Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Πώς να επιλέξεις ένα VPN Φύλλο εργασίας

Αξιολόγηση παρόχων VPN, προτύπων ασφάλειας, ελέγχων και πολιτικών καταγραφής

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ VPN

ΜΑΘΗΤΗΣ

ΙΔΙΟΤΗΤΑ ΦΟΙΤΗΤΗ

Διαδρομή Network Defender

ΑΣΦΑΛΕΣ

ΚΑΤΑΣΤΑΣΗ ΣΥΝΔΕΣΗΣ

Θωράκιση πακέτων δεδομένων

ΕΝΕΡΓΟ

ΠΡΟΣΤΑΣΙΑ ΔΙΑΡΡΟΩΝ

Προστασία από διαρροές DNS και IPv6

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στις βασικές αρχές των εικονικών ιδιωτικών δικτύων (VPN). Θα εξερευνήσεις πώς οι κρυπτογραφημένες σήραγγες ασφαλίζουν τα δεδομένα σου, πώς λειτουργούν τα πρωτόκολλα δικτύου και πώς να εντοπίζεις και να περιορίζεις τις διαρροές ιδιωτικότητας.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- ☐ **Μέρη 1-4: Κατάκτησε τις έννοιες και τα πρωτόκολλα των VPN.**
- ☐ **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 τα VPN

URL: https://www.vpn.com/el/vpn/

Η πορεία μάθησής σου: VPN

- Αξιολόγησε τη δικαιοδοσία του παρόχου και τις πολιτικές μηδενικής τήρησης αρχείων καταγραφής για το απόρρητο.
- Σύγκρινε πρωτόκολλα σηράγγωσης όπως το WireGuard και το OpenVPN ως προς την ταχύτητα.
- Ανάλυσε λειτουργίες ασφαλείας όπως οι kill switch και οι κόμβοι διακομιστών μόνο RAM.
- Αναγνώρισε τους ανεξάρτητους ελέγχους ασφαλείας και τα πακέτα τιμολόγησης κατά την επιλογή.
- Επίλεξε τοποθεσίες διακομιστών ανάλογα με την ταχύτητα και τις ανάγκες σου για άρση γεωγραφικών αποκλεισμών.

ΟΔΗΓΙΕΣ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ ΕΠΙΛΟΓΗΣ

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 επιλογή ασφαλούς υποδομής VPN. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΕΠΙΛΟΓΗ VPN (ΕΙΣΑΓΩΓΗ)

Για να επιλέξεις το σωστό VPN, πρέπει να κοιτάξεις πέρα από τη διαφημιστική υπερβολή. Ένας αξιόπιστος πάροχος πρέπει να έχει αποδεδειγμένη πολιτική μηδενικού ιστορικού (zero logs), ασφαλή πρωτόκολλα κρυπτογράφησης και πελάτες ανοιχτού κώδικα. Αξιολογώντας τα χαρακτηριστικά ασφαλείας, τις δικαιοδοσίες και την απόδοση ταχύτητας, μπορείς να επιλέξεις ένα VPN που ταιριάζει στις ανάγκες ψηφιακής προστασίας σου.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιος είναι ο βασικός παράγοντας κατά την επιλογή ενός ασφαλούς παρόχου VPN;**
   - A. Ο αριθμός των χωρών διακομιστών
   - B. Μια πολιτική no-logs με ανεξάρτητο έλεγχο
   - C. Η χαμηλότερη μηνιαία βαθμίδα τιμολόγησης
   - D. Εντυπωσιακές διαφημιστικές χορηγίες

2. **Ποιο πρωτόκολλο VPN προσφέρει την καλύτερη ισορροπία ταχύτητας και δυνατότητας ελέγχου;**
   - A. PPTP (παλαιό)
   - B. L2TP/IPSec
   - C. OpenVPN μόνο μέσω TCP
   - D. WireGuard

3. **Γιατί οι χρήστες πρέπει να αποφεύγουν τα δωρεάν VPN για ευαίσθητες δραστηριότητες;**
   - A. Απαγορεύονται στις Ηνωμένες Πολιτείες
   - B. Συχνά πουλούν το ιστορικό περιήγησής σου στον ιστό
   - C. Δεν υποστηρίζουν βασική περιήγηση στον ιστό
   - D. Απαιτούν ειδικό υλικό για σύνδεση

4. **Τι καθορίζει η νομική δικαιοδοσία της έδρας ενός παρόχου;**
   - A. Η ταχύτητα της σύνδεσης με τον διακομιστή
   - B. Οι τύποι των συσκευών που υποστηρίζονται
   - C. Τοπικοί νόμοι για τη διατήρηση δεδομένων και τα εντάλματα έρευνας
   - D. Το οπτικό θέμα της εφαρμογής-πελάτη

5. **Ποιος είναι ο κύριος σκοπός της λειτουργίας «kill switch» ενός πελάτη VPN;**
   - A. Για να αποκλείσει την πρόσβαση στο διαδίκτυο αν διακοπεί η σύνδεση VPN
   - B. Για τη διαγραφή όλων των εγκατεστημένων εφαρμογών στη συσκευή
   - C. Για να διπλασιάσεις την ταχύτητα της σύνδεσης με τον διακομιστή
   - D. Για επανεκκίνηση του λειτουργικού συστήματος όταν είναι αδρανές

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Ένα VPN προστατεύει τη συσκευή σου από λήψεις κακόβουλου λογισμικού και αρχεία ιών.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Ανεξάρτητοι έλεγχοι από εταιρείες όπως η Deloitte επαληθεύουν τους ισχυρισμούς μηδενικών καταγραφών.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Οι νόμοι της χώρας καταγωγής ενός παρόχου δεν επηρεάζουν την ιδιωτικότητα των δεδομένων των χρηστών.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Η συμπαγής βάση κώδικα του WireGuard είναι ευκολότερη στον έλεγχο από εκείνη του OpenVPN.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Τα δωρεάν VPN συχνά πουλούν διαφημίσεις ή παρακολουθούν τους χρήστες για να καλύψουν το κόστος των διακομιστών.

