Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Οδηγός VPN του VPN.com Φύλλο εργασίας

Πρακτικές ασκήσεις σε πρωτόκολλα δικτύου, τούνελ και ελέγχους ασφαλείας.

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

- Εξήγησε την έννοια του data tunneling και της ενθυλάκωσης.
- Αναγνώρισε τις τυπικές ρυθμίσεις πρωτοκόλλων και τις απαιτήσεις εύρους ζώνης.
- Ανάλυσε τους ρόλους των τειχών προστασίας και των γεωγραφικών αποκλεισμών στη δρομολόγηση του διαδικτύου.
- Κατανόησε πώς οι πάροχοι διαδικτύου παρακολουθούν τη μη κρυπτογραφημένη περιήγηση και πώς το VPN το αποτρέπει.
- Διέκρινε τα επιχειρησιακά όρια της τοποθεσίας διακομιστή και της δικαιοδοσίας.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ VPN

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 σε πραγματικά σενάρια στην ενότητα μελετών περίπτωσης. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΤΙ ΕΙΝΑΙ ΤΟ VPN; (ΕΙΣΑΓΩΓΗ)

Ένα εικονικό ιδιωτικό δίκτυο είναι κάτι περισσότερο από έναν διακόπτη ιδιωτικότητας. Είναι μια κρυπτογραφημένη σήραγγα που δρομολογεί την κίνησή σου στο διαδίκτυο μέσω ενός απομακρυσμένου διακομιστή. Αυτό κρύβει τη διεύθυνση IP σου, εμποδίζει τον ISP σου να καταρτίζει αρχεία καταγραφής των διαδικτυακών σου ενεργειών και ασφαλίζει τα δεδομένα σου σε δημόσια δίκτυα. Η κατανόηση της ορολογίας είναι απαραίτητη για τη διατήρηση της ψηφιακής ασφάλειας.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. Τι είναι ένα πρωτόκολλο VPN;

- A. Μια συσκευή υλικού που χρησιμοποιείται για τη σύνδεση καλωδίων.
- B. Ένα σύνολο κανόνων που ορίζει πώς κρυπτογραφούνται και αποστέλλονται τα δεδομένα.
- C. Ένα πρόσθετο προγράμματος περιήγησης που αποκλείει τις διαφημίσεις.
- D. Μια εταιρεία παρόχου υπηρεσιών διαδικτύου.

2. Αν η σύνδεση VPN σου φαίνεται αργή, ποια είναι η πιθανότερη αιτία;

- A. Ο διακομιστής VPN είναι πολύ μακριά ή υπερφορτωμένος.
- B. Η ανάλυση της οθόνης σου έχει οριστεί πολύ υψηλή.
- C. Έχεις απενεργοποιήσει τα cookies του προγράμματος περιήγησης.
- D. Η διάταξη του πληκτρολογίου σου έχει ρυθμιστεί λανθασμένα.

3. Γιατί συνιστάται ιδιαίτερα ένα VPN όταν συνδέεσαι σε δημόσιο Wi-Fi;

- A. Κάνει τη σύνδεση Wi-Fi δωρεάν.
- B. Αυξάνει την εμβέλεια του δρομολογητή.
- C. Κρυπτογραφεί την κίνηση για να εμποδίσει τους χάκερ στο ίδιο δίκτυο.
- D. Διαγράφει αυτόματα τα ανεπιθύμητα email.

4. Ποιο από τα παρακάτω περιγράφει έναν γεωγραφικό αποκλεισμό (geoblock);

- A. Ένα εργαλείο που μετρά τη φυσική απόσταση από έναν διακομιστή.
- B. Ένας περιορισμός που αποκλείει την πρόσβαση σε έναν ιστότοπο βάσει τοποθεσίας.
- C. Ένα πρωτόκολλο για τοπική συμπίεση αρχείων.
- D. Ένας μηχανισμός αποθήκευσης αντιγράφων ασφαλείας.

5. Τι μπορεί να δει ο πάροχος υπηρεσιών διαδικτύου (ISP) σου όταν χρησιμοποιείς ένα VPN;

- A. Λέξεις-κλειδιά αναζήτησης και περιεχόμενο ιστοσελίδων που βλέπεις.
- B. Ότι είσαι συνδεδεμένος σε VPN, αλλά όχι τις λεπτομέρειες της κίνησης.
- C. Καμία πληροφορία, ούτε καν ότι είσαι συνδεδεμένος στο διαδίκτυο.
- D. Τα αρχεία και οι φωτογραφίες σου στον τοπικό σκληρό δίσκο.

