντιγράψουν οπτικά ονόματα τομέα επωνυμιών με ακριβές ταίριασμα στα προγράμματα περιήγησης.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Με το «p=reject», ένα domain ζητά από τους παραλήπτες να απορρίπτουν τα μηνύματα που αποτυγχάνουν στον έλεγχο κατά την παράδοση, και όχι να τα καταχωρούν ως ανεπιθύμητα. [2]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιθέσεις whaling που στοχεύουν διευθύνοντες συμβούλους ζητούν συνήθως επείγουσες πληρωμές για εμπιστευτικές συγχωνεύσεις ή αγορές ονομάτων τομέα.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι πύλες συλλογής διαπιστευτηρίων αντιγράφουν πραγματικές σελίδες σύνδεσης, ώστε τα θύματα να πληκτρολογούν τους κωδικούς πρόσβασης απευθείας στη φόρμα του επιτιθέμενου.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι κοινές οδηγίες της CISA για το ηλεκτρονικό ψάρεμα συνιστούν εκπαίδευση των χρηστών παράλληλα με τα DMARC, SPF, DKIM και την MFA ανθεκτική στο ηλεκτρονικό ψάρεμα. [3]

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η αξιολόγηση SPF περιορίζεται σε 10 όρους που κάνουν ερωτήματα DNS· η υπέρβαση του ορίου επιστρέφει αποτέλεσμα 'permerror'. [1]

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα κλειδιά ασφαλείας υλικού FIDO2 παρέχουν κρυπτογραφικά θεμελιωμένη προστασία από την απομακρυσμένη συλλογή διαπιστευτηρίων.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το ηλεκτρονικό ψάρεμα είναι ένας από τους πιο συνηθισμένους τρόπους με τους οποίους οι επιτιθέμενοι αποκτούν αρχική πρόσβαση σε έναν οργανισμό, γι' αυτό η τακτική εκπαίδευση ευαισθητοποίησης είναι αποτελεσματική άμυνα.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι το spear phishing; → Ένα στοχευμένο email phishing προσαρμοσμένο σε ένα συγκεκριμένο άτομο ή οργανισμό

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το SPF δημοσιεύει στο DNS τους εξουσιοδοτημένους διακομιστές αποστολής ενός domain, ώστε οι παραλήπτες να ελέγχουν τον αποστολέα του φακέλου (envelope sender).

3 Ερώτηση 3

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι μια επίθεση whaling; → Μια εκστρατεία phishing που στοχεύει ειδικά εταιρικά στελέχη υψηλού προφίλ

4 Ερώτηση 4

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι κάνει το DKIM; → Προσθέτει κρυπτογραφική υπογραφή στα email για να επαληθεύεται η αυθεντικότητα του αποστολέα

5 Ερώτηση 5

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος είναι ο ρόλος του DMARC; → Οδηγίες προς τους διακομιστές email λήψης για το πώς να χειρίζονται αποτυχημένους ελέγχους SPF/DKIM

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το spear phishing προσαρμόζεται σε συγκεκριμένα άτομα, σε αντίθεση με το γενικό μαζικό ηλεκτρονικό ψάρεμα.

7 Ερώτηση 7

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι πολιτικές DMARC μπορούν να δώσουν εντολή στους διακομιστές αλληλογραφίας να απορρίπτουν μη εξουσιοδοτημένα πλαστά μηνύματα.

8 Ερώτηση 8

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το SPF ελέγχει την IP αποστολής έναντι του DNS· το DKIM είναι αυτό που επαληθεύει κρυπτογραφική υπογραφή.

9 Ερώτηση 9

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το whaling στοχεύει ανώτατα στελέχη, που μπορούν να εγκρίνουν πληρωμές και να έχουν πρόσβαση σε ευαίσθητα δεδομένα.

