Όνομα: _____ **Ημερομηνία:** _____ **Βαθμολογία:** _____

Απάτες στο διαδίκτυο και κοινωνική μηχανική
Οδηγός προστασίας

Ηλεκτρονικό ψάρεμα (phishing) μέσω email, πλαστά domain, vishing, απάτες υποστήριξης, επαλήθευση εκτός καναλιού, BEC

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

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 άμυνα απέναντι στις διαδικτυακές απάτες. Θα εξερευνήσεις ψεύτικους ιστότοπους ηλεκτρονικού ψαρέματος (phishing), τακτικές κοινωνικής μηχανικής, απάτες υποστήριξης, διαύλους απάτης με εμβάσματα και μεθόδους επαλήθευσης πληρωμών.

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/online-apates/

Η πορεία μάθησής σου: προστασία από διαδικτυακές απάτες

- Αναγνώρισε τους συνήθεις δείκτες απατών τεχνικής υποστήριξης και ονομάτων τομέα typosquatting.
- Εφάρμοσε πρωτόκολλα επαλήθευσης email (SPF, DKIM, DMARC) κατά της πλαστογράφησης.
- Θέσπισε επαλήθευση συναλλαγών εκτός καναλιού για την αποτροπή επιχειρηματικής απάτης με εμβάσματα.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΑΠΑΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

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 από διαδικτυακές απάτες. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ (ΕΙΣΑΓΩΓΗ)

Οι απάτες στο διαδίκτυο εκμεταλλεύονται την ανθρώπινη συμπεριφορά μέσω ηλεκτρονικού ψαρέματος (phishing), αναδυόμενων μηνυμάτων υποστήριξης, vishing και τραπεζικής απάτης. Η επαλήθευση συναλλαγών εκτός καναλιού και οι κανόνες τομέα SPF/DKIM/DMARC βοηθούν στον αποκλεισμό των φορέων κοινωνικής μηχανικής στην πύλη.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Ποιος είναι ο κύριος δείκτης μιας απάτης τεχνικής υποστήριξης;**
   - A. Ένα αναδυόμενο παράθυρο που ισχυρίζεται ότι το σύστημά σου είναι μολυσμένο και απαιτεί να καλέσεις έναν αριθμό τηλεφώνου
   - B. Μια αυτόματη ενημέρωση ασφαλείας που λαμβάνεται από επίσημο μητρώο
   - C. Ένας διαχειριστής κωδικών πρόσβασης που αρνείται να συμπληρώσει διαπιστευτήρια σε εταιρικό όνομα τομέα
   - D. Ένα αντίγραφο ασφαλείας αρχείων στο παρασκήνιο που τρέχει σε ρύθμιση εξωτερικού δίσκου

2. **2. Ποια τεχνική χρησιμοποιεί πλαστά ονόματα τομέα αποστολέα για να κλέψει τραπεζικά στοιχεία;**
   - A. Phishing μέσω email
   - B. Σάρωση θυρών
   - C. Έγχυση στη μνήμη
   - D. Κρυπτογραφικός τεμαχισμός (shredding)

3. **3. Τι αντιπροσωπεύει η απάτη με τραπεζική μεταφορά;**
   - A. Εξαπάτηση θυμάτων ώστε να στείλουν χρήματα σε πλαστούς εταιρικούς λογαριασμούς με χρήση κοινωνικής μηχανικής
   - B. Κρυπτογράφηση βάσεων δεδομένων συστήματος με ωφέλιμα φορτία ransomware
   - C. Αναζήτηση σε βάσεις δεδομένων με εντολές SQL injection
   - D. Δημιουργία αντιγράφων ασφαλείας αρχείων συστήματος σε δίσκους αποθήκευσης εκτός δικτύου

4. **4. Γιατί οι απατεώνες δημιουργούν ψεύτικους ιστότοπους αγορών;**
   - A. Για να κλέψει στοιχεία πιστωτικής κάρτας και διαπιστευτήρια πληρωμής από αγοραστές
   - B. Για τη φιλοξενία πινάκων βάσης δεδομένων ανάλυσης κακόβουλου λογισμικού σε sandbox
   - C. Για να επιταχύνεις την παράδοση των online παραγγελιών
   - D. Για δωρεάν δοκιμή νέων σχεδίων ιστοτόπων

5. **5. Τι σημαίνει vishing;**
   - A. Απάτες φωνητικού phishing μέσω τηλεφωνικών δικτύων για κλοπή διαπιστευτηρίων
   - B. Σάρωση τοπικών δικτύων για μη ασφαλείς συσκευές συστήματος
   - C. Επαναφορά βάσεων δεδομένων συστήματος μετά από μη εξουσιοδοτημένη παραβίαση
   - D. Εκτέλεση μη αξιόπιστου κώδικα μέσα σε ασφαλή εικονικά containers

