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

Προστασία προσωπικών δεδομένων και Τα δικαιώματά σου

Προσωπικά δεδομένα, δικαιώματα ιδιωτικότητας (GDPR, CCPA), μεσίτες δεδομένων, cookies, ηλεκτρονικό ψάρεμα, VPN και ασφαλέστεροι λογαριασμοί

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΙΔΙΩΤΙΚΟΤΗΤΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΕΝΗΜΕΡΩΜΕΝΗ

ΓΝΩΡΙΣΕ ΤΑ ΔΕΔΟΜΕΝΑ ΣΟΥ

Τι συλλέγεται και γιατί

ΕΝΔΥΝΑΜΩΜΕΝΟ

ΔΙΚΑΙΩΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Δικαιώματα GDPR και CCPA/CPRA

ΕΠΑΓΡΥΠΝΟΣ

ΕΞΥΠΝΕΣ ΣΥΝΗΘΕΙΕΣ

MFA, ενημερώσεις και εντοπισμός απατών

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στα παγκόσμια πρότυπα προστασίας προσωπικών δεδομένων. Θα εξερευνήσεις τη συναίνεση opt-in βάσει GDPR, τα δικαιώματα εξαίρεσης από πωλήσεις βάσει CCPA, τις πρακτικές ελαχιστοποίησης δεδομένων, την κρυπτογράφηση ολόκληρου του δίσκου σε αδράνεια και το TLS κατά τη μετάδοση.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Μάθε τα δικαιώματα ιδιωτικότητάς σου και τις ασφαλείς συνήθειες.**
- [ ] **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 ιδιωτικότητα δεδομένων

URL: https://www.vpn.com/el/kiberasfaleia/aporrito-dedomenon/

Η πορεία μάθησής σου: ιδιωτικότητα προσωπικών δεδομένων

- Κατανόησε τα δικαιώματα ιδιωτικότητάς σου βάσει του GDPR και του CCPA της Καλιφόρνιας.
- Αναγνώρισε πώς οι μεσίτες δεδομένων, τα cookies και οι εφαρμογές συλλέγουν προσωπικά δεδομένα.
- Εφάρμοσε την ελαχιστοποίηση δεδομένων, μοιράζοντας μόνο όσα χρειάζεται πραγματικά μια υπηρεσία.
- Κάνε ενημερωμένες επιλογές στα banner για cookies και στα αιτήματα αδειών των εφαρμογών.
- Μείωσε τον κίνδυνο από ηλεκτρονικό ψάρεμα, παραβιάσεις και δημόσιο Wi-Fi με MFA και ενημερώσεις.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΑΠΟΡΡΗΤΟΥ ΔΕΔΟΜΕΝΩΝ

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 των δικών σου προσωπικών δεδομένων. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΙΔΙΩΤΙΚΟΤΗΤΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΣΟΥ (ΕΙΣΑΓΩΓΗ)

Το απόρρητο δεδομένων είναι η δυνατότητά σου να ελέγχεις πώς συλλέγονται, χρησιμοποιούνται, αποθηκεύονται και κοινοποιούνται τα προσωπικά σου στοιχεία. Νόμοι όπως ο GDPR και ο CCPA σου δίνουν δικαιώματα, ενώ συνήθειες όπως ισχυροί κωδικοί πρόσβασης, MFA και προσεκτική κοινοποίηση μπορούν να βοηθήσουν στη μείωση του κινδύνου.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. Ποια επιλογή αντικατοπτρίζει καλύτερα την αρχή της ελαχιστοποίησης δεδομένων;

- A. Κοινοποίηση μόνο των δεδομένων που χρειάζεται μια υπηρεσία για τον σκοπό της
- B. Παραχώρηση πλήρους πρόσβασης σε κάθε εφαρμογή για ευκολότερη ρύθμιση
- C. Συμπλήρωση όλων των προαιρετικών πεδίων στις φόρμες εγγραφής
- D. Επαναχρησιμοποίηση ενός κωδικού πρόσβασης ώστε οι λογαριασμοί να διαχειρίζονται ευκολότερα

2. Ποιο βήμα συνιστάται αν ένας ιστότοπος που χρησιμοποιείς αναφέρει παραβίαση;

- A. Άλλαξε αυτόν τον κωδικό πρόσβασης και ενεργοποίησε το MFA όπου προσφέρεται
- B. Επαναχρησιμοποίηση του ίδιου κωδικού πρόσβασης σε νέο λογαριασμό
- C. Απάντησε στο email παραβίασης με το PIN σου
- D. Αγνόησέ το, αφού οι παραβιάσεις σπάνια έχουν σημασία