10 Ερώτηση 10

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: η επιβεβαίωση αιτημάτων πληρωμής μέσω ξεχωριστού, γνωστού καναλιού βοηθά στη διακοπή της απάτης με εμβάσματα.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

F 1. ΣΤΟΧΕΥΜΕΝΟ	G 2. ΠΛΑΣΤΟΓΡΑΦΗΣΗ	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	A 8. VISHING

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΣΤΟΧΕΥΜΕΝΟ	2 ΠΛΑΣΤΟΓΡΑΦΗΣΗ	3 SPF	4 DKIM
5 DMARC	6 ΦΑΛΑΙΝΟΘΗΡΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 Β – ΠΛΑΣΤΟΓΡΑΦΗΣΗ	2 Α – ΣΤΟΧΕΥΜΕΝΟ	3 Η – ΦΩΝΗΤΙΚΗΑΠΑΤΗ	4 C – ΕΓΓΡΑΦΗ
5 G – ΨΑΡΕΜΑ	6 Ε – ΠΟΛΙΤΙΚΗ	7 D – ΥΠΟΓΡΑΦΗ	8 F – ΦΑΛΑΙΝΟΘΗΡΑ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΣΤΟΧΕΥΜΕΝΟ, ΠΛΑΣΤΟΓΡΑΦΗΣΗ και SPF και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Η	Ψ	Η	Ξ	Ψ	Χ	Σ	Η	Τ	Χ	Α	Α	Ο	Υ	Ν
Τ	Ν	Φ	Ω	Ξ	Θ	Ο	Σ	Θ	Ο	Ρ	Υ	Τ	Ξ	Υ
Α	Τ	Α	Κ	Α	Ε	Ξ	Μ	Η	Λ	Η	Α	Ν	Υ	Ζ
Π	Η	Ρ	Ο	Π	Χ	Ψ	Κ	Ι	Κ	Θ	Υ	Ι	Ω	Φ
Α	Ψ	Γ	Ο	Κ	Θ	Ι	Ω	Ι	Ι	Ο	Ν	Α	Ε	Θ
Η	Α	Ο	Σ	Α	Τ	Ι	Ε	Φ	Ε	Ν	Κ	Η	Ω	Κ
Κ	Ε	Π	Κ	Ι	Π	Ν	Ι	Α	Ζ	Ι	Φ	Ξ	Κ	Ν
Ι	Γ	Υ	Λ	Ν	Γ	Δ	Η	Θ	Β	Α	Α	Ξ	Ρ	Λ
Τ	Ο	Ο	Φ	Τ	Θ	Ψ	Ζ	Ω	Ρ	Λ	Ρ	Η	Χ	Φ
Η	Π	Θ	Ε	Π	Τ	Ν	Τ	Γ	Κ	Α	Ρ	Δ	Τ	Σ
Ν	Π	Λ	Α	Σ	Τ	Ο	Γ	Ρ	Α	Φ	Η	Σ	Η	Λ
Ω	Ο	Λ	Ψ	Α	Ρ	Ε	Μ	Α	Μ	Σ	Θ	Κ	Ο	Θ
Φ	Ψ	Σ	Τ	Ο	Χ	Ε	Υ	Μ	Ε	Ν	Ο	Ξ	Λ	Χ
Υ	Ν	Ψ	Π	Π	Β	Α	Λ	Ο	Μ	Β	Λ	Θ	Ζ	Ι
Ν	Ψ	Β	Ω	Ω	Ψ	Β	Ν	Υ	Χ	Μ	Γ	Ε	Ξ	Χ

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

											Φ		Π	
											Ω		Ο	
											Ν		Λ	
			Ε								Η		Ι	
			Γ						Φ		Τ		Τ	
			Γ			Σ			Α		Ι		Ι	
Υ			Ρ			Τ			Λ		Κ		Κ	
Π	Λ	Α	Σ	Τ	Ο	Γ	Ρ	Α	Φ	Η	Σ		Η	
Ο		Φ			Χ			Ι		Α				
Γ		Η			Ε			Ν		Π				
Ρ					Υ			Ο		Α				
Α					Μ			Θ		Τ				
Φ					Ε			Η		Η				
Η					Ν			Ρ						
					Ο		Ψ	Α	Ρ	Ε	Μ	Α		

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

7 οριζόντια: ΠΛΑΣΤΟΓΡΑΦΗΣΗ Πλαστογράφηση της διεύθυνσης email του αποστολέα (13 γράμματα)