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Οι απάτες ηλεκτρονικού ψαρέματος στοχεύουν μόνο τελικούς χρήστες, ποτέ στελέχη-στόχους whaling.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Τα πλαστά ονόματα τομέα συχνά χρησιμοποιούν μικρά τυπογραφικά λάθη (όπως amaz0n.com) για να μιμηθούν αξιόπιστες μάρκες.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Οι απάτες τεχνικής υποστήριξης επιλύονται παρέχοντας απομακρυσμένη πρόσβαση στον καλούντα.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Η κοινωνική μηχανική εκμεταλλεύεται την ανθρώπινη ψυχολογία, όπως τον φόβο και την πίεση χρόνου, για να παρακάμψει τους κανόνες ασφαλείας.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Τα αιτήματα τραπεζικής μεταφοράς πρέπει πάντα να επαληθεύονται μέσω εκτός ζώνης (out-of-band) καναλιών επικοινωνίας.

○ 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. Τα δόλια email που ξεγελούν τους χρήστες ονομάζονται ηλεκτρονικό _____ .

2. Οι διευθύνσεις ιστού που μιμούνται αξιόπιστες επωνυμίες είναι _____ .

3. Οι τηλεφωνικές απάτες που στοχεύουν τραπεζικά στοιχεία ονομάζονται _____ .

4. Ένα αναδυόμενο παράθυρο που ζητά χρήματα για αφαίρεση ιών είναι μια _____ τεχνικής υποστήριξης.

5. Η επιβεβαίωση ενός αιτήματος πληρωμής απαιτεί _____ μέσω εναλλακτικού καναλιού.

6. Η ανακατεύθυνση επιχειρηματικών συναλλαγών σε λογαριασμούς κλεφτών είναι δόλιο _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΕΜΒΑΣΜΑ ΕΞΑΠΑΤΗΣΗ ΕΠΑΛΗΘΕΥΣΗ ΜΗΝΥΜΑΤΑ ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ ΦΑΛΑΙΝΟΘΗΡΑ ΦΩΝΗΤΙΚΗ ΑΠΑΤΗ ΨΑΡΕΜΑ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

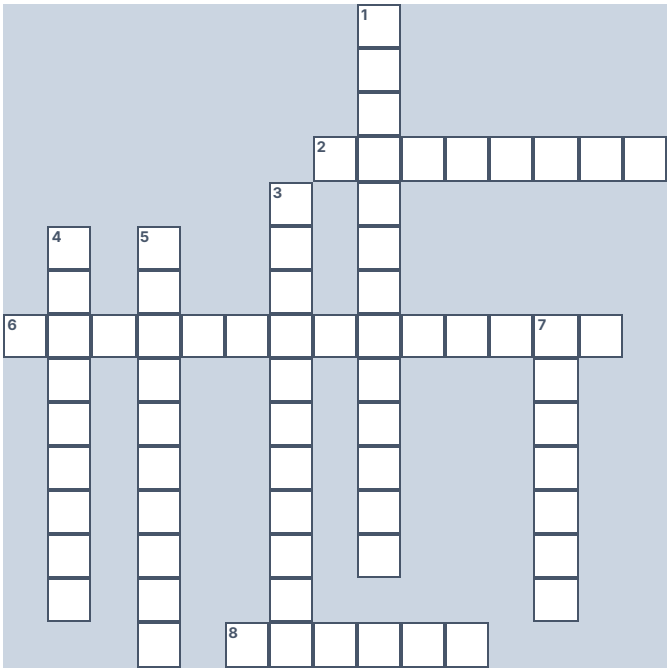
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	**A**	Δόλια εκτροπή τραπεζικών συναλλαγών σε λογαριασμούς εγκληματιών.
☐	2. ΠΛΑΣΤΟΓΡΑΦΗΜΕΝΟ	**B**	Δόλιο σχήμα που αποσκοπεί στην κλοπή χρημάτων ή διαπιστευτηρίων πρόσβασης από τα θύματα.
☐	3. VISHING	**C**	Αποστολή απατηλών μηνυμάτων κειμένου για κλοπή διαπιστευτηρίων κινητών λογαριασμών.
☐	4. ΑΠΑΤΗ	**D**	Δόλιες φωνητικές κλήσεις σχεδιασμένες να κλέβουν διαπιστευτήρια και στοιχεία λογαριασμών.
☐	5. ΕΠΑΛΗΘΕΥΣΗ	**E**	Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος που επιδιώκουν να κλέψουν διαπιστευτήρια από στελέχη C-level.
☐	6. WIRE	**F**	Πλαστογραφημένη διεύθυνση αποστολέα email ή ιστότοπου που φαίνεται νόμιμη.
☐	7. WHALING	**G**	Δόλιες εκστρατείες email σχεδιασμένες να κλέβουν διαπιστευτήρια σύνδεσης και κωδικούς πρόσβασης.
☐	8. SMISHING	**H**	Επιβεβαίωση των στοιχείων πληρωμής μέσω αξιόπιστης δευτερεύουσας μεθόδου επικοινωνίας.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

