Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Πρόληψη κλοπής ταυτότητας και περιουσιακά στοιχεία Οδηγός ασφαλείας

Διαρροές διαπιστευτηρίων, MFA, παρακολούθηση του dark web, ειδοποιήσεις παγώματος πίστωσης, κοινωνική μηχανική

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΓΙΑ ΤΗΝ ΠΡΟΛΗΨΗ ΚΛΟΠΗΣ ΤΑΥΤΟΤΗΤΑΣ

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 στην πρόληψη και τον περιορισμό της κλοπής ταυτότητας. Θα εξερευνήσεις διαρροές διαπιστευτηρίων, ταυτοποίηση πολλαπλών παραγόντων, παρακολούθηση του dark web, ειδοποιήσεις παγώματος πίστωσης και άμυνα απέναντι στην κοινωνική μηχανική.

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/klopi-tautotitas/

Η πορεία μάθησής σου: προστασία ταυτότητας

- Κατανόησε τους κινδύνους έκθεσης διαπιστευτηρίων σε φόρουμ του dark web.
- Εφάρμοσε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) και ειδοποιήσεις παγώματος πιστωτικού ιστορικού.
- Σχεδίασε εταιρικές άμυνες ασφάλειας απέναντι σε στοχευμένες απάτες κοινωνικής μηχανικής.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΚΛΟΠΗΣ ΤΑΥΤΟΤΗΤΑΣ

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 προστασία ταυτότητας. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΠΡΟΛΗΨΗ ΚΛΟΠΗΣ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ (ΕΙΣΑΓΩΓΗ)

Η κλοπή ταυτότητας εκμεταλλεύεται διαρρεύσαντα διαπιστευτήρια και αδύναμες συνδέσεις για να αποκτήσει τον έλεγχο προσωπικών και εταιρικών λογαριασμών. Η εφαρμογή MFA, πάγωμα πιστωτικού ιστορικού, σαρωτές dark web και πλαίσια SPF/DKIM/DMARC αποτελεί κρίσιμη άμυνα απέναντι στην ψηφιακή πλαστοπροσωπία.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποια είναι η κύρια μέθοδος που χρησιμοποιούν οι κλέφτες ταυτότητας για να υποκλέψουν διαπιστευτήρια σύνδεσης;**
   - A. Αποστολή ψεύτικων ειδοποιήσεων email που εξαπατούν τους χρήστες ώστε να εισαγάγουν κωδικούς πρόσβασης σε πλαστές πύλες
   - B. Ακρόαση ραδιοφωνικών εκπομπών κοντά στα εταιρικά γραφεία ενός χρήστη
   - C. Εκτέλεση ανασυγκρότησης στον τοπικό δίσκο αποθήκευσης διακομιστή ενός χρήστη
   - D. Αποσύνδεση εξωτερικών ρυθμίσεων αντιγράφων ασφαλείας δικτύου

2. **Ποιος έλεγχος ασφάλειας παρέχει την ισχυρότερη άμυνα απέναντι σε διαρροές διαπιστευτηρίων;**
   - A. Έλεγχος ταυτότητας πολλαπλών παραγόντων με κλειδιά υλικού
   - B. Δημιουργία μακριών κωδικών πρόσβασης με προεπιλεγμένες μορφές του προγράμματος περιήγησης
   - C. Αλλαγή ονομάτων χρήστη email κάθε έξι μήνες
   - D. Διαγραφή αποθηκευμένων ιστορικών περιήγησης με cookies παρακολούθησης

3. **Τι αντιπροσωπεύει το πάγωμα πίστωσης (credit freeze);**
   - A. Κλείδωμα των πιστωτικών αναφορών ώστε οι απατεώνες να μην ανοίγουν μη εξουσιοδοτημένα δάνεια
   - B. Διαγραφή ιστορικού συναλλαγών τραπεζικών λογαριασμών από βάσεις δεδομένων
   - C. Απενεργοποίηση μαγνητικών αναγνωστών πιστωτικών καρτών σε σαρωτές
   - D. Κρυπτογράφηση τοπικών σκληρών δίσκων βάσεων δεδομένων σε κατάσταση ηρεμίας

4. **Γιατί είναι χρήσιμη η παρακολούθηση του dark web;**
   - A. Ειδοποιεί τους χρήστες αν τα διαρρεύσαντα διαπιστευτήριά τους εμφανιστούν σε παράνομες βάσεις δεδομένων
   - B. Εμποδίζει την εκτέλεση ενεργού κακόβουλου λογισμικού σε εικονικά sandbox
   - C. Επιταχύνει τη δρομολόγηση του προγράμματος περιήγησης σε εικονικά δίκτυα
   - D. Αποκλείει απόπειρες πρόσβασης SQL injection στη βάση δεδομένων του παρασκηνίου