3. Σύμφωνα με τους κανόνες της ΕΕ, ποια είναι έγκυρη συναίνεση για cookies παρακολούθησης;

- A. Ενεργή επιλογή ενός μη προεπιλεγμένου πλαισίου μετά από σαφή ενημέρωση
- B. Προεπιλεγμένα τετραγωνίδια σε banner cookies ή εγγραφής
- C. Απλή συνέχιση της κύλισης ή της περιήγησης στον ιστότοπο
- D. Μια ειδοποίηση κρυμμένη στους όρους και τις προϋποθέσεις του ιστότοπου

4. Ποιο δικαίωμα έχουν οι καταναλωτές της Καλιφόρνιας βάσει του CCPA;

- A. Για να εξαιρεθούν από την πώληση ή την κοινοποίηση των δεδομένων τους
- B. Για να πληρώνεται σταθερή αμοιβή για κάθε αίτημα δεδομένων
- C. Για να απαιτήσεις την αφαίρεση οποιασδήποτε εφαρμογής από τα καταστήματα εφαρμογών
- D. Για να αποκλείσεις κάθε συλλογή δεδομένων από κάθε εταιρεία

5. Τι κάνει κυρίως ένα VPN όταν συνδέεσαι σε δημόσιο Wi-Fi;

- A. Κρυπτογραφεί την κίνηση μεταξύ της συσκευής σου και του διακομιστή VPN
- B. Εμποδίζει τους ιστότοπους να ορίζουν οποιαδήποτε cookies
- C. Αντικαθιστά την ανάγκη για MFA
- D. Αφαιρεί κακόβουλο λογισμικό που υπάρχει ήδη σε μια συσκευή

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση Σωστό/Λάθος 6

6. Το απόρρητο δεδομένων και η ασφάλεια δεδομένων σημαίνουν το ίδιο πράγμα.

○ Σωστό ○ Λάθος

7 Ερώτηση Σωστό/Λάθος 7

7. Ο GDPR μπορεί να εφαρμόζεται σε εταιρείες εκτός ΕΕ που προσφέρουν υπηρεσίες σε άτομα στην ΕΕ.

○ Σωστό ○ Λάθος

8 Ερώτηση Σωστό/Λάθος 8

8. Η χρήση VPN εμποδίζει τους ιστότοπους να σε παρακολουθούν με cookies.

○ Σωστό ○ Λάθος

9 Ερώτηση Σωστό/Λάθος 9

9. Το να μοιράζεσαι λιγότερα προσωπικά δεδομένα στο διαδίκτυο μπορεί να μειώσει τη ζημιά από μια παραβίαση.

○ Σωστό ○ Λάθος

10 Ερώτηση Σωστό/Λάθος 10

10. Ο CCPA επιτρέπει στους καταναλωτές να εξαιρεθούν από την πώληση ή την κοινοποίηση των δεδομένων τους.

○ 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. Σύμφωνα με τον GDPR, η _____ πρέπει να δίνεται ελεύθερα, να είναι συγκεκριμένη, ενημερωμένη και σαφής, επομένως τα προεπιλεγμένα πλαίσια δεν υπολογίζονται.

2. Ένας _____ συγκεντρώνει στοιχεία από δημόσια αρχεία, εφαρμογές και αγορές για να δημιουργεί και να πουλά προφίλ ανθρώπων.

3. Ένα μήνυμα που ισχυρίζεται ότι το δέμα σου κρατείται και σου ζητά να «επιβεβαιώσεις» στοιχεία κάρτας είναι τυπικό παράδειγμα επίθεσης τύπου: _____ .

4. Το HTTPS χρησιμοποιεί την _____ για να βοηθά στην προστασία των δεδομένων κατά τη μετάδοση μεταξύ του προγράμματος περιήγησης και ενός ιστότοπου.

5. Η κοινοποίηση μόνο των στοιχείων που χρειάζεται πραγματικά μια φόρμα εγγραφής εφαρμόζει την αρχή της: _____ .