2. Αποστολή απατηλών γραπτών μηνυμάτων (SMS) για την κλοπή διαπιστευτηρίων κινητού λογαριασμού. (8)

6. Μιμημένη διεύθυνση αποστολέα email ή ιστότοπου που φαίνεται νόμιμη (πλαστές διευθύνσεις). (14)

8. Δόλιες εκστρατείες email που σχεδιάζονται για να κλέψουν διαπιστευτήρια σύνδεσης και κωδικούς πρόσβασης. (6)

ΚΑΘΕΤΑ

1. Δόλιες φωνητικές κλήσεις που σχεδιάζονται για να κλέψουν διαπιστευτήρια και στοιχεία λογαριασμών (vishing). (13)

3. Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος που αποσκοπούν στην κλοπή διαπιστευτηρίων από ανώτατα στελέχη (C-level). (11)

4. Δόλιο σχέδιο που σχεδιάζεται για να κλέψει χρήματα ή διαπιστευτήρια πρόσβασης από τα θύματα. (9)

5. Επιβεβαίωση των στοιχείων πληρωμής μέσω μιας αξιόπιστης δευτερεύουσας μεθόδου επικοινωνίας. (10)

7. Δόλια ανακατεύθυνση τραπεζικών συναλλαγών σε λογαριασμούς εγκληματιών. (7)

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

2 οριζόντια: Αποστολή απατηλών γραπτών μηνυμάτων (SMS) για την κλοπή διαπιστευτηρίων κινητού λογαριασμού. (8 γράμματα):

6 οριζόντια: Μιμημένη διεύθυνση αποστολέα email ή ιστότοπου που φαίνεται νόμιμη (πλαστές διευθύνσεις). (14 γράμματα):

8 οριζόντια: Δόλιες εκστρατείες email που σχεδιάζονται για να κλέψουν διαπιστευτήρια σύνδεσης και κωδικούς πρόσβασης. (6 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Δόλιες φωνητικές κλήσεις που σχεδιάζονται για να κλέψουν διαπιστευτήρια και στοιχεία λογαριασμών (vishing). (13 γράμματα):

3 κάθετα: Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος που αποσκοπούν στην κλοπή διαπιστευτηρίων από ανώτατα στελέχη (C-level). (11 γράμματα):

4 κάθετα: Δόλιο σχέδιο που σχεδιάζεται για να κλέψει χρήματα ή διαπιστευτήρια πρόσβασης από τα θύματα. (9 γράμματα):

5 κάθετα: Επιβεβαίωση των στοιχείων πληρωμής μέσω μιας αξιόπιστης δευτερεύουσας μεθόδου επικοινωνίας. (10 γράμματα):

7 κάθετα: Δόλια ανακατεύθυνση τραπεζικών συναλλαγών σε λογαριασμούς εγκληματιών. (7 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.

Ζ Ω Ρ Η Χ Φ Θ Φ Ε Π Τ Ν Τ Κ Ρ

Δ Τ Σ Λ Ο Α Λ Ω Μ Σ Θ Κ Ο Ε Θ

Α Ψ Ξ Λ Χ Μ Υ Ν Ν Ψ Π Π Ξ Β Α

Ρ Λ Ο Μ Β Σ Λ Η Θ Ζ Ι Α Ν Ψ Β

Η Ω Ω Ψ Β Α Ν Τ Υ Χ Π Μ Γ Ε Ψ

Θ Ξ Χ Ο Π Β Χ Ι Η Α Δ Ψ Β Α Φ

Ο Λ Ε Η Η Μ Ω Κ Τ Φ Γ Ξ Ρ Π Κ

Ν Χ Χ Ρ Κ Ε Ω Η Α Ν Ρ Ε Ω Ρ Μ

Ι Ζ Σ Φ Ζ Λ Σ Α Χ Ι Μ Β Ψ Γ Β

Α Ψ Ξ Υ Ω Η Ξ Π Ω Α Υ Τ Β Θ Φ

Λ Π Α Ρ Α Π Λ Α Ν Η Τ Ι Κ Ε Σ

Α Ο Χ Γ Ν Μ Θ Τ Ο Χ Ψ Ω Χ Η Ν

Φ Ι Η Σ Υ Ε Θ Η Λ Α Π Ε Ξ Ρ Φ

Ζ Υ Υ Ε Χ Θ Ψ Ν Τ Η Υ Μ Κ Ε Λ

Μ Α Τ Α Μ Υ Ν Η Μ Ζ Ν Κ Υ Ι Η

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΨΑΡΕΜΑ
ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ ΕΜΒΑΣΜΑ
ΦΩΝΗΤΙΚΗΑΠΑΤΗ ΦΑΛΑΙΝΟΘΗΡΑ
ΕΞΑΠΑΤΗΣΗ ΜΗΝΥΜΑΤΑ
ΕΠΑΛΗΘΕΥΣΗ