5. **Τι σημαίνει κοινωνική μηχανική;**
   - A. Χειραγώγηση ατόμων ώστε να αποκαλύψουν οικειοθελώς εμπιστευτικά διαπιστευτήρια
   - B. Σάρωση θυρών εταιρικών διακομιστών για ενεργές εκμεταλλεύσεις ασφαλείας
   - C. Δημιουργία αντιγράφων ασφαλείας των αρχείων βάσεων δεδομένων συστήματος σε σκληρούς δίσκους εκτός σύνδεσης
   - D. Δρομολόγηση πακέτων δικτύου μέσω τριών κρυπτογραφημένων κόμβων onion

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Η κλοπή ταυτότητας επηρεάζει μόνο ψηφιακούς λογαριασμούς στο διαδίκτυο και όχι την ταχυδρομική αλληλογραφία.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Η επιβολή MFA σε όλους τους προσωπικούς λογαριασμούς αποκλείει τις περισσότερες επιθέσεις bot credential stuffing.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Το πάγωμα πίστωσης αποκλείει τους ελέγχους πίστωσης αλλά σε εμποδίζει να έχεις πρόσβαση στον δικό σου τραπεζικό λογαριασμό.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Οι διαχειριστές κωδικών προστατεύουν τους χρήστες από το ηλεκτρονικό ψάρεμα, αρνούμενοι να συμπληρώσουν αυτόματα κωδικούς σε πλαστά ονόματα τομέα.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Τα email ηλεκτρονικού ψαρέματος χρησιμοποιούν συχνά επείγουσα γλώσσα για να προκαλέσουν συναισθηματικές, γρήγορες αντιδράσεις.

○ 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. Οι κλέφτες ταυτότητας στοχεύουν προσωπικούς κωδικούς πρόσβασης και τα _____ των χρηστών.

2. Η ειδοποίηση των χρηστών για παραβιάσεις βάσεων δεδομένων εντοπίζει ιδιωτικές _____ λογαριασμών.

3. Η απαίτηση προσωρινού κωδικού για σύνδεση ονομάζεται πολυπαραγοντική ταυτοποίηση, δηλαδή _____ .

4. Η σάρωση φόρουμ χάκερ για κλεμμένα δεδομένα είναι η _____ του dark web.

5. Ο αποκλεισμός μη εξουσιοδοτημένων ελέγχων πιστοληπτικής ικανότητας απαιτεί ένα _____ του πιστωτικού φακέλου.

6. Η εκπαίδευση των υπαλλήλων στην ενημέρωση για το ηλεκτρονικό ψάρεμα χτίζει μια ενεργή _____ ασφαλείας.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΜΥΝΑ ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ ΔΙΑΡΡΟΕΣ ΠΑΓΩΜΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΠΛΑΣΤΟΓΡΑΦΗΣΗ ΨΑΡΕΜΑ MFA

Γράψε τις απαντήσεις σου εδώ:

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

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

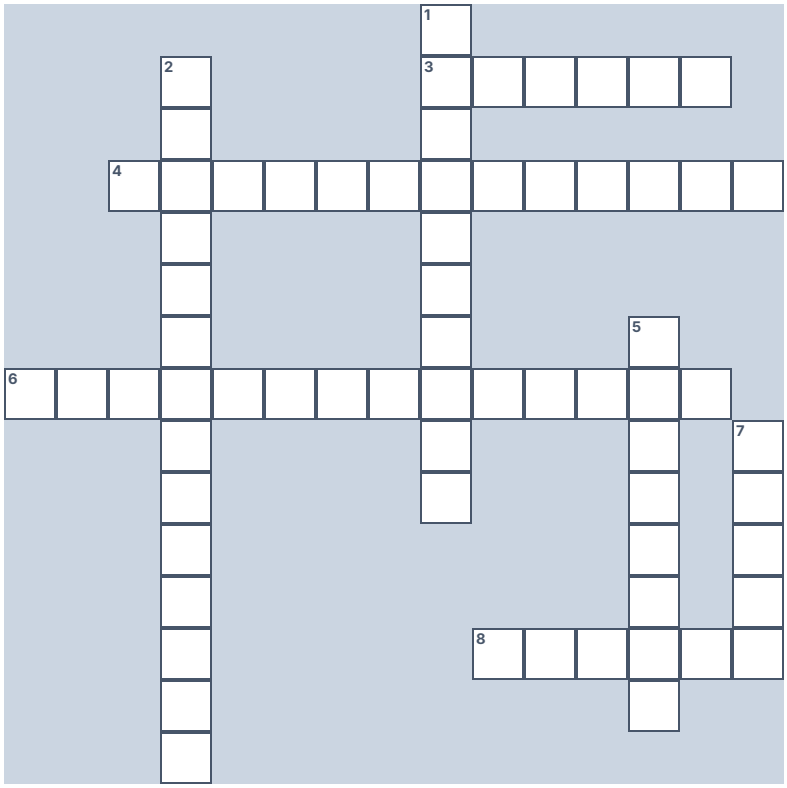
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ	**A**	Δευτερεύον βήμα επαλήθευσης (όπως κλειδιά υλικού) που προστατεύει τις συνδέσεις σε λογαριασμούς.
☐	2. ΔΙΑΡΡΟΕΣ	**B**	Δημιουργία πλαστού ιστότοπου ή email που μιμείται έναν νόμιμο οργανισμό.
☐	3. MFA	**C**	Περιορισμός της πρόσβασης στους πιστωτικούς φακέλους για την αποτροπή δόλιων αιτήσεων δανείου.
☐	4. ΠΑΡΑΚΟΛΟΥΘΗΣΗ	**D**	Μη εξουσιοδοτημένη έκθεση ιδιωτικών βάσεων δεδομένων που περιέχουν προσωπικές εγγραφές χρηστών.
☐	5. ΠΑΓΩΜΑ	**E**	Εκπαίδευση και τεχνικοί έλεγχοι που χρησιμοποιούνται για την προστασία από κλοπή ταυτότητας.
☐	6. ΑΜΥΝΑ	**F**	Αποστολή δόλιων μηνυμάτων για να εξαπατηθούν οι χρήστες ώστε να αποκαλύψουν διαπιστευτήρια.
☐	7. ΠΛΑΣΤΟΓΡΑΦΗΣΗ	**G**	Σάρωση διαδικτυακών φόρουμ και καναλιών χάκερ για κλεμμένα εταιρικά δεδομένα.
☐	8. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	**H**	Ονόματα χρήστη, κωδικοί πρόσβασης και ιδιωτικά διακριτικά που χρησιμοποιούνται για την πιστοποίηση ψηφιακών ταυτοτήτων.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