○ 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. Μια ανεξάρτητα επαληθευμένη πολιτική δεσμεύει τον πάροχο VPN να μην καταγράφει το ιστορικό σου: _____ .

2. Το σύγχρονο πρωτόκολλο _____ προσφέρει υψηλή ταχύτητα και χρησιμοποιεί πολύ μικρή βάση κώδικα.

3. Ο _____ ασφαλείας διακόπτει όλη την κίνηση αν η σύνδεση VPN αποτύχει ξαφνικά.

4. Η αξιολόγηση της νομικής _____ ενός παρόχου καθορίζει αν υπόκειται σε συνθήκες παρακολούθησης.

5. Η ασφάλιση των διακομιστών με τεχνολογία _____ βοηθά ώστε τα δεδομένα των χρηστών να μη διατηρούνται μετά από επανεκκίνηση.

6. Η επαλήθευση ισχυρισμών περί μηδενικής γνώσης απαιτεί έναν ανεξάρτητο _____ ασφαλείας από αξιόπιστες εταιρείες.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΔΙΑΚΟΠΤΗΣ ΔΙΚΑΙΟΔΟΣΙΑ ΔΩΡΕΑΝ ΕΛΕΓΧΟΣ ΜΗ ΚΑΤΑΓΡΑΦΗ ΜΟΝΟ ΜΝΗΜΗ ΣΗΡΑΓΓΑ WIREGUARD

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών δικτύου

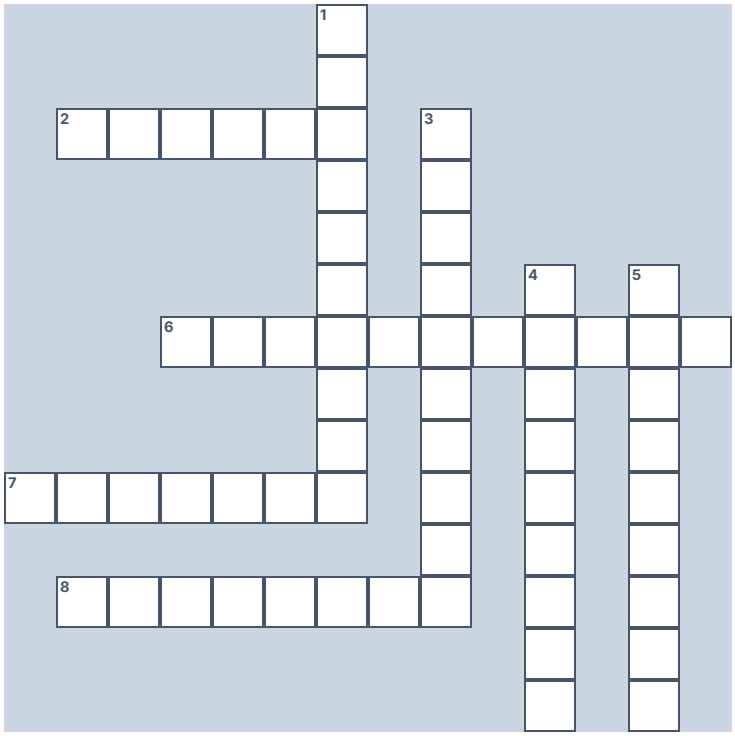
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. WireGuard	A	Υπηρεσία σύνδεσης υψηλού κινδύνου που συχνά αποκομίζει έσοδα καταγράφοντας και πουλώντας δεδομένα περιήγησης.
☐	2. Ελεγμένα αρχεία καταγραφής	B	Μηχανισμός ασφαλείας που αποκλείει τη δρομολόγηση διαδικτύου αν διακοπεί η ασφαλής σήραγγα.
☐	3. Δικαιοδοσία	C	Διεθνής συμμαχία ανταλλαγής πληροφοριών μεταξύ ΗΠΑ, ΗΒ, ΚΑ, ΑΥ και ΝΖ.
☐	4. Kill switch	D	Υποδομή υλικού που λειτουργεί σε πτητική μνήμη, ώστε τα δεδομένα να μην αποθηκεύονται στον δίσκο.
☐	5. Five Eyes	E	Η γεωγραφική περιοχή που διέπει τις νομικές υποχρεώσεις του παρόχου VPN.
☐	6. Δωρεάν VPN	F	Σύγχρονο, γρήγορο πρωτόκολλο που χρησιμοποιεί περίπου 4.000 γραμμές κώδικα ιδιαίτερα εύκολου στον έλεγχο.
☐	7. Διακομιστές μόνο RAM	G	Ώριμο πρωτόκολλο ανοιχτού κώδικα με εκτεταμένους ελέγχους και πολύ μεγαλύτερη βάση κώδικα από το WireGuard.
☐	8. OpenVPN	H	Ισχυρισμός ιδιωτικότητας που έχει επαληθευτεί από ανεξάρτητες εταιρείες κυβερνοασφάλειας τρίτων.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

2. Υπηρεσία σύνδεσης υψηλού κινδύνου που συχνά βγάζει χρήματα καταγράφοντας και πουλώντας δεδομένα περιήγησης (6)

6. Η γεωγραφική περιοχή που καθορίζει τις νομικές υποχρεώσεις του παρόχου VPN (11)

7. Κρυπτογραφημένος δίαυλος ανοιχτού κώδικα, ώριμος και ευρέως ελεγμένος, με πολύ μεγαλύτερη βάση κώδικα από το WireGuard (7)

8. Ισχυρισμός απορρήτου που έχει επαληθευτεί από ανεξάρτητες εταιρείες κυβερνοασφάλειας (8)

ΚΑΘΕΤΑ

1. Διεθνής συμμαχία ανταλλαγής πληροφοριών μεταξύ ΗΠΑ, ΗΒ, Καναδά, Αυστραλίας και Νέας Ζηλανδίας (10)

3. Σύγχρονο, γρήγορο σύνολο κανόνων με περίπου 4.000 γραμμές εύκολα ελέγξιμου κώδικα (10)

4. Υποδομή υλικού που λειτουργεί εξ ολοκλήρου σε προσωρινή μνήμη και δεν αποθηκεύει δεδομένα (9)