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. ΨΑΡΕΜΑ

B. ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ

C. ΦΩΝΗΤΙΚΗΑΠΑΤΗ

D. ΕΞΑΠΑΤΗΣΗ

E. ΕΠΑΛΗΘΕΥΣΗ

F. ΕΜΒΑΣΜΑ

G. ΦΑΛΑΙΝΟΘΗΡΑ

H. ΜΗΝΥΜΑΤΑ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Μιμημένη διεύθυνση αποστολέα email ή ιστότοπου που φαίνεται νόμιμη (πλαστές διευθύνσεις).

2. Επιβεβαίωση των στοιχείων πληρωμής μέσω μιας αξιόπιστης δευτερεύουσας μεθόδου επικοινωνίας.

3. Δόλια ανακατεύθυνση τραπεζικών συναλλαγών σε λογαριασμούς εγκληματιών.

4. Αποστολή απατηλών γραπτών μηνυμάτων (SMS) για την κλοπή διαπιστευτηρίων κινητού λογαριασμού.

5. Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος που αποσκοπούν στην κλοπή διαπιστευτηρίων από ανώτατα στελέχη (C-level).

6. Δόλιες φωνητικές κλήσεις που σχεδιάζονται για να κλέψουν διαπιστευτήρια και στοιχεία λογαριασμών (vishing).

7. Δόλιες εκστρατείες email που σχεδιάζονται για να κλέψουν διαπιστευτήρια σύνδεσης και κωδικούς πρόσβασης.

8. Δόλιο σχέδιο που σχεδιάζεται για να κλέψει χρήματα ή διαπιστευτήρια πρόσβασης από τα θύματα.

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. **ΡΨΕΜΑΑ**

2. **ΤΤΩΙΝΦΑΚΗΑΠΗΗ**

3. **ΕΘΣΕΠΗΗΛΥΑ**

4. **ΟΡΑΝΛΙΗΘΦΑΑ**

5. **ΤΡΚΑΝΗΠΣΛΙΑΠΕΑ**

6. **ΣΠΞΗΤΕΑΗΑ**

7. **ΕΜΣΑΜΑΒ**

8. **ΥΗΜΑΜΤΑΝ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Συσκευές που μπορούν να παραβιαστούν			
2	Φράσεις που χρησιμοποιούν συχνά οι απατεώνες			
3	Τρόποι πληρωμής που ζητούν οι απατεώνες			
4	Τύποι διαδικτυακών απατών			
5	Προσφορές που είναι πολύ καλές για να είναι αληθινές			
6	Μέρη όπου αναφέρεις μια απάτη			
7	Λέξεις που σχετίζονται με την κυβερνοασφάλεια			
8	Άνθρωποι που μπορείς να προειδοποιήσεις για απάτες			
9	Πράγματα που παίρνεις αντίγραφο ασφαλείας			
10	Προειδοποιητικά σημάδια σε ένα email			
11	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
12	Τρόποι να ελέγξεις ένα ηλεκτρονικό κατάστημα			
13	Τρόποι να προστατεύσεις τους λογαριασμούς σου			
14	Πράγματα που κάνεις αν πέσεις θύμα απάτης			
15	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΡΟΛΗΨΗ ΑΠΑΤΗΣ ΜΕ ΕΤΑΙΡΙΚΟ ΕΜΒΑΣΜΑ



Σενάριο: Ένα οικονομικό τμήμα λαμβάνει ένα επείγον email από πλαστογραφημένη διεύθυνση προμηθευτή, που ζητά τα μελλοντικά εμβάσματα τιμολογίων να κατευθύνονται σε νέο αριθμό δρομολόγησης.

Ερώτηση συζήτησης: Περίγραψε συνοπτικά την πολιτική επαλήθευσης απάτης με εμβάσματα και προσδιόρισε τα μέτρα ταυτοποίησης email.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΕΡΙΣΤΑΤΙΚΟ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ WHALING ΣΕ ΑΝΩΤΑΤΟ ΣΤΕΛΕΧΟΣ



Σενάριο: Ένα στέλεχος πάτησε σε σύνδεσμο ηλεκτρονικού ψαρέματος που ισχυριζόταν ότι περιέχει ασφαλές έγγραφο συνεδρίασης διοικητικού συμβουλίου, εισάγοντας τα κύρια εταιρικά του διαπιστευτήρια σε πλαστογραφημένη πύλη.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τα βήματα αντιμετώπισης του περιστατικού και εξήγησε πώς ελέγχονται οι συνδέσεις των στελεχών.