3. Περιορισμός της πρόσβασης στους πιστωτικούς φακέλους για την αποτροπή δόλιων αιτήσεων δανείου. (6)

4. Σάρωση διαδικτυακών φόρουμ και καναλιών χάκερ για κλεμμένα εταιρικά δεδομένα. (13)

6. Ονόματα χρήστη, κωδικοί πρόσβασης και ιδιωτικά διακριτικά που χρησιμοποιούνται για την ταυτοποίηση ψηφιακών ταυτοτήτων. (14)

8. Αποστολή δόλιων μηνυμάτων για να ξεγελαστούν οι χρήστες και να αποκαλύψουν διαπιστευτήρια. (6)

ΚΑΘΕΤΑ

1. Δευτερεύον βήμα επαλήθευσης (όπως τα φυσικά κλειδιά) που προστατεύει τις συνδέσεις σε λογαριασμούς. (10)

2. Δημιουργία ψεύτικου ιστότοπου ή email που μιμείται έναν νόμιμο οργανισμό. (14)

5. Μη εξουσιοδοτημένη έκθεση ιδιωτικών βάσεων δεδομένων που περιέχουν προσωπικά στοιχεία χρηστών. (8)

7. Εκπαίδευση και τεχνικοί έλεγχοι που χρησιμοποιούνται για προστασία από την κλοπή ταυτότητας. (5)

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

3 οριζόντια: Περιορισμός της πρόσβασης στους πιστωτικούς φακέλους για την αποτροπή δόλιων αιτήσεων δανείου. (6 γράμματα):

4 οριζόντια: Σάρωση διαδικτυακών φόρουμ και καναλιών χάκερ για κλεμμένα εταιρικά δεδομένα. (13 γράμματα):

6 οριζόντια: Ονόματα χρήστη, κωδικοί πρόσβασης και ιδιωτικά διακριτικά που χρησιμοποιούνται για την ταυτοποίηση ψηφιακών ταυτοτήτων. (14 γράμματα):

8 οριζόντια: Αποστολή δόλιων μηνυμάτων για να ξεγελαστούν οι χρήστες και να αποκαλύψουν διαπιστευτήρια. (6 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Δευτερεύον βήμα επαλήθευσης (όπως τα φυσικά κλειδιά) που προστατεύει τις συνδέσεις σε λογαριασμούς. (10 γράμματα):

2 κάθετα: Δημιουργία ψεύτικου ιστότοπου ή email που μιμείται έναν νόμιμο οργανισμό. (14 γράμματα):

5 κάθετα: Μη εξουσιοδοτημένη έκθεση ιδιωτικών βάσεων δεδομένων που περιέχουν προσωπικά στοιχεία χρηστών. (8 γράμματα):

7 κάθετα: Εκπαίδευση και τεχνικοί έλεγχοι που χρησιμοποιούνται για προστασία από την κλοπή ταυτότητας. (5 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.