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Απόκρυψη τοποθεσίας

6. Ένα VPN κρύβει τη δημόσια διεύθυνση IP της συσκευής σου, εμποδίζοντας τους ιστότοπους τρίτων να εντοπίζουν εύκολα τη φυσική σου τοποθεσία.

Σωστό Λάθος

7 Επίδραση του VPN στην ταχύτητα

7. Η ενεργοποίηση μιας σύνδεσης VPN κάνει την βασική ταχύτητα internet σου διπλάσια σε σχέση με τη σύνδεση χωρίς VPN.

Σωστό Λάθος

8 Υποκλοπή σε δημόσιο Wi-Fi

8. Αν χρησιμοποιείς ένα μη ασφαλές δημόσιο δίκτυο Wi-Fi χωρίς VPN, άλλοι χρήστες στο ίδιο δίκτυο μπορούν ενδεχομένως να καταγράψουν τη μη κρυπτογραφημένη κίνησή σου.

Σωστό Λάθος

9 Τείχη προστασίας και αποκλεισμένες συνδέσεις

9. Οι διαχειριστές δικτύου μπορούν να ρυθμίσουν τα τείχη προστασίας ώστε να εντοπίζουν και να αποκλείουν τις εξερχόμενες σήραγγες σύνδεσης VPN.

Σωστό Λάθος

10 Αυστηρές πολιτικές μηδενικής καταγραφής

10. Μια αυστηρή πολιτική «μη τήρησης αρχείων καταγραφής» σημαίνει ότι ο πάροχος VPN υποχρεούται νομικά να αποθηκεύει τα ερωτήματα αναζήτησης και τους συνδέσμους που επισκέφτηκες για τουλάχιστον 30 ημέρες.

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. Για να ασφαλίσει την κίνησή σου, το VPN τυλίγει τα πακέτα δεδομένων σου μέσα σε άλλο πρωτόκολλο, μια διαδικασία γνωστή ως _____ .

2. Αν παρατηρείς αργές ταχύτητες λήψης κατά το streaming, ίσως οφείλεται στο περιορισμένο _____ του δικτύου.

3. Ο _____ είναι ο περιορισμός που εφαρμόζει μια υπηρεσία streaming διαθέσιμη μόνο σε μια συγκεκριμένη χώρα για να αποκλείει τους χρήστες άλλων περιοχών.

4. Οι κανόνες σύνδεσης που ορίζουν τις παραμέτρους κρυπτογράφησης και σύνδεσης ονομάζονται _____ του VPN.

5. Ο υπολογιστής σου χρησιμοποιεί ένα τοπικό _____ προστασίας για να παρακολουθεί την κίνηση δικτύου και να μπλοκάρει μη ασφαλείς συνδέσεις.

6. Όταν συνδέεσαι σε VPN, ο απομακρυσμένος _____ δρομολογεί τα δεδομένα σου και κρύβει τη δημόσια IP σου.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΠΟΡΡΗΤΟ ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ ΔΙΑΚΟΜΙΣΤΗΣ ΕΥΡΟΣ ΖΩΝΗΣ ΠΑΡΟΧΟΣ
ΠΡΩΤΟΚΟΛΛΟ ΣΗΡΑΓΓΟΠΟΙΗΣΗ ΤΕΙΧΟΣ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών δικτύου