5. Μηχανισμός ασφαλείας που μπλοκάρει τη δρομολόγηση του διαδικτύου αν διακοπεί η ασφαλής σήραγγα (9)

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: Υπηρεσία σύνδεσης υψηλού κινδύνου που συχνά βγάζει χρήματα καταγράφοντας και πουλώντας δεδομένα περιήγησης (6 γράμματα):

6 οριζόντια: Η γεωγραφική περιοχή που καθορίζει τις νομικές υποχρεώσεις του παρόχου VPN (11 γράμματα):

7 οριζόντια: Κρυπτογραφημένος δίαυλος ανοιχτού κώδικα, ώριμος και ευρέως ελεγμένος, με πολύ μεγαλύτερη βάση κώδικα από το WireGuard (7 γράμματα):

8 οριζόντια: Ισχυρισμός απορρήτου που έχει επαληθευτεί από ανεξάρτητες εταιρείες κυβερνοασφάλειας (8 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Διεθνής συμμαχία ανταλλαγής πληροφοριών μεταξύ ΗΠΑ, ΗΒ, Καναδά, Αυστραλίας και Νέας Ζηλανδίας (10 γράμματα):

3 κάθετα: Σύγχρονο, γρήγορο σύνολο κανόνων με περίπου 4.000 γραμμές εύκολα ελέγξιμου κώδικα (10 γράμματα):

4 κάθετα: Υποδομή υλικού που λειτουργεί εξ ολοκλήρου σε προσωρινή μνήμη και δεν αποθηκεύει δεδομένα (9 γράμματα):

5 κάθετα: Μηχανισμός ασφαλείας που μπλοκάρει τη δρομολόγηση του διαδικτύου αν διακοπεί η ασφαλής σήραγγα (9 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.

Τ Σ Σ Ε Λ Ι Β Μ Α Β Γ Ξ Ψ Λ Κ

Ψ Λ Χ Τ Κ Δ Π Ο Μ Ι Ε Δ Θ Ν Ν

Ο Κ Π Ο Η Μ Μ Ν Π Ρ Λ Σ Τ Τ Η

Λ Ν Γ Σ Ο Ξ Θ Ο Ρ Β Ε Φ Δ Σ Ω

Λ Α Υ Γ Ω Δ Φ Μ Ζ Κ Γ Η Ω Π Δ

Ο Ε Ν Δ Π Ι Χ Ν Ο Γ Μ Τ Β Ε Α

Κ Ρ Ω Ν Δ Κ Λ Η Δ Α Ε Δ Ξ Ν Δ

Ο Ω Ε Η Θ Α Δ Μ Ι Σ Ν Ρ Π Τ Μ

Τ Δ Ε Θ Ρ Ι Ω Η Α Η Ο Σ Ε Ε Π

Ω Υ Ε Α Α Ο Π Ξ Κ Ρ Ν Ο Τ Μ Χ

Ρ Π Κ Ρ Τ Δ Ρ Γ Ο Α Ν Ψ Β Α Ζ

Π Ρ Χ Φ Ι Ο Α Ρ Π Γ Ω Ψ Ψ Τ Λ

Ζ Θ Μ Π Κ Σ Μ Μ Τ Γ Σ Ξ Η Ι Ο

Π Η Ω Α Ξ Ι Υ Ζ Η Α Υ Β Ψ Α Ρ

Ψ Β Η Μ Ω Α Η Κ Σ Ξ Ο Ν Χ Γ Μ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΠΡΩΤΟΚΟΛΛΟ
ΕΛΕΓΜΕΝΟ
ΔΙΚΑΙΟΔΟΣΙΑ
ΜΟΝΟΜΝΗΜΗ
ΔΙΑΚΟΠΤΗΣ
ΣΗΡΑΓΓΑ
ΠΕΝΤΕΜΑΤΙΑ
ΔΩΡΕΑΝ

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. ΠΡΩΤΟΚΟΛΛΟ**
- **B. ΕΛΕΓΜΕΝΟ**
- **C. ΔΙΚΑΙΟΔΟΣΙΑ**
- **D. ΔΙΑΚΟΠΤΗΣ**
- **E. ΠΕΝΤΕΜΑΤΙΑ**
- **F. ΔΩΡΕΑΝ**
- **G. ΜΟΝΟΜΝΗΜΗ**
- **H. ΣΗΡΑΓΓΑ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Διεθνής συμμαχία ανταλλαγής πληροφοριών μεταξύ ΗΠΑ, ΗΒ, Καναδά, Αυστραλίας και Νέας Ζηλανδίας.
2. Σύγχρονο, γρήγορο σύνολο κανόνων με περίπου 4.000 γραμμές εύκολα ελέγξιμου κώδικα.
3. Κρυπτογραφημένος δίαυλος ανοιχτού κώδικα, ώριμος και ευρέως ελεγμένος, με πολύ μεγαλύτερη βάση κώδικα από το WireGuard.
4. Υπηρεσία σύνδεσης υψηλού κινδύνου που συχνά βγάζει χρήματα καταγράφοντας και πουλώντας δεδομένα περιήγησης.
5. Μηχανισμός ασφαλείας που μπλοκάρει τη δρομολόγηση του διαδικτύου αν διακοπεί η ασφαλής σήραγγα.
6. Υποδομή υλικού που λειτουργεί εξ ολοκλήρου σε προσωρινή μνήμη και δεν αποθηκεύει δεδομένα.
7. Η γεωγραφική περιοχή που καθορίζει τις νομικές υποχρεώσεις του παρόχου VPN.
8. Ισχυρισμός απορρήτου που έχει επαληθευτεί από ανεξάρτητες εταιρείες κυβερνοασφάλειας.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους των VPN. Γράψε τις απαντήσεις σου στα πλαίσια εισαγωγής.