Π Λ Α Σ Τ Ο Π Ρ Ο Σ Ω Π Ι Α Γ

Μ Ω Η Σ Υ Ε Θ Η Λ Α Π Ε Ψ Ζ Π

Ψ Ξ Φ Υ Λ Υ Ο Β Ν Φ Τ Μ Η Α Υ

Γ Ψ Υ Κ Ρ Α Χ Ω Ψ Μ Ρ Π Γ Χ Θ

Ξ Δ Α Γ Κ Π Φ Χ Χ Λ Ι Ω Θ Τ Θ

Ζ Β Ε Θ Κ Σ Ρ Φ Π Ω Μ Ε Θ Ε Ρ

Γ Α Λ Ο Γ Ω Μ Κ Φ Α Ρ Υ Α Ρ Χ

Κ Μ Μ Η Θ Ν Θ Π Ζ Α Ν Υ Μ Α Λ

Σ Λ Ρ Χ Θ Β Τ Ζ Ψ Ξ Ψ Χ Σ Η Τ

Α Χ Α Ο Σ Ε Ο Ρ Ρ Α Ι Δ Υ Ν Ν

Μ Δ Ι Α Π Ι Σ Τ Ε Υ Τ Η Ρ Ι Α

Ε Ω Ξ Θ Ο Σ Θ Ο Υ Τ Ξ Υ Τ Κ Α

Ρ Ε Π Α Ρ Α Κ Ο Λ Ο Υ Θ Η Σ Η

Α Ξ Μ Λ Α Ν Υ Ζ Η Ο Π Χ Ψ Ι Κ

Ψ Υ Ι Ω Φ Ψ Ο Κ Θ Ω Ι Ι Ν Α Ε

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ
ΔΙΑΡΡΟΕΣ
ΑΜΥΝΑ
ΕΠΑΛΗΘΕΥΣΗ
ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ
ΠΑΡΑΚΟΛΟΥΘΗΣΗ
ΨΑΡΕΜΑ
ΠΑΓΩΜΑ

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. ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ

B. ΔΙΑΡΡΟΕΣ

C. ΕΠΑΛΗΘΕΥΣΗ

D. ΠΑΡΑΚΟΛΟΥΘΗΣΗ

E. ΠΑΓΩΜΑ

F. ΑΜΥΝΑ

G. ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ

H. ΨΑΡΕΜΑ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Αποστολή δόλιων μηνυμάτων για να ξεγελαστούν οι χρήστες και να αποκαλύψουν διαπιστευτήρια.

_____ 2. Ονόματα χρήστη, κωδικοί πρόσβασης και ιδιωτικά διακριτικά που χρησιμοποιούνται για την ταυτοποίηση ψηφιακών ταυτοτήτων.

_____ 3. Δημιουργία ψεύτικου ιστότοπου ή email που μιμείται έναν νόμιμο οργανισμό.

_____ 4. Εκπαίδευση και τεχνικοί έλεγχοι που χρησιμοποιούνται για προστασία από την κλοπή ταυτότητας.

_____ 5. Σάρωση διαδικτυακών φόρουμ και καναλιών χάκερ για κλεμμένα εταιρικά δεδομένα.

_____ 6. Περιορισμός της πρόσβασης στους πιστωτικούς φακέλους για την αποτροπή δόλιων αιτήσεων δανείου.

_____ 7. Μη εξουσιοδοτημένη έκθεση ιδιωτικών βάσεων δεδομένων που περιέχουν προσωπικά στοιχεία χρηστών.

_____ 8. Δευτερεύον βήμα επαλήθευσης (όπως τα φυσικά κλειδιά) που προστατεύει τις συνδέσεις σε λογαριασμούς.

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. **ΗΣΕΤΤΑΙΥΡΔΙΑΙΠ**
2. **ΣΛΕΠΗΗΕΥΘΑ**
3. **ΠΓΩΑΜΑ**
4. **ΛΠΙΣΣΟΟΑΡΠΩΠΑΤ**
5. **ΡΟΙΣΡΔΕΑ**
6. **ΚΘΛΟΗΡΣΥΠΑΟΗΑ**
7. **ΝΑΑΥΜ**
8. **ΡΑΨΜΕΑ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πράγματα που κάνεις αν κλαπεί η ταυτότητά σου			
2	Πράγματα που δεν μοιράζεσαι στα μέσα κοινωνικής δικτύωσης			
3	Πράγματα που παίρνεις αντίγραφο ασφαλείας			
4	Κάρτες ή ταυτότητες στο πορτοφόλι σου			
5	Έγγραφα που πρέπει να προστατεύεις			
6	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			
7	Λόγοι για να ενημερώνεις το λογισμικό			
8	Πληροφορίες που θέλει ένας κλέφτης ταυτότητας			
9	Συσκευές που μπορούν να παραβιαστούν			
10	Μέρη από όπου μπορούν να διαρρεύσουν τα δεδομένα σου			
11	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
12	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
13	Τρόποι να αποδείξεις ποιος είσαι			
14	Ενδείξεις κλοπής ταυτότητας			
15	Προειδοποιητικά σημάδια σε ένα email			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ ΑΝΩΤΑΤΩΝ ΣΤΕΛΕΧΩΝ



Σενάριο: Ένα υψηλόβαθμο στέλεχος C-suite έχει γίνει στόχος ονομάτων τομέα με ορθογραφικά λάθη (typosquatting) που μιμούνται το προσωπικό του email για να εξαπατήσουν πελάτες. Σχεδίασε ένα σχέδιο προστασίας brand.