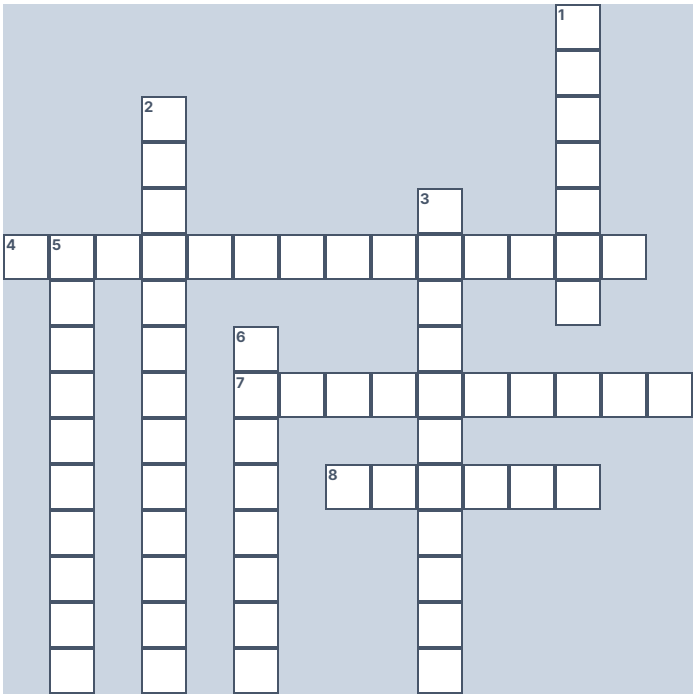
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. Τούνελ	A	Ένα σύνολο κανόνων που καθορίζουν πώς μεταδίδονται τα δεδομένα στο δίκτυο.
☐	2. Πρωτόκολλο	B	Ο μέγιστος ρυθμός μεταφοράς δεδομένων μέσω μιας σύνδεσης.
☐	3. Εύρος ζώνης	C	Ένας περιορισμός που εμποδίζει την πρόσβαση στον ιστό βάσει φυσικής τοποθεσίας.
☐	4. Διακομιστής	D	Ένα σύστημα ασφαλείας που παρακολουθεί και αποκλείει τη μη εξουσιοδοτημένη κίνηση.
☐	5. Γεωγραφικός αποκλεισμός (geoblock)	E	Ένας απομακρυσμένος υπολογιστής που δρομολογεί την κίνησή σου και κρύβει την IP σου.
☐	6. Τείχος προστασίας	F	Η κατάσταση του να είσαι ελεύθερος από ιχνηλάτηση ή δημόσια επιτήρηση.
☐	7. Ιδιωτικότητα	G	Πάροχος υπηρεσιών διαδικτύου που μεταφέρει την κίνησή σου και μπορεί να βλέπει τη μη κρυπτογραφημένη δραστηριότητα.
☐	8. ISP	H	Περιτύλιξη πακέτων δεδομένων μέσα σε ένα άλλο πακέτο για ασφαλή μετάδοση.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

4. Περιορισμός που εμποδίζει την πρόσβαση στον ιστό ανάλογα με τη φυσική τοποθεσία (14)

7. Σύνολο κανόνων που καθορίζει πώς μεταδίδονται τα δεδομένα στο δίκτυο (10)

8. Σύστημα ασφαλείας που παρακολουθεί και μπλοκάρει την μη εξουσιοδοτημένη κίνηση (τείχος προστασίας) (6)

ΚΑΘΕΤΑ

1. Ο πάροχος υπηρεσιών διαδικτύου (ISP), που καταγράφει την κίνησή σου αν δεν είναι κρυπτογραφημένη (7)

2. Τύλιγμα των πακέτων δεδομένων μέσα σε άλλο πακέτο για ασφαλή μετάδοση (13)

3. Ένας απομακρυσμένος υπολογιστής που δρομολογεί την κίνησή σου και κρύβει την IP σου (11)

5. Ο μέγιστος ρυθμός μεταφοράς δεδομένων μέσω μιας σύνδεσης (10)

6. Η κατάσταση του να είσαι απαλλαγμένος από παρακολούθηση ή δημόσια επιτήρηση (8)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

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

ΟΡΙΖΟΝΤΙΑ

4 οριζόντια: Περιορισμός που εμποδίζει την πρόσβαση στον ιστό ανάλογα με τη φυσική τοποθεσία (14 γράμματα):

7 οριζόντια: Σύνολο κανόνων που καθορίζει πώς μεταδίδονται τα δεδομένα στο δίκτυο (10 γράμματα):

8 οριζόντια: Σύστημα ασφαλείας που παρακολουθεί και μπλοκάρει την μη εξουσιοδοτημένη κίνηση (τείχος προστασίας) (6 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Ο πάροχος υπηρεσιών διαδικτύου (ISP), που καταγράφει την κίνησή σου αν δεν είναι κρυπτογραφημένη (7 γράμματα):

2 κάθετα: Τύλιγμα των πακέτων δεδομένων μέσα σε άλλο πακέτο για ασφαλή μετάδοση (13 γράμματα):