8 οριζόντια: ΨΑΡΕΜΑ Email κοινωνικής μηχανικής (6 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΦΩΝΗΤΙΚΗΑΠΑΤΗ Απατηλές τηλεφωνικές κλήσεις με φωνή (13 γράμματα)

2 κάθετα: ΠΟΛΙΤΙΚΗ Οδηγίες για το τι θα γίνεται με τα email που αποτυγχάνουν στον έλεγχο του αποστολέα, όπως η απόρριψη (8 γράμματα)

3 κάθετα: ΕΓΓΡΑΦΗ Εγγραφή DNS με τις εξουσιοδοτημένες IP αποστολέων (SPF) (7 γράμματα)

4 κάθετα: ΦΑΛΑΙΝΟΘΗΡΑ Στόχευση ανώτατων στελεχών (C-level) (11 γράμματα)

5 κάθετα: ΣΤΟΧΕΥΜΕΝΟ Εξατομικευμένο στοχευμένο email (10 γράμματα)

6 κάθετα: ΥΠΟΓΡΑΦΗ Κρυπτογραφικός κωδικός πιστοποίησης που επισυνάπτεται σε κάθε email (8 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΝΜΥΕΤΣΕΟΧΟ — **ΣΤΟΧΕΥΜΕΝΟ**
2. ΕΓΗΦΑΡΓ — **ΕΓΓΡΑΦΗ**
3. ΙΟΠΤΙΗΚΛ — **ΠΟΛΙΤΙΚΗ**
4. ΑΕΡΜΨΑ — **ΨΑΡΕΜΑ**
5. ΑΗΛΑΡΤΗΟΦΓΠΣΣ — **ΠΛΑΣΤΟΓΡΑΦΗΣΗ**
6. ΦΗΓΑΥΡΠΟ — **ΥΠΟΓΡΑΦΗ**
7. ΘΙΦΑΟΑΗΡΛΝΑ — **ΦΑΛΑΙΝΟΘΗΡΑ**
8. ΑΝΤΙΑΗΗΦΚΩΤΠΗ — **ΦΩΝΗΤΙΚΗΑΠΑΤΗ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΝΤΟΠΙΣΕ ΤΗΝ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ ΜΕ ΕΛΕΓΧΟΥΣ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Αποκατάσταση επίθεσης whaling σε ανώτατα στελέχη

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας Οικονομικός Διευθυντής λαμβάνει ένα εξαιρετικά εξατομικευμένο email που ισχυρίζεται ότι προέρχεται από τον Διευθύνοντα Σύμβουλο, ζητώντας άμεσο έμβασμα $50.000 για το κλείσιμο μιας εμπιστευτικής αγοράς ονόματος τομέα.
- Προτεινόμενη στρατηγική και λύση: Ρύθμισε το DMARC με πολιτική 'p=reject' για να αποκλείονται τα πλαστά domain αποστολέα. Πρόσθεσε banner προειδοποίησης εξωτερικού αποστολέα στην πύλη και απαίτησε προφορική επιβεβαίωση εκτός ζώνης (out-of-band) για όλες τις οικονομικές συναλλαγές.

B Μελέτη περίπτωσης 2: Εφαρμογή πολιτικών πύλης SPF/DKIM/DMARC

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια επιχείρηση αποτυγχάνει σε ελέγχους ασφαλείας επειδή τα εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου μάρκετινγκ επισημαίνονται συχνά ως ανεπιθύμητα και οι χάκερ πλαστογραφούν ενεργά το όνομα τομέα της μάρκας της εταιρείας.
- Προτεινόμενη στρατηγική και λύση: Δημοσίευσε μια εγγραφή TXT για το SPF με τις εξουσιοδοτημένες IP αποστολέων. Ρύθμισε κλειδιά υπογραφής DKIM στους εξερχόμενους διακομιστές αλληλογραφίας και ανάλυσε τις εισερχόμενες αναφορές ανάδρασης DMARC XML για να εντοπίσεις κατάχρηση.