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΕΚΘΕΣΗ ΕΤΑΙΡΙΚΩΝ ΔΙΑΠΙΣΤΕΥΤΗΡΙΩΝ ΣΤΟ DARK WEB



Σενάριο: Ένα dump βάσης δεδομένων του dark web περιέχει αρκετές εκατοντάδες εταιρικά διαπιστευτήρια διαχειριστών συστημάτων μιας επιχείρησης. Σχεδίασε μια στρατηγική μετριασμού.

Ερώτηση συζήτησης: Περίγραψε συνοπτικά τη διαδικασία εκκαθάρισης διαπιστευτηρίων και σχεδίασε την ανάπτυξη ενός διαχειριστή κωδικών πρόσβασης.

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

16	17	15	18	19	1	19	5	23	5		19	7	13

23	7	21	9	1	10	7		19	1	20	19	15	19	7	19	1		12	5

16	15	11	11	1		2	7	12	1	19	1

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 η κλοπή ταυτότητας;

Ένα έγκλημα όπου ο επιτιθέμενος κλέβει προσωπικά στοιχεία (όπως κωδικούς πρόσβασης ή AMKA/SSN) για να υποδυθεί κάποιον άλλον με σκοπό το οικονομικό όφελος.

Q2: Ποια είναι η πιο συνηθισμένη αιτία κλοπής ταυτότητας;

Το ηλεκτρονικό ψάρεμα είναι ένας από τους κύριους τρόπους με τους οποίους οι δράστες αποκτούν κωδικούς πρόσβασης, παρασύροντας τους χρήστες σε ψεύτικους, πλαστούς ιστότοπους.

Q3: Πώς προστατεύει την ταυτότητα ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA);

Το MFA απαιτεί δεύτερη απόδειξη ταυτότητας (όπως ένα κλειδί υλικού) για τη σύνδεση, αποκλείοντας τους επιτιθέμενους ακόμη κι αν κλέψουν τον κωδικό πρόσβασής σου.

Q4: Τι είναι το πάγωμα πίστωσης (credit freeze);

Μια δωρεάν υπηρεσία που εμποδίζει τα πιστωτικά γραφεία να μοιράζονται τον πιστωτικό σου φάκελο, αποτρέποντας τους απατεώνες από το να ανοίξουν νέα δάνεια στο όνομά σου. [2]

Q5: Τι είναι η παρακολούθηση του dark web;

Λογισμικό που ελέγχει φόρουμ χάκερ για διαρρεύσαντα email, κωδικούς πρόσβασης και προσωπικά αρχεία και σε ειδοποιεί αν τα δεδομένα σου έχουν εκτεθεί.

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 σημαίνει credential stuffing;

Αυτοματοποιημένα bots που δοκιμάζουν λίστες διαρρεύσαντων κωδικών πρόσβασης σε εκατοντάδες ιστότοπους για να αναλάβουν ενεργούς λογαριασμούς.

Q7: Γιατί είναι επικίνδυνη η πλαστογράφηση email;

Επιτρέπει στους επιτιθέμενους να πλαστογραφούν το όνομα του αποστολέα στα email, κάνοντας τα μηνύματα ηλεκτρονικού ψαρέματος να μοιάζουν ότι προέρχονται από έμπιστους συναδέλφους.

Q8: Πώς σταματούν οι διαχειριστές κωδικών πρόσβασης την κλοπή ταυτότητας;

Αποθηκεύουν σύνθετους, μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό και αρνούνται να συμπληρώσουν αυτόματα διαπιστευτήρια σε ψεύτικους τομείς ηλεκτρονικού ψαρέματος.

Q9: Τι είναι το spear phishing;

Μια εξαιρετικά στοχευμένη επίθεση phishing προσαρμοσμένη με το όνομα και τα στοιχεία του θύματος για να αυξηθεί η πιθανότητα εξαπάτησης.