3 κάθετα: Ένας απομακρυσμένος υπολογιστής που δρομολογεί την κίνησή σου και κρύβει την IP σου (11 γράμματα):

5 κάθετα: Ο μέγιστος ρυθμός μεταφοράς δεδομένων μέσω μιας σύνδεσης (10 γράμματα):

6 κάθετα: Η κατάσταση του να είσαι απαλλαγμένος από παρακολούθηση ή δημόσια επιτήρηση (8 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

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

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

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΣΗΡΑΓΓΟΠΟΙΗΣΗ ΠΡΩΤΟΚΟΛΛΟ ΕΥΡΟΖΩΝΗΣ ΔΙΑΚΟΜΙΣΤΗΣ ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ
ΤΕΙΧΟΣ ΑΠΟΡΡΗΤΟ ΠΑΡΟΧΟΣ

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. ΣΗΡΑΓΓΟΠΟΙΗΣΗ**
- **B. ΠΡΩΤΟΚΟΛΛΟ**
- **C. ΕΥΡΟΣΖΩΝΗΣ**
- **D. ΔΙΑΚΟΜΙΣΤΗΣ**
- **E. ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ**
- **F. ΤΕΙΧΟΣ**
- **G. ΑΠΟΡΡΗΤΟ**
- **H. ΠΑΡΟΧΟΣ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Η κατάσταση του να είσαι απαλλαγμένος από παρακολούθηση ή δημόσια επιτήρηση.
2. Περιορισμός που εμποδίζει την πρόσβαση στον ιστό ανάλογα με τη φυσική τοποθεσία.
3. Σύνολο κανόνων που καθορίζει πώς μεταδίδονται τα δεδομένα στο δίκτυο.
4. Σύστημα ασφαλείας που παρακολουθεί και μπλοκάρει την μη εξουσιοδοτημένη κίνηση (τείχος προστασίας).
5. Ο μέγιστος ρυθμός μεταφοράς δεδομένων μέσω μιας σύνδεσης.
6. Ένας απομακρυσμένος υπολογιστής που δρομολογεί την κίνησή σου και κρύβει την IP σου.
7. Ο πάροχος υπηρεσιών διαδικτύου (ISP), που καταγράφει την κίνησή σου αν δεν είναι κρυπτογραφημένη.
8. Τύλιγμα των πακέτων δεδομένων μέσα σε άλλο πακέτο για ασφαλή μετάδοση.

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. ΟΡΟΣΓΗΠΙΣΗΗΓΑ
2. ΗΟΕΥΣΣΩΝΖΡ
3. ΓΕΕΟΛΣΙΣΩΚΠΟΜΑ
4. ΡΤΟΗΡΑΠΟ
5. ΛΚΟΡΤΟΟΠΛΩ
6. ΟΣΜΣΗΤΔΙΙΑΚ
7. ΟΤΧΣΙΕ
8. ΑΟΣΠΟΧΡ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πράγματα που συνδέεις με τη λέξη «τούνελ»			
2	Πράγματα που θα δίδασκες στην οικογένειά σου για τα VPN			
3	Πράγματα σε έναν ιστότοπο που μπορούν να σε παρακολουθήσουν			
4	Μύθοι για τα VPN			
5	Λέξεις από αυτό το φύλλο εργασίας που θέλεις να θυμάσαι			
6	Συσκευές που μπορούν να χρησιμοποιήσουν VPN			
7	Πράγματα από τα οποία ένα VPN δεν μπορεί να σε προστατεύσει			
8	Χώρες που θα ήθελες να «επισκεφτείς» διαδικτυακά			
9	Υποσχέσεις που δίνει ένας καλός πάροχος VPN			
10	Τρόποι να εντοπίσεις ένα ψεύτικο δίκτυο Wi-Fi			
11	Ερωτήσεις που έχεις για τα VPN			
12	Υπηρεσίες VPN που γνωρίζεις			
13	Λέξεις που σχετίζονται με το απόρρητο			
14	Πράγματα που ένα VPN μπορεί να κρύψει			
15	Λόγοι για να χρησιμοποιείς VPN σε ένα καφέ			

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

Ένα VPN κρυπτογραφεί την κίνησή σου για να την ασφαλίσει. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα κυβερνοασφάλειας 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	15
1	16	15	17	17	7	19	15	18	15	20	12	5
1	18	21	1	11	7	18	7	17	1	3	3	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: Είναι νόμιμη η χρήση VPN;

Η χρήση VPN είναι νόμιμη σε πολλές χώρες, αλλά ορισμένες δικαιοδοσίες περιορίζουν, ρυθμίζουν ή αποκλείουν υπηρεσίες VPN. Οι χρήστες πρέπει να επαληθεύουν τους ισχύοντες τοπικούς νόμους πριν από τη χρήση. Για περισσότερες λεπτομέρειες, συμβουλεύσου τους οδηγούς νομιμότητας στο VPN.com.