6. Το δικαίωμα που σου επιτρέπει να ζητάς από έναν οργανισμό να διαγράψει τα προσωπικά σου δεδομένα, αν και ισχύουν εξαιρέσεις, ονομάζεται δικαίωμα στη _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΠΟΕΓΓΡΑΦΗ · ΔΙΑΓΡΑΦΗ · ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ · ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ · ΚΡΥΠΤΟΓΡΑΦΗΣΗ · ΜΕΣΙΤΗΣ ΔΕΔΟΜΕΝΩΝ · ΜΠΙΣΚΟΤΟ · ΣΥΓΚΑΤΑΘΕΣΗ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών απορρήτου

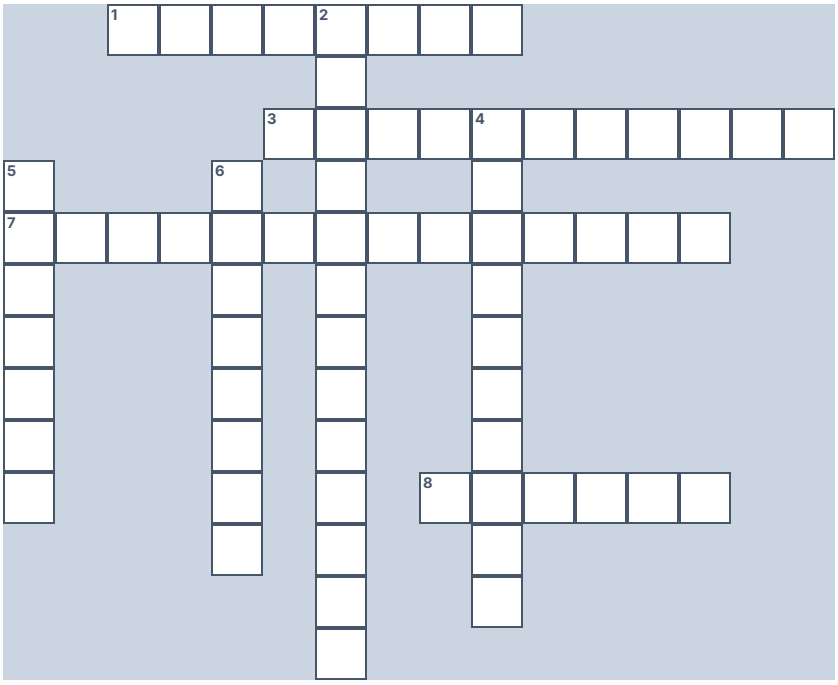
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. Δικαίωμα διαγραφής	A	Δικαίωμα στην Καλιφόρνια να σταματήσεις μια επιχείρηση από το να πουλά ή να κοινοποιεί τα δεδομένα σου.
☐	2. Δικαίωμα εξαίρεσης (opt-out)	B	Το δικαίωμα βάσει του GDPR να διαγραφούν τα προσωπικά σου δεδομένα, με την επιφύλαξη εξαιρέσεων.
☐	3. Ελαχιστοποίηση δεδομένων	C	Μικρό αρχείο του προγράμματος περιήγησης που χρησιμοποιείται για να παρακολουθεί τη δραστηριότητά σου σε διάφορους ιστότοπους.
☐	4. Κρυπτογράφηση	D	Ελεύθερα δοσμένη, συγκεκριμένη, τεκμηριωμένη και σαφής συγκατάθεση.
☐	5. Μεσίτης δεδομένων	E	Συλλογή μόνο των προσωπικών δεδομένων που χρειάζονται για έναν δηλωμένο σκοπό.
☐	6. Συναίνεση	F	Ψεύτικα μηνύματα που ξεγελούν τους ανθρώπους ώστε να αποκαλύψουν δεδομένα ή στοιχεία σύνδεσης.
☐	7. Phishing	G	Ανακάτεμα δεδομένων ώστε μόνο όποιος έχει το σωστό κλειδί να μπορεί να τα διαβάσει.
☐	8. Cookie παρακολούθησης	H	Εταιρεία που συγκεντρώνει και πουλά προσωπικά προφίλ από πολλές πηγές.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

1. Μικρό αρχείο του προγράμματος περιήγησης που μπορεί να ακολουθεί τη δραστηριότητά σου σε διάφορους ιστότοπους (8)

3. Ελεύθερα δοσμένη, συγκεκριμένη, ενημερωμένη και σαφής συμφωνία για τη χρήση των δεδομένων (11)

7. Ελαχιστοποίηση δεδομένων: συλλογή μόνο όσων χρειάζονται για έναν δηλωμένο σκοπό (14)

8. Ψεύτικα μηνύματα που σε εξαπατούν ώστε να αποκαλύψεις στοιχεία σύνδεσης ή κάρτας (6)

ΚΑΘΕΤΑ

2. Αλλοίωση των δεδομένων ώστε να τα διαβάσει μόνο όποιος έχει το σωστό κλειδί (13)

4. Δικαίωμα του CCPA να σταματήσεις την πώληση ή την κοινοποίηση των δεδομένων σου (10)

5. Εταιρεία που συγκεντρώνει και πουλά προφίλ ανθρώπων (7)

6. Δικαίωμα που σου επιτρέπει να ζητήσεις από έναν οργανισμό να διαγράψει τα προσωπικά σου δεδομένα (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