1. ΛΟΚΟΡΠΛΟΤΩ
2. ΙΑΙΔΙΟΚΣΟΔΑ
3. ΠΜΙΑΕΕΑΤΤΝ
4. ΜΗΜΟΗΝΜΟΝ
5. ΜΕΛΟΓΕΝΕ
6. ΗΚΙΤΠΔΟΣΑ
7. ΑΔΕΝΡΩ
8. ΗΑΑΣΓΓΡ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πράγματα που ένα VPN μπορεί να κρύψει			
2	Πράγματα που μετρούν περισσότερο από την τιμή			
3	Μέρη όπου διαβάζεις κριτικές για VPN			
4	Πράγματα από τα οποία ένα VPN δεν μπορεί να σε προστατεύσει			
5	Ερωτήσεις προς μια ομάδα πωλήσεων VPN			
6	Πράγματα που μπορεί να δει ο πάροχος internet σου			
7	Στοιχεία στη λίστα ελέγχου σου όταν επιλέγεις VPN			
8	Μέρη όπου θα χρησιμοποιούσες ένα VPN			
9	Προειδοποιητικά σημάδια σε έναν πάροχο VPN			
10	Λέξεις που σχετίζονται με το απόρρητο			
11	Πράγματα που θα δοκίμαζες πρώτα			
12	Υποσχέσεις που δίνει ένας καλός πάροχος VPN			
13	Λόγοι για να χρησιμοποιείς VPN όταν ταξιδεύεις			
14	Συσκευές που μπορούν να χρησιμοποιήσουν VPN			
15	Μύθοι για τα VPN			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN

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

SARAH (ΦΟΙΤΗΤΡΙΑ ΣΤΟ ΚΑΦΕ)

👩‍💻 «Γεια! Κάθομαι στο Coffee & Bytes. Υπάρχει ένα μη ασφαλές δημόσιο δίκτυο με όνομα 'Free_Wi-Fi_No_Password'. Θέλω να συνδεθώ στο σχολικό μου email και να ανεβάσω την εργασία μου, αλλά ανησυχώ για τους χάκερ. Ποιοι είναι οι κίνδυνοι της χρήσης αυτού του δικτύου χωρίς VPN και πώς ένα VPN ασφαλίζει τα δεδομένα μου;»

ALEX (ΦΟΙΤΗΤΗΣ ΠΟΥ ΤΑΞΙΔΕΥΕΙ)

👩‍💻 «Ωχ όχι! Ταξιδεύω στο εξωτερικό για ένα project και προσπαθώ να δω ένα ντοκιμαντέρ βιολογίας που φιλοξενείται σε διακομιστή στη χώρα μου. Αλλά ο ιστότοπος λέει 'Αυτό το βίντεο δεν είναι διαθέσιμο στην τρέχουσα τοποθεσία σου.' Γιατί αποκλείομαι και πώς μπορεί ένα VPN να με βοηθήσει να το δω;»

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Για να ολοκληρώσεις την εκπαίδευσή σου στον οδηγό επιλογής, αποκρυπτογράφησε αυτό το κρυφό μήνυμα για την επιλογή ασφαλούς υποδομής.

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

18	20	3	10	17	9	13	5		19	9	18		1	13	1	21	15	17	5	18
		18	15	20		12	5		5	13	1		1	18	21	1	11	5	18	
					18	20	18	19	7	12	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 τα VPN – βασικό επίπεδο (Μέρος Α)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις που έχουν οι υποψήφιοι πελάτες για τη χρήση εικονικών ιδιωτικών δικτύων.

Q1: Τι είναι ένα VPN και πώς λειτουργεί;

Ένα εικονικό ιδιωτικό δίκτυο (VPN) κρυπτογραφεί τη σύνδεσή σου στο διαδίκτυο και δρομολογεί την κίνησή σου μέσω ενός ασφαλούς απομακρυσμένου διακομιστή. Έτσι κρύβεται η δημόσια διεύθυνση IP σου και περιορίζεται τι μπορούν να δουν για την κίνηση που περνά από τη σήραγγα VPN οι παρατηρητές του τοπικού δικτύου και ο ISP σου.

Q2: Γιατί να χρησιμοποιήσω VPN;

Ένα VPN προστατεύει την ψηφιακή σου ιδιωτικότητα, ασφαλίζει τη σύνδεσή σου σε δημόσια δίκτυα Wi-Fi (όπως σε καφετέριες ή αεροδρόμια), μπορεί να μειώσει τον περιορισμό ταχύτητας βάσει δραστηριότητας όταν ο ISP δεν μπορεί να αναγνωρίσει τον τύπο της κρυπτογραφημένης κίνησης, παρακάμπτει γεωγραφικούς περιορισμούς για πρόσβαση σε παγκόσμιο περιεχόμενο και βοηθά στην ασφάλεια των πόρων απομακρυσμένης εργασίας.

Q3: Με κάνει ένα VPN εντελώς ανώνυμο στο διαδίκτυο;

Όχι. Ενώ ένα VPN κρύβει τη διεύθυνση IP σου και κρυπτογραφεί την κίνηση, μπορείς ακόμη να παρακολουθείσαι μέσω cookies του προγράμματος περιήγησης, ενεργών λογαριασμών (όπως Google ή Facebook), fingerprinting του προγράμματος περιήγησης ή αν ο πάροχος του VPN καταγράφει τα δεδομένα σου.

Q4: Θα επιβραδύνει ένα VPN την ταχύτητα του διαδικτύου μου;

Ναι, ελαφρώς. Η διαδικασία κρυπτογράφησης και η φυσική απόσταση από τον διακομιστή VPN προσθέτουν καθυστέρηση και επιβάρυνση. Η επίδραση διαφέρει ανάλογα με τον πάροχο, το πρωτόκολλο, την απόσταση από τον διακομιστή, τη συσκευή και τις συνθήκες του δικτύου.

Q5: Πώς βγάζει χρήματα;

Έλεγξε το επιχειρηματικό μοντέλο. Οι συνδρομές, οι δωρεάν βαθμίδες και οι πωλήσεις δεδομένων επηρεάζουν όλα το πόσο μπορείς να εμπιστευτείς ένα VPN, και μια υπηρεσία που δεν συλλέγει ποτέ τα δεδομένα σου δεν μπορεί να τα πουλήσει. Διάβασε πρώτα την πολιτική απορρήτου. [1]

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Β)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις που έχουν οι υποψήφιοι πελάτες για τη χρήση εικονικών ιδιωτικών δικτύων.