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. [3]

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 την κίνηση VPN ώστε να μοιάζει με συνηθισμένη κίνηση HTTPS (θύρα 443). Αυτό μπορεί να βοηθήσει 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: Μπορεί ένα VPN να παρακάμψει τον περιορισμό ταχύτητας του πάροχου ίντερνετ;

Μερικές φορές. Ένα VPN μπορεί να βοηθήσει όταν ένας πάροχος διαδικτύου επιβραδύνει επιλεκτικά αναγνωρίσιμες δραστηριότητες, αλλά δεν θα ξεπεράσει τη συμφόρηση, τα όρια δεδομένων, τα όρια ταχύτητας σε επίπεδο λογαριασμού ή την κακή ποιότητα δικτύου.

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) αναπτύχθηκε από ομάδα προμηθευτών που περιλάμβανε τη Microsoft και δημοσιεύθηκε ως RFC 2637 τον Ιούλιο του 1999 για την υποστήριξη VPN απομακρυσμένης πρόσβασης. [6]

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 εξωτερικούς ελεγκτές (όπως η Cure53 ή η PwC) για ανεξάρτητους ελέγχους κώδικα και για να επαληθεύσουν ότι δεν καταγράφουν καμία δραστηριότητα των χρηστών.

5. ΟΙ ΑΡΧΕΣ ΤΗΣ ΣΥΜΜΑΧΙΑΣ 5-EYES

Η συμμαχία Five Eyes προέκυψε από τη συμφωνία πληροφοριών σημάτων UKUSA του 1946 μεταξύ ΗΠΑ και Ηνωμένου Βασιλείου, στην οποία αργότερα προστέθηκαν ο Καναδάς, η Αυστραλία και η Νέα Ζηλανδία.

6. ΑΝΑΛΥΣΗ ΒΑΘΟΥΣ ΠΑΚΕΤΩΝ

Η βαθιά επιθεώρηση πακέτων (DPI) εξετάζει το περιεχόμενο των πακέτων και τα μοτίβα κίνησης, όχι μόνο τις κεφαλίδες, και ορισμένα τείχη προστασίας τη χρησιμοποιούν για να εντοπίζουν και να αποκλείουν συνηθισμένα πρωτόκολλα VPN.

7. ΕΤΑΙΡΙΚΗ ΧΡΗΣΗ

Μεγάλο ποσοστό των εταιρικών υπαλλήλων παγκοσμίως χρησιμοποιεί ασφαλή VPN για να συνδέεται σε εσωτερικές βάσεις δεδομένων, γεγονός που το καθιστά βασικό πρότυπο ασφαλείας.

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 και exit), ώστε κανένας μεμονωμένος αναμεταδότης να μη γνωρίζει και τα δύο άκρα.

10. ΚΟΣΤΟΣ ΤΩΝ ΠΑΡΑΒΙΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ

Η χρήση ενός μοντέλου ασφαλούς πρόσβασης μηδενικής εμπιστοσύνης με VPN βοηθά τους οργανισμούς να προστατεύουν την πνευματική ιδιοκτησία και να μετριάζουν τις οικονομικές επιπτώσεις των παραβιάσεων δεδομένων.

Τεχνικές αναφορές και πηγές

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

ΑΚΑΔΗΜΑΪΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ ΚΑΙ ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ

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

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.

https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

ΣΥΝΟΨΗ ΤΕΧΝΙΚΩΝ ΠΡΟΤΥΠΩΝ

- Πρότυπα ενθυλάκωσης: Το RFC 4301 ορίζει την ασφαλή δρομολόγηση πακέτων internet IPsec/L2TP.
- Παρακολούθηση από τον ISP: Η δρομολόγηση των ερωτημάτων DNS μέσω της κρυπτογραφημένης σήραγγας VPN μπορεί να μειώσει την ορατότητα του DNS στον τοπικό ISP.
- Πρωτόκολλα ελέγχου τείχους προστασίας: Τα πακέτα stealth με απόκρυψη παρακάμπτουν τα φίλτρα βαθιάς επιθεώρησης πακέτων.