1 οριζόντια: Μικρό αρχείο του προγράμματος περιήγησης που μπορεί να ακολουθεί τη δραστηριότητά σου σε διάφορους ιστότοπους (8 γράμματα):

3 οριζόντια: Ελεύθερα δοσμένη, συγκεκριμένη, ενημερωμένη και σαφής συμφωνία για τη χρήση των δεδομένων (11 γράμματα):

7 οριζόντια: Ελαχιστοποίηση δεδομένων: συλλογή μόνο όσων χρειάζονται για έναν δηλωμένο σκοπό (14 γράμματα):

8 οριζόντια: Ψεύτικα μηνύματα που σε εξαπατούν ώστε να αποκαλύψεις στοιχεία σύνδεσης ή κάρτας (6 γράμματα):

ΚΑΘΕΤΑ

2 κάθετα: Αλλοίωση των δεδομένων ώστε να τα διαβάσει μόνο όποιος έχει το σωστό κλειδί (13 γράμματα):

4 κάθετα: Δικαίωμα του CCPA να σταματήσεις την πώληση ή την κοινοποίηση των δεδομένων σου (10 γράμματα):

5 κάθετα: Εταιρεία που συγκεντρώνει και πουλά προφίλ ανθρώπων (7 γράμματα):

6 κάθετα: Δικαίωμα που σου επιτρέπει να ζητήσεις από έναν οργανισμό να διαγράψει τα προσωπικά σου δεδομένα (8 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

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

Η Κ Σ Ρ Φ Π Ω Ε Θ Ε Ρ Γ Α Λ Ο

Σ Γ Η Φ Α Ρ Γ Γ Ε Ο Π Α Ω Μ Μ

Η Μ Κ Φ Ψ Α Ρ Ε Μ Α Ρ Υ Ε Π Α

Φ Ρ Χ Κ Μ Μ Η Θ Ν Θ Π Σ Ι Ζ Λ

Α Σ Λ Ρ Χ Θ Β Τ Ζ Ψ Ι Σ Ξ Ψ Χ

Ρ Σ Η Τ Χ Α Ο Υ Ν Τ Κ Ν Ω Ξ Θ

Γ Ο Σ Θ Ο Υ Τ Ξ Η Ο Υ Τ Κ Α Ε

Ο Ξ Μ Λ Α Ν Υ Σ Τ Ζ Η Ο Π Χ Ψ

Τ Ι Κ Υ Ι Ω Φ Ο Ψ Ο Κ Θ Ω Ι Ι

Π Ν Α Ε Η Φ Α Ρ Γ Α Ι Δ Θ Α Σ

Υ Ε Λ Α Χ Ι Σ Τ Ο Π Ο Ι Η Σ Η

Ρ Α Ι Ε Φ Ε Κ Ω Κ Ε Κ Π Ν Ι Α

Κ Ζ Σ Υ Γ Κ Α Τ Α Θ Ε Σ Η Ξ Κ

Ν Γ Ν Γ Δ Η Θ Β Α Ξ Ρ Λ Ο Φ Τ

Θ Ψ Ζ Ω Ρ Η Χ Φ Θ Ε Π Τ Ν Τ Κ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΔΙΑΓΡΑΦΗ ΑΠΟΕΓΓΡΑΦΗ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΕΣΙΤΗΣ
ΣΥΓΚΑΤΑΘΕΣΗ ΨΑΡΕΜΑ ΜΠΙΣΚΟΤΟ

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. ΔΙΑΓΡΑΦΗ**
- **B. ΑΠΟΕΓΓΡΑΦΗ**
- **C. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ**
- **D. ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
- **E. ΜΕΣΙΤΗΣ**
- **F. ΣΥΓΚΑΤΑΘΕΣΗ**
- **G. ΨΑΡΕΜΑ**
- **H. ΜΠΙΣΚΟΤΟ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Δικαίωμα του CCPA να σταματήσεις την πώληση ή την κοινοποίηση των δεδομένων σου.