Q6: Μπορώ να χρησιμοποιήσω δωρεάν VPN;

Τα δωρεάν VPN μπορεί να βασίζονται σε διαφημίσεις, περιορισμένες λειτουργίες, αναλύσεις χρήσης, όρια δεδομένων ή άλλα μοντέλα εσόδων. Οι χρήστες πρέπει να ελέγχουν την πολιτική απορρήτου, την ιδιοκτησία, τους ελέγχους και το επιχειρηματικό μοντέλο του παρόχου πριν από τη χρήση.

Q7: Τι είναι η πολιτική «no-logs»;

Η πολιτική μη τήρησης αρχείων καταγραφής περιγράφει ποια δεδομένα δραστηριότητας και σύνδεσης δηλώνει ο πάροχος ότι δεν διατηρεί. Η ακριβής έκταση διαφέρει, γι' αυτό οι αναγνώστες πρέπει να ελέγχουν την πολιτική και τα ευρήματα ανεξάρτητων ελέγχων.

Q8: Πώς επιλέγω το καλύτερο VPN;

Αναζήτησε ελεγμένες πολιτικές μη καταγραφής, ισχυρά πρωτόκολλα (WireGuard, OpenVPN), ασφαλείς τοποθεσίες διακομιστών, γρήγορες ταχύτητες, διακομιστές μόνο RAM, λειτουργία kill switch και δικαιοδοσία εκτός συμμαχιών ανταλλαγής πληροφοριών (όπως οι 5/9/14 Eyes).

Q9: Μπορώ να χρησιμοποιήσω VPN στο κινητό και στην έξυπνη τηλεόρασή μου;

Ναι. Οι σύγχρονοι πάροχοι VPN προσφέρουν ειδικές εφαρμογές για iOS, Android, macOS, Windows, Linux και έξυπνες τηλεοράσεις, καθώς και ρυθμίσεις router για την προστασία όλων των συσκευών του οικιακού σου δικτύου.

Q10: Τι είναι ο Kill Switch;

Ο Kill Switch είναι μια λειτουργία ασφαλείας που αποσυνδέει αυτόματα τη συσκευή σου από το διαδίκτυο αν διακοπεί η σύνδεση VPN. Έτσι αποτρέπεται η διαρροή των μη κρυπτογραφημένων δεδομένων ή της πραγματικής διεύθυνσης IP σου.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε τεχνικές και δομικές πτυχές των εικονικών ιδιωτικών δικτύων και των ασφαλών πρωτοκόλλων τούνελ.

Q1: Ποια είναι η διαφορά μεταξύ WireGuard, OpenVPN και IKEv2;

Το WireGuard είναι ένα σύγχρονο, ελαφρύ πρωτόκολλο (μόλις ~4.000 γραμμές κώδικα) που προσφέρει γρήγορες ταχύτητες και σύντομους χρόνους σύνδεσης. Το OpenVPN είναι ένα εξαιρετικά ασφαλές, δοκιμασμένο στην πράξη πρωτόκολλο ανοιχτού κώδικα. Το IKEv2 είναι εξαιρετικό για κινητές συσκευές χάρη στη δυνατότητά του να επανασυνδέεται γρήγορα όταν αλλάζεις δίκτυο.

Q2: Τι είναι η δρομολόγηση διπλού VPN ή Multi-Hop;

Το Multi-Hop δρομολογεί την κίνησή σου μέσω δύο ή περισσότερων διακομιστών VPN διαδοχικά. Αυτό προσθέτει δεύτερο επίπεδο κρυπτογράφησης και βοηθά να μένει κρυφή η πραγματική σου διεύθυνση IP από τον δεύτερο κόμβο αν παραβιαστεί ένας διακομιστής.

Q3: Τι είναι η διαρροή WebRTC και πώς την αποτρέπει ένα VPN;

Το WebRTC είναι ένα πρωτόκολλο προγράμματος περιήγησης που μπορεί να αποκαλύψει τις πραγματικές τοπικές και δημόσιες διευθύνσεις IP σου ακόμη και όταν το VPN είναι ενεργό. Τα premium VPN μπλοκάρουν ή παραποιούν τα αιτήματα WebRTC στις εφαρμογές για υπολογιστή και κινητό και στις επεκτάσεις προγράμματος περιήγησης.

Q4: Τι είναι οι διακομιστές μόνο με RAM και γιατί έχουν σημασία;

Οι παραδοσιακοί διακομιστές γράφουν δεδομένα σε σκληρούς δίσκους, που μπορούν να κατασχεθούν ή να παραβιαστούν. Οι διακομιστές μόνο RAM (χωρίς δίσκο) λειτουργούν εξ ολοκλήρου σε προσωρινή μνήμη (RAM). Όταν ο διακομιστής επανεκκινείται ή σβήνει, τα δεδομένα στη μνήμη διαγράφονται.

Q5: Πώς παρακάμπτει η παραπλάνηση (obfuscation) τους αποκλεισμούς VPN;

Η συσκότιση (ή «Stealth VPN») μεταμφιέζει τα πακέτα κίνησης VPN ώστε να μοιάζουν με συνηθισμένη κίνηση ιστού HTTPS (θύρα 443). Αυτό βοηθά στην παράκαμψη της Βαθιάς Επιθεώρησης Πακέτων (DPI) που χρησιμοποιούν κυβερνήσεις ή δίκτυα σχολείων/γραφείων για να αποκλείουν τα VPN.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε τεχνικές και δομικές πτυχές των εικονικών ιδιωτικών δικτύων και των ασφαλών πρωτοκόλλων τούνελ.

Q6: Τι είναι το Split Tunneling και πότε πρέπει να το χρησιμοποιήσω;

Το Split Tunneling σου επιτρέπει να επιλέγεις ποιες εφαρμογές δρομολογούνται μέσω του κρυπτογραφημένου τούνελ VPN και ποιες συνδέονται απευθείας στο διαδίκτυο. Χρησιμοποίησέ το για να δρομολογείς ευαίσθητες τραπεζικές εφαρμογές μέσω του VPN, ενώ τα τοπικά παιχνίδια συνδέονται απευθείας, αποφεύγοντας την καθυστέρηση που προσθέτει το VPN.