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: B

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα πρωτόκολλο VPN ορίζει τους κανόνες για τη δημιουργία του τούνελ και την κρυπτογράφηση των δεδομένων· οι άλλες επιλογές περιγράφουν καλώδια, προγράμματα αποκλεισμού διαφημίσεων και παρόχους internet.

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η απόσταση προσθέτει latency και ένας υπερφορτωμένος διακομιστής έχει λιγότερη χωρητικότητα να μοιράσει· η ανάλυση οθόνης, τα cookies και η διάταξη πληκτρολογίου δεν επηρεάζουν την ταχύτητα σύνδεσης.

3 Ερώτηση 3

Σωστή απάντηση: C

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Στα ανοιχτά δίκτυα άλλοι μπορούν να υποκλέψουν μη κρυπτογραφημένα πακέτα· ένα VPN κρυπτογραφεί την κίνηση ώστε τα δεδομένα που υποκλέπτονται να μη διαβάζονται.

4 Ερώτηση 4

Σωστή απάντηση: B

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο γεωγραφικός αποκλεισμός αντιστοιχίζει τη δημόσια διεύθυνση IP ενός επισκέπτη σε βάση δεδομένων τοποθεσιών και απαγορεύει την πρόσβαση εκτός των επιτρεπόμενων περιοχών.

5 Ερώτηση 5

Σωστή απάντηση: B

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο πάροχος internet μπορεί να δει ότι στέλνεις κρυπτογραφημένα δεδομένα σε διακομιστή VPN, αλλά όχι ποιους ιστότοπους επισκέπτεσαι ή τι αναζητάς.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι ιστότοποι βλέπουν τη διεύθυνση IP του διακομιστή VPN αντί για τη δική σου, κάτι που κρύβει από αυτούς την ενδεικτική τοποθεσία σου.

7 Ερώτηση 7

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η κρυπτογράφηση και η επιπλέον αναπήδηση προς τον διακομιστή VPN συνήθως μειώνουν ελαφρά την ταχύτητα· ένα VPN δεν μπορεί να διπλασιάσει τη βασική ταχύτητα της σύνδεσής σου.

8 Ερώτηση 8

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Στο μη ασφαλές Wi-Fi, εργαλεία παρακολούθησης πακέτων μπορούν να συλλάβουν μη κρυπτογραφημένη κίνηση, όπως στοιχεία σύνδεσης που στέλνονται χωρίς HTTPS.

9 Ερώτηση 9

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διαχειριστές μπορούν να μπλοκάρουν γνωστές θύρες VPN, όπως η 1194 του OpenVPN, ή να χρησιμοποιούν βαθύ έλεγχο πακέτων (DPI) για να εντοπίζουν κίνηση VPN.

10 Ερώτηση 10

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Μια πολιτική μη τήρησης αρχείων καταγραφής είναι η υπόσχεση ενός παρόχου να μην κρατά αρχεία της δραστηριότητάς σου· κανένας νόμος δεν απαιτεί από τα VPN να αποθηκεύουν τις αναζητήσεις για 30 ημέρες.

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. Τούνελ	A 2. Πρωτόκολλο	B 3. Εύρος ζώνης	E 4. Διακομιστής
C 5. Γεωγραφικός αποκλεισμός (geoblock)	D 6. Τείχος προστασίας	F 7. Ιδιωτικότητα	G 8. ISP

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΣΗΡΑΓΓΟΠΟΙΗΣΗ	2 ΕΥΡΟΣ ΖΩΝΗΣ	3 ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ	4 ΠΡΩΤΟΚΟΛΛΟ
5 ΤΕΙΧΟΣ	6 ΔΙΑΚΟΜΙΣΤΗΣ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 G – ΑΠΟΡΡΗΤΟ	2 E – ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ	3 B – ΠΡΩΤΟΚΟΛΛΟ	4 F – ΤΕΙΧΟΣ
5 C – ΕΥΡΟΖΩΝΗΣ	6 D – ΔΙΑΚΟΜΙΣΤΗΣ	7 H – ΠΑΡΟΧΟΣ	8 A – ΣΗΡΑΓΓΟΠΟΙΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Τούνελ, Πρωτόκολλο και Εύρος ζώνης 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.