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	15		23	1	17	5	12	1		12	5

5	16	1	11	7	8	5	20	18	7		18	1	17	24	19	7

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 μια απάτη στο διαδίκτυο;

Ένα δόλιο σχέδιο που χρησιμοποιεί ψηφιακά κανάλια για να εξαπατήσει τα θύματα ώστε να στείλουν χρήματα ή να αποκαλύψουν προσωπικά διαπιστευτήρια.

Q2: Ποιος είναι ο κύριος δείκτης ηλεκτρονικού ψαρέματος μέσω email;

Ένα μήνυμα που ισχυρίζεται ότι είναι επείγον (όπως αναστολή λογαριασμού) και σε κατευθύνει σε έναν σύνδεσμο που δεν ταιριάζει με το επίσημο όνομα τομέα.

Q3: Τι είναι το typosquatting;

Καταχώριση ονομάτων τομέα με συνηθισμένα τυπογραφικά λάθη δημοφιλών επωνυμιών (όπως amaz0n.com) για τη φιλοξενία ψεύτικων ιστότοπων ηλεκτρονικού ψαρέματος.

Q4: Τι είναι η απάτη τεχνικής υποστήριξης;

Ένα αναδυόμενο παράθυρο που ισχυρίζεται ότι ο υπολογιστής σου είναι μολυσμένος, σε κατευθύνει να καλέσεις έναν αριθμό και να πληρώσεις για ψεύτικο λογισμικό καθαρισμού ή υπηρεσίες απομακρυσμένης πρόσβασης. [1]

Q5: Τι είναι το vishing;

Επιθέσεις ηλεκτρονικού ψαρέματος μέσω φωνητικών τηλεφωνικών κλήσεων για να εξαπατηθούν τα θύματα και να δώσουν στοιχεία τραπεζικού λογαριασμού ή σύνδεσης.

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 τηλεγραφική απάτη (wire fraud);

Ανακατεύθυνση συναλλαγών πληρωμής σε λογαριασμούς απάτης με πλαστοπροσωπία προμηθευτών ή στελεχών.

Q7: Τι είναι το whaling;

Μια εξαιρετικά στοχευμένη μορφή spear phishing που στοχεύει απευθείας υψηλής αξίας στόχους, όπως ανώτατα εταιρικά στελέχη (C-level).

Q8: Τι είναι το smishing;

Απατηλά μηνύματα κειμένου που στέλνονται σε κινητές συσκευές, με συνδέσμους προς ψεύτικες πύλες ή ενημερώσεις παρακολούθησης.

Q9: Γιατί είναι κρίσιμη η επαλήθευση εκτός ζώνης (out-of-band);

Επιβεβαιώνει τις λεπτομέρειες της συναλλαγής μέσω ξεχωριστού καναλιού επικοινωνίας (όπως τηλεφωνική κλήση), αποφεύγοντας τις παραβιασμένες αλυσίδες email.

Q10: Πώς λειτουργεί μια απάτη με πλαστό λογαριασμό μεσεγγύησης;

Οι απατεώνες δημιουργούν έναν πλαστό ιστότοπο μεσεγγύησης (escrow), ισχυριζόμενοι ότι τα κεφάλαια κρατούνται με ασφάλεια, και στη συνέχεια κλέβουν την κατάθεση με έμβασμα του αγοραστή.

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 χρησιμοποιούν οι απατεώνες το BEC (Business Email Compromise) για να εκτελέσουν τραπεζική απάτη;

Παραβιάζουν τον λογαριασμό email ενός νόμιμου υπαλλήλου, παρακολουθούν τις συζητήσεις για τιμολόγια και στέλνουν ενημερωμένα στοιχεία χρέωσης με δόλιους τραπεζικούς λογαριασμούς.

Q2: Ποιος είναι ο κίνδυνος των επιθέσεων ομογραφίας IDN σε απάτες στο διαδίκτυο;

Χρήση χαρακτήρων εκτός ASCII που μοιάζουν πανομοιότυποι με κανονικά γράμματα (π.χ. το κυριλλικό 'a') για την καταχώριση πλαστών τομέων που μιμούνται πραγματικές μάρκες.

Q3: Γιατί είναι σημαντικός ο έλεγχος των κεφαλίδων email στον εντοπισμό απάτης;

Αποκαλύπτει την πραγματική IP του διακομιστή προέλευσης και την κατάσταση επικύρωσης SPF/DKIM, δείχνοντας αν το όνομα τομέα του αποστολέα είναι πλαστό.