Q10: Σε τι διαφέρει μια ειδοποίηση πίστωσης από ένα πάγωμα;

Μια ειδοποίηση ζητά από τους δανειστές να επαληθεύσουν την ταυτότητά σου πριν ανοίξουν λογαριασμούς, ενώ το πάγωμα αποκλείει εντελώς την πρόσβαση στον πιστωτικό σου φάκελο. [2]

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 οδηγεί το SIM swapping στην κλοπή ταυτότητας;

Οι επιτιθέμενοι πείθουν το προσωπικό του παρόχου να μεταφέρει τον αριθμό τηλεφώνου του θύματος σε νέα κάρτα SIM, υφαρπάζοντας κωδικούς 2FA που αποστέλλονται με SMS.

Q2: Ποιος είναι ο ρόλος του DMARC στην πρόληψη της κλοπής ταυτότητας;

Το DMARC επιτρέπει στους κατόχους ονομάτων τομέα να εμποδίζουν τα πλαστά email να φτάνουν στα εισερχόμενα, σταματώντας τα ψεύτικα email που μιμούνται εταιρικά ονόματα τομέα.

Q3: Γιατί είναι δύσκολο να εντοπιστεί η κλοπή συνθετικής ταυτότητας;

Οι κλέφτες συνδυάζουν πραγματικούς αριθμούς SSN με ψεύτικα ονόματα και ημερομηνίες γέννησης για να δημιουργήσουν εντελώς νέα πιστωτικά προφίλ, παρακάμπτοντας τις βασικές ειδοποιήσεις απάτης.

Q4: Πώς εκμεταλλεύονται οι μεσίτες δεδομένων τις προσωπικές ταυτότητες;

Οι μεσίτες συλλέγουν δημόσια αρχεία, συμπεριφορά στον ιστό και ιστορικό αγορών για να συντάξουν φακέλους προφίλ, οι οποίοι μπορεί να διαρρεύσουν ή να πουληθούν.

Q5: Γιατί το MFA μέσω SMS θεωρείται ευάλωτο;

Η κίνηση SMS είναι ευάλωτη σε υποκλοπή, ηλεκτρονικό ψάρεμα και εκμεταλλεύσεις SIM-swapping σε επίπεδο παρόχου.

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: Τι είναι το κλείδωμα αρχείου πίστωσης;

Μια εμπορική υπηρεσία παρόμοια με το πάγωμα, που επιτρέπει στους χρήστες να ξεκλειδώνουν ή να κλειδώνουν αμέσως τον πιστωτικό τους φάκελο μέσω εφαρμογής κινητού.

Q7: Πώς τροφοδοτούν οι εταιρικές παραβιάσεις δεδομένων την κλοπή ταυτότητας;

Οι βάσεις δεδομένων που έχουν διαρρεύσει εκθέτουν εκατομμύρια διαπιστευτήρια σε απλό κείμενο και δίνουν στους κλέφτες τα ακατέργαστα δεδομένα που χρειάζονται για στοχευμένη απάτη ταυτότητας.

Q8: Ποιος είναι ο κίνδυνος της υπερβολικής κοινοποίησης στα μέσα κοινωνικής δικτύωσης;

Η δημόσια κοινοποίηση ονομάτων κατοικίδιων, τόπων γέννησης και πατρικών επωνύμων της μητέρας δίνει στους δράστες τις απαντήσεις σε συνηθισμένες ερωτήσεις ανάκτησης λογαριασμού.

Q9: Πώς προστατεύουν τα προφίλ ταυτότητας οι βιομετρικές συνδέσεις;

Τα βιομετρικά στοιχεία συνδέουν τις συνδέσεις με χαρακτηριστικά όπως δακτυλικά αποτυπώματα ή πρόσωπα· όταν παραμένουν στη συσκευή είναι δύσκολο να κλαπούν, αλλά τα αποθηκευμένα βιομετρικά δεδομένα μπορεί να διαρρεύσουν.

Q10: Πώς καταπολεμά ο κανόνας Red Flags Rule την κλοπή ταυτότητας;

Ένας ομοσπονδιακός κανονισμός που απαιτεί από τα χρηματοπιστωτικά ιδρύματα να αναπτύσσουν γραπτά προγράμματα για τον εντοπισμό και την αντιμετώπιση προειδοποιητικών σημείων κλοπής ταυτότητας.

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 IdentityTheft.gov, που διαχειρίζεται η FTC, επιτρέπει στα θύματα στις ΗΠΑ να αναφέρουν κλοπή ταυτότητας και να λάβουν ένα προσωπικό σχέδιο ανάκαμψης. [1]

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα κλειδιά ασφαλείας υλικού είναι MFA ανθεκτικό στο ηλεκτρονικό ψάρεμα (phishing), το ισχυρότερο είδος MFA που προτείνει έντονα η CISA. [4]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι παραβιασμένοι κωδικοί πρόσβασης είναι ένα συχνό σημείο εισόδου στις παραβιάσεις δεδομένων και τροφοδοτούν μεταγενέστερες απάτες ταυτότητας.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το πάγωμα πίστωσης είναι δωρεάν βάσει ομοσπονδιακού νόμου και εμποδίζει τους δανειστές να ελέγχουν τους πιστωτικούς φακέλους μέχρι να ξεκλειδωθεί. [2]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το DMARC επιτρέπει στους κατόχους ονομάτων τομέα να λένε στους διακομιστές αλληλογραφίας να απορρίπτουν ή να θέτουν σε καραντίνα τα πλαστά email που αποτυγχάνουν στους ελέγχους. [7]