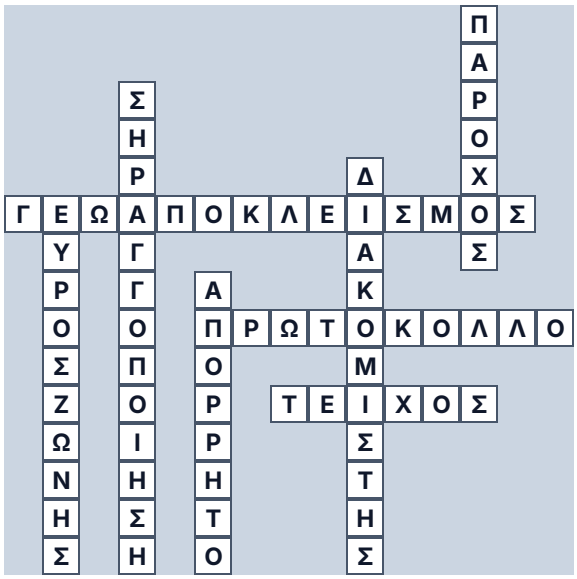
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΡΙΖΟΝΤΙΑ

4 οριζόντια: ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ Περιορισμός που εμποδίζει την πρόσβαση στον ιστό ανάλογα με τη φυσική τοποθεσία (14 γράμματα)

7 οριζόντια: ΠΡΩΤΟΚΟΛΛΟ Σύνολο κανόνων που καθορίζει πώς μεταδίδονται τα δεδομένα στο δίκτυο (10 γράμματα)

8 οριζόντια: ΤΕΙΧΟΣ Σύστημα ασφαλείας που παρακολουθεί και μπλοκάρει την μη εξουσιοδοτημένη κίνηση (τείχος προστασίας) (6 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΠΑΡΟΧΟΣ Ο πάροχος υπηρεσιών διαδικτύου (ISP), που καταγράφει την κίνησή σου αν δεν είναι κρυπτογραφημένη (7 γράμματα)

2 κάθετα: ΣΗΡΑΓΓΟΠΟΙΗΣΗ Τύλιγμα των πακέτων δεδομένων μέσα σε άλλο πακέτο για ασφαλή μετάδοση (13 γράμματα)

3 κάθετα: ΔΙΑΚΟΜΙΣΤΗΣ Ένας απομακρυσμένος υπολογιστής που δρομολογεί την κίνησή σου και κρύβει την IP σου (11 γράμματα)

5 κάθετα: ΕΥΡΟΣΖΩΝΗΣ Ο μέγιστος ρυθμός μεταφοράς δεδομένων μέσω μιας σύνδεσης (10 γράμματα)

6 κάθετα: ΑΠΟΡΡΗΤΟ Η κατάσταση του να είσαι απαλλαγμένος από παρακολούθηση ή δημόσια επιτήρηση (8 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΟΡΟΣΓΗΠΙΣΗΗΓΑ — **ΣΗΡΑΓΓΟΠΟΙΗΣΗ**
2. ΗΟΕΥΣΣΩΝΖΡ — **ΕΥΡΟΣΖΩΝΗΣ**
3. ΓΕΕΟΛΣΙΣΩΚΠΟΜΑ — **ΓΕΩΑΠΟΚΛΕΙΣΜΟΣ**
4. ΡΤΟΗΡΑΠΟ — **ΑΠΟΡΡΗΤΟ**
5. ΛΚΟΡΤΟΟΠΛΩ — **ΠΡΩΤΟΚΟΛΛΟ**
6. ΟΣΜΣΗΤΔΙΙΑΚ — **ΔΙΑΚΟΜΙΣΤΗΣ**
7. ΟΤΧΣΙΕ — **ΤΕΙΧΟΣ**
8. ΑΟΣΠΟΧΡ — **ΠΑΡΟΧΟΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΠΡΟΣΤΑΤΕΨΕ ΤΟ ΑΠΟΡΡΗΤΟ ΣΟΥ ΜΕ ΑΣΦΑΛΗ ΣΗΡΑΓΓΑ"

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.