Q4: Πώς εκμεταλλεύονται οι απατεώνες τεχνικής υποστήριξης το λογισμικό απομακρυσμένης επιφάνειας εργασίας;

Χρησιμοποιούν βοηθητικά προγράμματα όπως το AnyDesk ή το TeamViewer για να συνδεθούν στη συσκευή του θύματος, να φυτέψουν κακόβουλο λογισμικό και να κλέψουν αποθηκευμένους κωδικούς πρόσβασης.

Q5: Ποιος είναι ο στόχος των απατών προκαταβολικής πληρωμής;

Εξαπάτηση των θυμάτων ώστε να πληρώσουν εκ των προτέρων τέλη επεξεργασίας με αντάλλαγμα μια μεγάλη οικονομική ανταμοιβή που δεν υπάρχει.

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 χρησιμοποιούν οι απατεώνες τη δημιουργία προφίλ από τα μέσα κοινωνικής δικτύωσης για στοχευμένο ηλεκτρονικό ψάρεμα (phishing);

Συγκεντρώνουν εταιρικές οργανωτικές δομές και ονόματα υπαλλήλων για να συντάξουν πειστικά email spear-phishing.

Q7: Γιατί τα ψεύτικα ηλεκτρονικά καταστήματα προσφέρουν μεγάλες εκπτώσεις;

Για να παρασύρουν αγοραστές να εισάγουν τα στοιχεία της πιστωτικής τους κάρτας, συλλέγοντας διαπιστευτήρια για επαναχρησιμοποίηση ή μεταπώληση σε φόρουμ carding.

Q8: Πώς αποκλείουν οι εγγραφές DMARC τις απάτες ηλεκτρονικού ψαρέματος (phishing);

Το DMARC επιτρέπει στους κατόχους ονομάτων τομέα να ζητούν από τους παραλήπτες να θέσουν σε καραντίνα ή να απορρίψουν την αλληλογραφία που αποτυγχάνει στους ελέγχους SPF και DKIM με ευθυγράμμιση, εμποδίζοντας την άμεση πλαστογράφηση. [5]

Q9: Ποια είναι η απειλή των πυλών συλλογής διαπιστευτηρίων;

Πλαστές σελίδες προορισμού σχεδιασμένες να μοιάζουν ακριβώς με περιβάλλοντα Microsoft 365 ή Google Workspace, που κλέβουν τα διαπιστευτήρια σύνδεσης καθώς πληκτρολογούνται.

Q10: Πώς αναφέρουν και απενεργοποιούν οι ομάδες ασφαλείας τους τομείς απάτης;

Υποβάλλοντας αποδείξεις απάτης στο email κατάχρησης του καταχωρητή, στον πάροχο φιλοξενίας και στο μητρώο Google Safe Browsing.

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. [2]

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η παραβίαση επιχειρηματικού email (BEC) προκάλεσε απώλειες άνω των $3 δισεκατομμυρίων που αναφέρθηκαν στο IC3 του FBI το 2025. [2]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι τομείς με typosquatting διαφέρουν από τα πραγματικά ονόματα μαρκών κατά έναν ή δύο χαρακτήρες, οπότε μια γρήγορη ματιά μπορεί να τους προσπεράσει.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι απάτες τεχνικής υποστήριξης προκάλεσαν ζημιές άνω των 2,1 δισ. $ που αναφέρθηκαν στο IC3 του FBI το 2025. [2]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιθέσεις ομόγλυφων φαίνονται πανομοιότυπες στη γραμμή διευθύνσεων των προγραμμάτων περιήγησης, εκτός αν το πρόγραμμα περιήγησης εμφανίζει τις μορφές punycode.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι απάτες με μηνύματα SMS (smishing) χρησιμοποιούν σύντομα, επείγοντα μηνύματα με συνδέσμους, αφήνοντας στα θύματα ελάχιστο πλαίσιο για να εντοπίσουν την απάτη.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιθέσεις whaling στοχεύουν τα email στελεχών επειδή ελέγχουν την πρόσβαση σε μεγάλες τραπεζικές μεταφορές πληρωμών.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η επαλήθευση αλλαγών πληρωμής με κλήση σε γνωστό, αποθηκευμένο τηλεφωνικό αριθμό είναι βασική άμυνα απέναντι στην απάτη τραπεζικού εμβάσματος BEC.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι ψεύτικοι ιστότοποι λογαριασμού μεσεγγύησης (escrow) είναι συνηθισμένη απάτη στις διαδικτυακές αγορές: μοιάζουν με ασφαλή υπηρεσία πληρωμών αλλά κλέβουν το έμβασμα του αγοραστή.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το Google Safe Browsing προειδοποιεί τους χρήστες πριν ανοίξουν ιστότοπους που έχει επισημάνει για ηλεκτρονικό ψάρεμα (phishing) ή κακόβουλο λογισμικό.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