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το SIM swapping επιτρέπει στους χάκερ να παρακάμπτουν τον έλεγχο ταυτότητας δύο παραγόντων μέσω SMS στις τραπεζικές πύλες.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η απάτη συνθετικής ταυτότητας αναμειγνύει πραγματικά και ψεύτικα στοιχεία, κάνοντας δύσκολο για τους δανειστές να την εντοπίσουν.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Πολλοί άνθρωποι επαναχρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε διαδικτυακούς λογαριασμούς, οπότε μία παραβίαση μπορεί να εκθέσει αρκετούς από αυτούς.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι μεσίτες δεδομένων συγκεντρώνουν λεπτομερείς φακέλους για μεγάλο αριθμό καταναλωτών, δημιουργώντας συγκεντρωμένο κίνδυνο για το απόρρητο.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η ανάκαμψη από κλοπή ταυτότητας μπορεί να απαιτήσει μήνες εργασίας, όπως η αμφισβήτηση χρεώσεων και η διόρθωση των πιστωτικών αναφορών.

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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

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

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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποια είναι η κύρια μέθοδος που χρησιμοποιούν οι κλέφτες ταυτότητας για να υποκλέψουν διαπιστευτήρια σύνδεσης; → Αποστολή ψεύτικων ειδοποιήσεων email που εξαπατούν τους χρήστες ώστε να εισαγάγουν κωδικούς πρόσβασης σε πλαστές πύλες

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος έλεγχος ασφάλειας παρέχει την ισχυρότερη άμυνα απέναντι σε διαρροές διαπιστευτηρίων; → Έλεγχος ταυτότητας πολλαπλών παραγόντων με κλειδιά υλικού

3 Ερώτηση 3

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι αντιπροσωπεύει το πάγωμα πίστωσης (credit freeze); → Κλείδωμα των πιστωτικών αναφορών ώστε οι απατεώνες να μην ανοίγουν μη εξουσιοδοτημένα δάνεια

4 Ερώτηση 4

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Γιατί είναι χρήσιμη η παρακολούθηση του dark web; → Ειδοποιεί τους χρήστες αν τα διαρρεύσαντα διαπιστευτήριά τους εμφανιστούν σε παράνομες βάσεις δεδομένων

5 Ερώτηση 5

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι σημαίνει κοινωνική μηχανική; → Χειραγώγηση ατόμων ώστε να αποκαλύψουν οικειοθελώς εμπιστευτικά διαπιστευτήρια

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η κλοπή ταυτότητας μπορεί να ξεκινήσει και εκτός διαδικτύου, για παράδειγμα με κλεμμένη αλληλογραφία ή έγγραφα.

7 Ερώτηση 7

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η επιβολή MFA σε όλους τους προσωπικούς λογαριασμούς αποκλείει τις περισσότερες επιθέσεις bot credential stuffing.

8 Ερώτηση 8

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το πάγωμα πίστωσης σταματά νέους ελέγχους πίστωσης αλλά δεν επηρεάζει τους υπάρχοντες λογαριασμούς σου.

9 Ερώτηση 9

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διαχειριστές κωδικών προστατεύουν τους χρήστες από το ηλεκτρονικό ψάρεμα, αρνούμενοι να συμπληρώσουν αυτόματα κωδικούς σε πλαστά ονόματα τομέα.

10 Ερώτηση 10

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα email ηλεκτρονικού ψαρέματος χρησιμοποιούν συχνά επείγουσα γλώσσα για να προκαλέσουν συναισθηματικές, γρήγορες αντιδράσεις.

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

H 1. ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ	D 2. ΔΙΑΡΡΟΕΣ	A 3. MFA	G 4. ΠΑΡΑΚΟΛΟΥΘΗΣΗ
C 5. ΠΑΓΩΜΑ	E 6. ΑΜΥΝΑ	B 7. ΠΛΑΣΤΟΓΡΑΦΗΣΗ	F 8. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ	2 ΔΙΑΡΡΟΕΣ	3 MFA	4 ΠΑΡΑΚΟΛΟΥΘΗΣΗ
5 ΠΑΓΩΜΑ	6 ΑΜΥΝΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 H – ΨΑΡΕΜΑ	2 A – ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ	3 G – ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ	4 F – ΑΜΥΝΑ
5 D – ΠΑΡΑΚΟΛΟΥΘΗΣΗ	6 E – ΠΑΓΩΜΑ	7 B – ΔΙΑΡΡΟΕΣ	8 C – ΕΠΑΛΗΘΕΥΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ, ΔΙΑΡΡΟΕΣ και MFA 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