Q7: Πώς λειτουργεί το προωθητικό απόρρητο (Forward Secrecy / Perfect Forward Secrecy);

Το PFS διασφαλίζει ότι δημιουργείται ένα μοναδικό, προσωρινό κλειδί κρυπτογράφησης για κάθε συνεδρία. Ακόμη και αν ένα ιδιωτικό κλειδί παραβιαστεί στο μέλλον, δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση παλαιότερων ή μελλοντικών συνεδριών, επειδή χρησιμοποίησαν ανεξάρτητα κλειδιά.

Q8: Τι είναι οι συμμαχίες 5/9/14 Eyes και γιατί να με ενδιαφέρουν;

Η δικαιοδοσία μπορεί να επηρεάσει τη νομική διαδικασία που μπορεί να αντιμετωπίσει ένας πάροχος, αλλά ο πρακτικός κίνδυνος για την ιδιωτικότητα εξαρτάται επίσης από τα δεδομένα που διατηρεί ο πάροχος, την τεχνική αρχιτεκτονική, την ιδιοκτησία, την έκδοση εκθέσεων διαφάνειας και το ιστορικό ελέγχων.

Q9: Τι είναι η προστασία από διαρροές DNS;

Η προστασία από διαρροές DNS αναγκάζει τη συσκευή σου να στέλνει τα ερωτήματα αναζήτησης ιστοτόπων (ερωτήματα DNS) μέσω των ιδιωτικών, κρυπτογραφημένων διακομιστών DNS του VPN αντί για τους διακομιστές του παρόχου internet σου. Έτσι ο πάροχος δεν μπορεί να παρακολουθεί ποιους ιστοτόπους επισκέπτεσαι.

Q10: Γιατί να ελέγχεις ποιος διαχειρίζεται και υποστηρίζει ένα VPN;

Η φήμη έχει σημασία. Ερεύνησε τους ιδιοκτήτες και τους ηγέτες της εταιρείας, αναζήτησε δημόσιους ελέγχους από τρίτους και δες τι λένε ανεξάρτητοι ειδικοί ασφαλείας και ο Τύπος προτού την εμπιστευτείς. [1]

Μέρος 11: 10 ενδιαφέροντα στοιχεία και πραγματικές διαπιστώσεις για τα VPN

Εξέτασε αυτά τα πολύτιμα, πραγματικά στοιχεία και πληροφορίες για την ιστορία, την αγορά και την τεχνολογία των VPN.

1. ΤΟ ΠΡΩΤΟ ΠΡΩΤΟΚΟΛΛΟ VPN

Το PPTP (Point-to-Point Tunneling Protocol), ένα πρώιμο πρωτόκολλο VPN από ομάδα υπό την ηγεσία της Microsoft τη δεκαετία του 1990, θεωρείται πλέον ανασφαλές, γι' αυτό τα σύγχρονα VPN χρησιμοποιούν WireGuard ή OpenVPN. [1]

2. ΑΠΟΤΙΜΗΣΗ ΑΓΟΡΑΣ

Η παγκόσμια αγορά VPN έχει γνωρίσει ταχεία ανάπτυξη, την οποία τροφοδοτούν οι αυξανόμενες ανάγκες τηλεργασίας και οι απαιτήσεις ασφάλειας των επιχειρήσεων.

3. Η ΕΠΑΝΑΣΤΑΣΗ ΤΟΥ WIREGUARD

Το WireGuard διαθέτει μια εξαιρετικά απλοποιημένη βάση κώδικα, σχεδιασμένη για αποδοτικότητα, που την κάνει ευκολότερη στον έλεγχο για ευπάθειες ασφαλείας από τα παραδοσιακά πρωτόκολλα. [3]

4. ΑΥΣΤΗΡΑ ΠΡΟΤΥΠΑ ΕΛΕΓΧΟΥ

Οι κορυφαίοι πάροχοι VPN προσλαμβάνουν εταιρείες όπως η Deloitte, η KPMG ή η PwC για να ελέγξουν τους ισχυρισμούς μη καταγραφής, και εταιρείες ασφάλειας όπως η Cure53 για να δοκιμάσουν τις εφαρμογές και τους διακομιστές τους. [4]

5. ΟΙ ΑΡΧΕΣ ΤΗΣ ΣΥΜΜΑΧΙΑΣ 5-EYES

Η συνεργασία πληροφοριών Five Eyes των ΗΠΑ, του Ηνωμένου Βασιλείου, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας προέκυψε από τη συνεργασία των Συμμάχων στις πληροφορίες σημάτων την εποχή του Β΄ Παγκοσμίου Πολέμου.

6. ΑΝΑΛΥΣΗ ΒΑΘΟΥΣ ΠΑΚΕΤΩΝ

Τα προηγμένα τείχη προστασίας χρησιμοποιούν Deep Packet Inspection (DPI) για να αναλύουν τα μεταδεδομένα των πακέτων δικτύου και να αποκλείουν τα τυπικά χαρακτηριστικά συνδέσεων VPN.

7. ΕΤΑΙΡΙΚΗ ΧΡΗΣΗ

Πολλοί οργανισμοί δίνουν στους απομακρυσμένους υπαλλήλους ένα VPN για πρόσβαση σε εσωτερικά συστήματα όπως βάσεις δεδομένων, κάτι που κάνει τα VPN συνηθισμένο εργαλείο ασφάλειας στον χώρο εργασίας.

8. ΑΠΟΚΕΝΤΡΩΜΕΝΑ VPN

Τα αποκεντρωμένα VPN (dVPN) διανέμουν την κίνηση σε ένα δίκτυο κόμβων που τρέχουν οι ίδιοι οι χρήστες, μειώνοντας την εξάρτηση από έναν μόνο συγκεντρωτικό πάροχο.