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

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

[5] 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

Ποιος είναι ο κύριος δείκτης μιας απάτης τεχνικής υποστήριξης; → Ένα αναδυόμενο παράθυρο που ισχυρίζεται ότι το σύστημά σου είναι μολυσμένο και απαιτεί να καλέσεις έναν αριθμό τηλεφώνου

2 Ερώτηση 2 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποια τεχνική χρησιμοποιεί πλαστά ονόματα τομέα αποστολέα για να κλέψει τραπεζικά στοιχεία; → Phishing μέσω email

3 Ερώτηση 3 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι αντιπροσωπεύει η απάτη με τραπεζική μεταφορά; → Εξαπάτηση θυμάτων ώστε να στείλουν χρήματα σε πλαστούς εταιρικούς λογαριασμούς με χρήση κοινωνικής μηχανικής

4 Ερώτηση 4 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Γιατί οι απατεώνες δημιουργούν ψεύτικους ιστότοπους αγορών; → Για να κλέψει στοιχεία πιστωτικής κάρτας και διαπιστευτήρια πληρωμής από αγοραστές

5 Ερώτηση 5 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι σημαίνει vishing; → Απάτες φωνητικού phishing μέσω τηλεφωνικών δικτύων για κλοπή διαπιστευτηρίων

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το ηλεκτρονικό ψάρεμα στοχεύει και στελέχη· το whaling είναι ηλεκτρονικό ψάρεμα που στοχεύει ανώτατα στελέχη.

7 Ερώτηση 7

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα πλαστά ονόματα τομέα συχνά χρησιμοποιούν μικρά τυπογραφικά λάθη (όπως amaz0n.com) για να μιμηθούν αξιόπιστες μάρκες.

8 Ερώτηση 8

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: αν δώσεις απομακρυσμένη πρόσβαση σε απατεώνα που παριστάνει την υποστήριξη, μπορεί να φυτέψει κακόβουλο λογισμικό και να κλέψει δεδομένα.

9 Ερώτηση 9

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η κοινωνική μηχανική εκμεταλλεύεται την ανθρώπινη ψυχολογία, όπως τον φόβο και την πίεση χρόνου, για να παρακάμψει τους κανόνες ασφαλείας.

10 Ερώτηση 10

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα αιτήματα τραπεζικής μεταφοράς πρέπει πάντα να επαληθεύονται μέσω εκτός ζώνης (out-of-band) καναλιών επικοινωνίας.

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

G 1. ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	F 2. ΠΛΑΣΤΟΓΡΑΦΗΜΕΝΟ	D 3. VISHING	B 4. ΑΠΑΤΗ
H 5. ΕΠΑΛΗΘΕΥΣΗ	A 6. WIRE	E 7. WHALING	C 8. SMISHING

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΨΑΡΕΜΑ	2 ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ	3 ΦΩΝΗΤΙΚΗ ΑΠΑΤΗ	4 ΕΞΑΠΑΤΗΣΗ
5 ΕΠΑΛΗΘΕΥΣΗ	6 ΕΜΒΑΣΜΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 Β – ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ	2 Ε – ΕΠΑΛΗΘΕΥΣΗ	3 F – ΕΜΒΑΣΜΑ	4 Η – ΜΗΝΥΜΑΤΑ
5 G – ΦΑΛΑΙΝΟΘΗΡΑ	6 C – ΦΩΝΗΤΙΚΗΑΠΑΤΗ	7 Α – ΨΑΡΕΜΑ	8 D – ΕΞΑΠΑΤΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ, ΠΛΑΣΤΟΓΡΑΦΗΜΕΝΟ και VISHING 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.

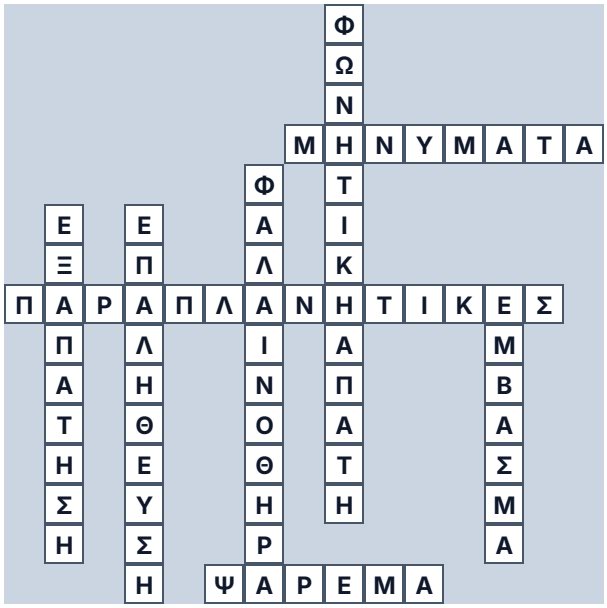
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: ΜΗΝΥΜΑΤΑ Αποστολή απατηλών γραπτών μηνυμάτων (SMS) για την κλοπή διαπιστευτηρίων κινητού λογαριασμού. (8 γράμματα)