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: ΠΑΓΩΜΑ Περιορισμός της πρόσβασης στους πιστωτικούς φακέλους για την αποτροπή δόλιων αιτήσεων δανείου. (6 γράμματα)

4 οριζόντια: ΠΑΡΑΚΟΛΟΥΘΗΣΗ Σάρωση διαδικτυακών φόρουμ και καναλιών χάκερ για κλεμμένα εταιρικά δεδομένα. (13 γράμματα)

6 οριζόντια: ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ Ονόματα χρήστη, κωδικοί πρόσβασης και ιδιωτικά διακριτικά που χρησιμοποιούνται για την ταυτοποίηση ψηφιακών ταυτοτήτων. (14 γράμματα)

8 οριζόντια: ΨΑΡΕΜΑ Αποστολή δόλιων μηνυμάτων για να ξεγελαστούν οι χρήστες και να αποκαλύψουν διαπιστευτήρια. (6 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΕΠΑΛΗΘΕΥΣΗ Δευτερεύον βήμα επαλήθευσης (όπως τα φυσικά κλειδιά) που προστατεύει τις συνδέσεις σε λογαριασμούς. (10 γράμματα)

2 κάθετα: ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ Δημιουργία ψεύτικου ιστότοπου ή email που μιμείται έναν νόμιμο οργανισμό. (14 γράμματα)

5 κάθετα: ΔΙΑΡΡΟΕΣ Μη εξουσιοδοτημένη έκθεση ιδιωτικών βάσεων δεδομένων που περιέχουν προσωπικά στοιχεία χρηστών. (8 γράμματα)

7 κάθετα: ΑΜΥΝΑ Εκπαίδευση και τεχνικοί έλεγχοι που χρησιμοποιούνται για προστασία από την κλοπή ταυτότητας. (5 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΗΣΕΤΤΑΙΥΡΔΙΑΙΠ — **ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ**
2. ΣΛΕΠΗΗΕΥΘΑ — **ΕΠΑΛΗΘΕΥΣΗ**
3. ΠΓΩΑΜΑ — **ΠΑΓΩΜΑ**
4. ΛΠΙΣΣΟΟΑΡΠΩΠΑΤ — **ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ**
5. ΡΟΙΣΡΔΕΑ — **ΔΙΑΡΡΟΕΣ**
6. ΚΘΛΟΗΡΣΥΠΑΟΗΑ — **ΠΑΡΑΚΟΛΟΥΘΗΣΗ**
7. ΝΑΑΥΜ — **ΑΜΥΝΑ**
8. ΡΑΨΜΕΑ — **ΨΑΡΕΜΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΠΡΟΣΤΑΤΕΨΕ ΤΗΝ ΨΗΦΙΑΚΗ ΤΑΥΤΟΤΗΤΑ ΜΕ ΠΟΛΛΑ ΒΗΜΑΤΑ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Προστασία από πλαστοπροσωπία ανώτατων στελεχών

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα υψηλόβαθμο στέλεχος της ανώτατης διοίκησης έχει γίνει στόχος ονομάτων τομέα με τυπογραφικά λάθη που μιμούνται το προσωπικό του email για να εξαπατηθούν πελάτες. Σχεδίασε ένα σχέδιο προστασίας επωνυμίας.
- Προτεινόμενη στρατηγική και λύση: Καταχώρισε όλες τις συνηθισμένες ορθογραφικές παραλλαγές του ονόματος του στελέχους. Ανάπτυξε πρωτόκολλα ελέγχου ταυτότητας email (DMARC, DKIM, SPF) για να αποτρέψεις την πλαστογράφηση ονόματος τομέα. Επίβαλε MFA με υλικό κλειδί σε όλες τις εταιρικές συνδέσεις της ανώτατης διοίκησης.

B Μελέτη περίπτωσης 2: Έκθεση εταιρικών διαπιστευτηρίων στο dark web

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα αρχείο βάσης δεδομένων από το dark web περιέχει αρκετές εκατοντάδες εταιρικά διαπιστευτήρια διαχειριστών συστήματος μιας επιχείρησης. Σχεδίασε μια στρατηγική μετριασμού.
- Προτεινόμενη στρατηγική και λύση: Πραγματοποίησε επαναφορά κωδικών πρόσβασης σε όλη την εταιρεία. Επέβαλε τη χρήση επιχειρησιακού διαχειριστή κωδικών πρόσβασης. Επέβαλε MFA σε όλες τις πύλες του συστήματος και ρύθμισε συνεχείς αυτοματοποιημένες ειδοποιήσεις παρακολούθησης του dark web.