9. ΑΝΩΝΥΜΙΑ TOR ΕΝΑΝΤΙ VPN

Ένα VPN περνά την κίνηση μέσω ενός μόνο παρόχου, ενώ το Tor (The Onion Router) τη στέλνει μέσω τριών εθελοντικών αναμεταδοτών (guard, middle, exit) για μέγιστη ιδιωτικότητα. [5]

10. ΚΟΣΤΟΣ ΤΩΝ ΠΑΡΑΒΙΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ

Ο συνδυασμός ενός VPN με ένα μοντέλο πρόσβασης zero trust, που ελέγχει κάθε χρήστη και συσκευή, βοηθά τους οργανισμούς να προστατεύουν δεδομένα και να περιορίζουν τη ζημιά από παραβιάσεις δεδομένων.

Τεχνικές αναφορές και πηγές

Παρατιθέμενες δημοσιεύσεις, κρυπτογραφικές προδιαγραφές και επίσημα πρότυπα εγγράφων που χρησιμοποιούνται σε αυτό το φύλλο εργασίας.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.

https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

Λύσεις: Αξιολόγηση παρόχων VPN, προτύπων ασφάλειας, ελέγχων και πολιτικών καταγραφής

1 **Πολιτική καταγραφών με έλεγχο** ΠΡΩΤΟΚΟΛΛΑ

Σωστή απάντηση: B

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Μια πολιτική μη τήρησης αρχείων καταγραφής που ελέγχεται από ανεξάρτητους φορείς είναι ο πιο πρακτικός τρόπος να ελεγχθούν οι ισχυρισμοί ιδιωτικότητας μηδενικής γνώσης ενός παρόχου. Το εντυπωσιακό μάρκετινγκ ή οι αυτοδηλώσεις δεν επαρκούν. Παραπομπή: Deloitte Advisory, Cure53 Audit.

2 **Υπεροχή του WireGuard** ΚΑΘΥΣΤΕΡΗΣΗ

Σωστή απάντηση: D

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard προσφέρει σύγχρονη, γρήγορη δρομολόγηση συνδέσεων στον χώρο πυρήνα με συμπαγή βάση κώδικα (~4.000 γραμμές), κάνοντας τους ελέγχους ιδιαίτερα αποδοτικούς. Παραπομπή: IETF Protocol RFC, WireGuard Project.

3 **Ερώτηση 3**

Σωστή απάντηση: B

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα δωρεάν VPN πληρώνουν κι αυτά για διακομιστές, και η FTC προειδοποιεί ότι ορισμένες εφαρμογές VPN μοιράζονται δεδομένα χρηστών με τρίτους, για παράδειγμα για να προβάλλουν διαφημίσεις.

4 **Νομικές δικαιοδοσίες** ΕΛΕΓΧΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ

Σωστή απάντηση: C

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η δικαιοδοσία καθορίζει αν το VPN υπόκειται σε νόμους παρακολούθησης, τοπικές υποχρεώσεις διατήρησης δεδομένων και μυστικά κυβερνητικά εντάλματα κλήτευσης. Παραπομπή: Privacy Rights Clearinghouse.

5 **Προστασία Kill Switch** ΙΔΙΩΤΙΚΟΤΗΤΑ

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το kill switch διακόπτει αμέσως τη δρομολόγηση του προσαρμογέα δικτύου του συστήματος αν διακοπεί η σήραγγα, αποτρέποντας διαρροές έκθεσης της πραγματικής IP και του DNS. Παραπομπή: IETF Tunnel RFC.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Περιορισμοί του κακόβουλου λογισμικού** ΑΠΟΚΡΥΨΗ IP — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα VPN παρέχει έναν ασφαλή κρυπτογραφημένο αγωγό, αλλά δεν σαρώνει φορτία ή αρχεία. Απαιτείται λογισμικό antivirus για τον αποκλεισμό κακόβουλου λογισμικού. Παραπομπή: Deloitte Advisory.

7 **Ανεξάρτητος έλεγχος** ΤΑΧΥΤΗΤΕΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι εκθέσεις ελέγχου επαληθεύουν τις ρυθμίσεις του λογισμικού διακομιστών, τη συμμόρφωση με τη ρύθμιση μόνο RAM και την απουσία βάσεων δεδομένων καταγραφής. Παραπομπή: Deloitte Advisory, Cure53 Audit.

8 **Ερώτηση 8** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι πάροχοι πρέπει να ακολουθούν τους νόμους της χώρας τους, οι οποίοι μπορεί να περιλαμβάνουν κανόνες διατήρησης δεδομένων και εντολές παράδοσης των δεδομένων που διατηρούν.

9 **Μέγεθος βάσης κώδικα πρωτοκόλλου** ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Μια μικρότερη βάση κώδικα μειώνει την πιθανή επιφάνεια επίθεσης και διευκολύνει τις ομάδες ασφαλείας να επαληθεύσουν την ακεραιότητα του πρωτοκόλλου. Παραπομπή: WireGuard Project.

10 **Χρηματοποίηση διαφημίσεων** ΧΩΡΙΣ ΚΑΤΑΓΡΑΦΗ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Χωρίς συνδρομητικές χρεώσεις, τα δωρεάν VPN βασίζονται στην εξόρυξη δεδομένων, στη δημιουργία προφίλ κίνησης και στην ένθεση διαφημίσεων στο πρόγραμμα περιήγησης για να παράγουν έσοδα. Παραπομπή: EDRi Retention Guidelines.

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. WireGuard	H 2. Ελεγμένα αρχεία καταγραφής	E 3. Δικαιοδοσία	B 4. Kill switch
C 5. Five Eyes	A 6. Δωρεάν VPN	D 7. Διακομιστές μόνο RAM	G 8. OpenVPN

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΜΗ ΚΑΤΑΓΡΑΦΗ	2 WIREGUARD	3 ΔΙΑΚΟΠΤΗΣ	4 ΔΙΚΑΙΟΔΟΣΙΑ
5 ΜΟΝΟ ΜΝΗΜΗ	6 ΕΛΕΓΧΟΣ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 Ε – ΠΕΝΤΕΜΑΤΙΑ	2 Α – ΠΡΩΤΟΚΟΛΛΟ	3 Η – ΣΗΡΑΓΓΑ	4 F – ΔΩΡΕΑΝ
5 D – ΔΙΑΚΟΠΤΗΣ	6 G – ΜΟΝΟΜΝΗΜΗ	7 C – ΔΙΚΑΙΟΔΟΣΙΑ	8 Β – ΕΛΕΓΜΕΝΟ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους WireGuard, Ελεγμένα αρχεία καταγραφής και Δικαιοδοσία 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.