6 οριζόντια: ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ Μιμημένη διεύθυνση αποστολέα email ή ιστότοπου που φαίνεται νόμιμη (πλαστές διευθύνσεις). (14 γράμματα)

8 οριζόντια: ΨΑΡΕΜΑ Δόλιες εκστρατείες email που σχεδιάζονται για να κλέψουν διαπιστευτήρια σύνδεσης και κωδικούς πρόσβασης. (6 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΦΩΝΗΤΙΚΗΑΠΑΤΗ Δόλιες φωνητικές κλήσεις που σχεδιάζονται για να κλέψουν διαπιστευτήρια και στοιχεία λογαριασμών (vishing). (13 γράμματα)

3 κάθετα: ΦΑΛΑΙΝΟΘΗΡΑ Στοχευμένες επιθέσεις ηλεκτρονικού ψαρέματος που αποσκοπούν στην κλοπή διαπιστευτηρίων από ανώτατα στελέχη (C-level). (11 γράμματα)

4 κάθετα: ΕΞΑΠΑΤΗΣΗ Δόλιο σχέδιο που σχεδιάζεται για να κλέψει χρήματα ή διαπιστευτήρια πρόσβασης από τα θύματα. (9 γράμματα)

5 κάθετα: ΕΠΑΛΗΘΕΥΣΗ Επιβεβαίωση των στοιχείων πληρωμής μέσω μιας αξιόπιστης δευτερεύουσας μεθόδου επικοινωνίας. (10 γράμματα)

7 κάθετα: ΕΜΒΑΣΜΑ Δόλια ανακατεύθυνση τραπεζικών συναλλαγών σε λογαριασμούς εγκληματιών. (7 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΡΨΕΜΑΑ — **ΨΑΡΕΜΑ**
2. ΤΤΩΙΝΦΑΚΗΑΠΗΗ — **ΦΩΝΗΤΙΚΗΑΠΑΤΗ**
3. ΕΘΣΕΠΗΗΛΥΑ — **ΕΠΑΛΗΘΕΥΣΗ**
4. ΟΡΑΝΛΙΗΘΦΑΑ — **ΦΑΛΑΙΝΟΘΗΡΑ**
5. ΤΡΚΑΝΗΠΣΛΙΑΠΕΑ — **ΠΑΡΑΠΛΑΝΗΤΙΚΕΣ**
6. ΣΠΞΗΤΕΑΗΑ — **ΕΞΑΠΑΤΗΣΗ**
7. ΕΜΣΑΜΑΒ — **ΕΜΒΑΣΜΑ**
8. ΥΗΜΑΜΤΑΝ — **ΜΗΝΥΜΑΤΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΝΤΟΠΙΣΕ ΤΟ ΨΑΡΕΜΑ ΜΕ ΕΠΑΛΗΘΕΥΣΗ ΣΑΡΩΤΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Πρόληψη απάτης με εταιρικό έμβασμα

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα οικονομικό τμήμα λαμβάνει ένα επείγον email από πλαστογραφημένη διεύθυνση προμηθευτή, που ζητά τα μελλοντικά εμβάσματα τιμολογίων να κατευθύνονται σε νέο αριθμό δρομολόγησης.
- Προτεινόμενη στρατηγική και λύση: Επιβάλλεται πολιτική διπλής εξουσιοδότησης για όλες τις πληρωμές. Εφάρμοσε επαλήθευση εκτός καναλιού με προαποθηκευμένο αριθμό τηλεφώνου και αποκλεισμό στην πύλη των email από πλαστογραφημένα ονόματα τομέα.

B Μελέτη περίπτωσης 2: Περιστατικό ηλεκτρονικού ψαρέματος whaling σε ανώτατο στέλεχος

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα στέλεχος πάτησε έναν σύνδεσμο ηλεκτρονικού ψαρέματος (phishing) που υποσχόταν ασφαλές έγγραφο για συνεδρίαση διοικητικού συμβουλίου και εισήγαγε τα κύρια εταιρικά διαπιστευτήριά του σε μια πλαστή πύλη.
- Προτεινόμενη στρατηγική και λύση: Απομόνωσε τη συσκευή του στελέχους. Επανέφερε όλα τα διακριτικά συνεδρίας και τα διαπιστευτήρια της εταιρείας. Εξέτασε τα αρχεία καταγραφής πρόσβασης για εξαγωγή δεδομένων και εφάρμοσε MFA με υλικό κλειδί σε όλες τις συνδέσεις.