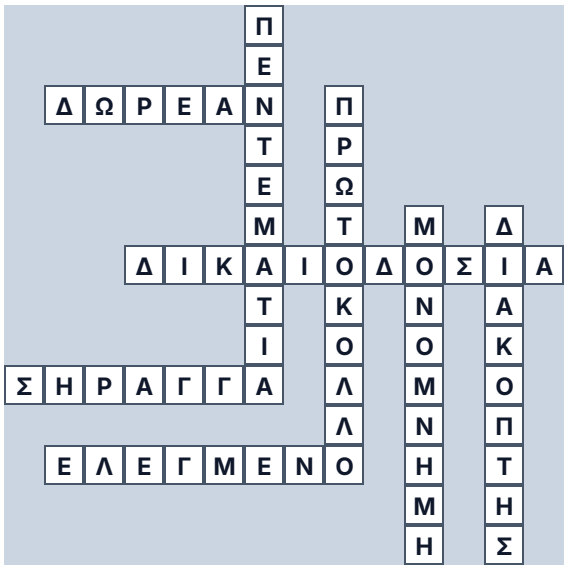
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: ΔΩΡΕΑΝ Υπηρεσία σύνδεσης υψηλού κινδύνου που συχνά βγάζει χρήματα καταγράφοντας και πουλώντας δεδομένα περιήγησης (6 γράμματα)

6 οριζόντια: ΔΙΚΑΙΟΔΟΣΙΑ Η γεωγραφική περιοχή που καθορίζει τις νομικές υποχρεώσεις του παρόχου VPN (11 γράμματα)

7 οριζόντια: ΣΗΡΑΓΓΑ Κρυπτογραφημένος δίαυλος ανοιχτού κώδικα, ώριμος και ευρέως ελεγμένος, με πολύ μεγαλύτερη βάση κώδικα από το WireGuard (7 γράμματα)

8 οριζόντια: ΕΛΕΓΜΕΝΟ Ισχυρισμός απορρήτου που έχει επαληθευτεί από ανεξάρτητες εταιρείες κυβερνοασφάλειας (8 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΠΕΝΤΕΜΑΤΙΑ Διεθνής συμμαχία ανταλλαγής πληροφοριών μεταξύ ΗΠΑ, ΗΒ, Καναδά, Αυστραλίας και Νέας Ζηλανδίας (10 γράμματα)

3 κάθετα: ΠΡΩΤΟΚΟΛΛΟ Σύγχρονο, γρήγορο σύνολο κανόνων με περίπου 4.000 γραμμές εύκολα ελέγξιμου κώδικα (10 γράμματα)

4 κάθετα: ΜΟΝΟΜΝΗΜΗ Υποδομή υλικού που λειτουργεί εξ ολοκλήρου σε προσωρινή μνήμη και δεν αποθηκεύει δεδομένα (9 γράμματα)

5 κάθετα: ΔΙΑΚΟΠΤΗΣ Μηχανισμός ασφαλείας που μπλοκάρει τη δρομολόγηση του διαδικτύου αν διακοπεί η ασφαλής σήραγγα (9 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΛΟΚΟΡΠΛΟΤΩ — **ΠΡΩΤΟΚΟΛΛΟ**
2. ΙΑΙΔΙΟΚΣΟΔΑ — **ΔΙΚΑΙΟΔΟΣΙΑ**
3. ΠΜΙΑΕΕΑΤΤΝ — **ΠΕΝΤΕΜΑΤΙΑ**
4. ΜΗΜΟΗΝΜΟΝ — **ΜΟΝΟΜΝΗΜΗ**
5. ΜΕΛΟΓΕΝΕ — **ΕΛΕΓΜΕΝΟ**
6. ΗΚΙΤΠΔΟΣΑ — **ΔΙΑΚΟΠΤΗΣ**
7. ΑΔΕΝΡΩ — **ΔΩΡΕΑΝ**
8. ΗΑΑΣΓΓΡ — **ΣΗΡΑΓΓΑ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΣΥΓΚΡΙΝΕ ΤΙΣ ΑΝΑΦΟΡΕΣ ΣΟΥ ΜΕ ΕΝΑ ΑΣΦΑΛΕΣ ΣΥΣΤΗΜΑ"

Λύσεις των μελετών περίπτωσης

A Σενάριο Α: Ασφάλεια δημόσιου δικτύου

ΥΠΟΚΛΟΠΗ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Το δίλημμα της Sarah

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Κίνδυνοι: Υποκλοπή πακέτων, υποκλοπή δεδομένων και επιθέσεις man-in-the-middle. Κάποιος στο ίδιο δίκτυο του καφέ θα μπορούσε να καταγράψει τα στοιχεία σύνδεσής της ή το αρχείο της εργασίας της.
- Προστασία VPN: Κρυπτογραφεί τα φορτία των πακέτων δικτύου, καθιστώντας την υποκλαπείσα κίνηση της σήραγγας μη αναγνώσιμη σε παθητικούς κατασκόπους τοπικού δικτύου όταν το VPN έχει ρυθμιστεί σωστά.

B Σενάριο Β: Πρόσβαση σε αποκλεισμένους πόρους

ΓΕΩΓΡΑΦΙΚΟΣ ΑΠΟΚΛΕΙΣΜΟΣ ΚΑΙ IP

Το δίλημμα του Alex

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Γιατί μπλοκαρίστηκε: Ο διακομιστής streaming χρησιμοποιεί γεωγραφικό αποκλεισμό, που αντιστοιχίζει την τοπική διεύθυνση IP του ταξιδιώτη με τη φυσική του χώρα και την μπλοκάρει βάσει εδαφικών αδειών χρήσης.
- Πώς βοηθά το VPN: Συγκαλύπτει την πραγματική του τοποθεσία δρομολογώντας την κίνηση μέσω διακομιστή στη χώρα του. Ο ιστότοπος βλέπει την IP της χώρας του, επιτρέποντας την πρόσβαση.