_____ 2. Ελεύθερα δοσμένη, συγκεκριμένη, ενημερωμένη και σαφής συμφωνία για τη χρήση των δεδομένων.

_____ 3. Εταιρεία που συγκεντρώνει και πουλά προφίλ ανθρώπων.

_____ 4. Δικαίωμα που σου επιτρέπει να ζητήσεις από έναν οργανισμό να διαγράψει τα προσωπικά σου δεδομένα.

_____ 5. Ελαχιστοποίηση δεδομένων: συλλογή μόνο όσων χρειάζονται για έναν δηλωμένο σκοπό.

_____ 6. Ψεύτικα μηνύματα που σε εξαπατούν ώστε να αποκαλύψεις στοιχεία σύνδεσης ή κάρτας.

_____ 7. Μικρό αρχείο του προγράμματος περιήγησης που μπορεί να ακολουθεί τη δραστηριότητά σου σε διάφορους ιστότοπους.

_____ 8. Αλλοίωση των δεδομένων ώστε να τα διαβάσει μόνο όποιος έχει το σωστό κλειδί.

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. **ΦΓΡΔΑΙΗΑ**
2. **ΙΛΣΑΤΣΕΗΟΗ ΟΙΠΧ**
3. **ΙΜΤΣΣΗΕ**
4. **ΑΕΡΜΨΑ**
5. **ΑΓΗΠΕΡΓΑΦΟ**
6. **ΤΦΓΟΗΥΣΑΚΡ ΡΗΠ**
7. **ΘΑΣΥΑΗΕΣΓΤ Κ**
8. **ΣΠΚΟΜΤΟΙ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Βήματα που κάνεις μετά από μια παραβίαση δεδομένων			
2	Εφαρμογές που ζητούν την τοποθεσία σου			
3	Ρυθμίσεις απορρήτου που πρέπει να ελέγξεις σε ένα νέο κινητό			
4	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
5	Ενδείξεις ότι ένα μήνυμα μπορεί να είναι ηλεκτρονικό ψάρεμα			
6	Λόγοι για να ενημερώνεις το λογισμικό			
7	Προσωπικά στοιχεία που δεν πρέπει να βάζεις στα μέσα κοινωνικής δικτύωσης			
8	Τρόποι να προστατεύσεις τους λογαριασμούς σου			
9	Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι			
10	Λογαριασμοί που πρέπει να έχουν ενεργοποιημένο το MFA			
11	Πράγματα που παίρνεις αντίγραφο ασφαλείας			
12	Μέρη όπου μπορεί να χρησιμοποιήσεις δημόσιο Wi-Fi			
13	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			
14	Εταιρείες που μπορεί να συλλέγουν δεδομένα περιήγησής σου			
15	Προειδοποιητικά σημάδια σε ένα email			

Σημείο ελέγχου 8: Μελέτες περίπτωσης απορρήτου δεδομένων

Εφάρμοσε τις έννοιες που έμαθες στα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΑΙΤΗΜΑ ΔΙΑΓΡΑΦΗΣ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΕΝΑΝ ΙΣΤΟΤΟΠΟ



Σενάριο: Η Μάγια, που ζει στη Γαλλία, έκλεισε τον λογαριασμό της σε μια εφαρμογή αγορών πριν από δύο χρόνια αλλά εξακολουθεί να λαμβάνει τα διαφημιστικά της email. Θέλει η εφαρμογή να διαγράψει τα προσωπικά της δεδομένα βάσει του δικαιώματος διαγραφής του GDPR.

Ερώτηση συζήτησης: Ποια βήματα μπορεί να κάνει η Μάγια και ποια δεδομένα μπορεί η εφαρμογή να κρατήσει νόμιμα;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΜΙΑ ΕΦΑΡΜΟΓΗ ΚΟΥΙΖ ΚΑΙ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΗΣ



Σενάριο: Μια δωρεάν εφαρμογή κουίζ προσωπικότητας ζητά από τον Λέο την τοποθεσία, τις επαφές, το μικρόφωνο και την ημερομηνία γέννησής του πριν μπορέσει να ξεκινήσει.

Ερώτηση συζήτησης: Ποιες άδειες φαίνονται περιττές και ποιες επιλογές έχει ο Λέο για να μειώσει όσα μοιράζεται;

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Όσοι ενδιαφέρονται για την ιδιωτικότητα σκέφτονται πριν μοιραστούν προσωπικά στοιχεία στο διαδίκτυο. Χρησιμοποίησε το παρακάτω κλειδί Γράμματος-Αριθμού 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

18	10	5	23	15	20		16	17	9	13			
12	15	9	17	1	18	19	5	9	18		18	19	15
		4	9	1	4	9	10	19	20	15			

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 το απόρρητο δεδομένων – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για την προστασία των προσωπικών σου δεδομένων.

Q1: Ποια είναι η διαφορά μεταξύ ιδιωτικότητας δεδομένων και ασφάλειας δεδομένων;

Η ιδιωτικότητα είναι ο έλεγχός σου στον τρόπο συλλογής, χρήσης και κοινοποίησης των προσωπικών δεδομένων· η ασφάλεια είναι η προστασία που τα κρατά μακριά από μη εξουσιοδοτημένη πρόσβαση.

Q2: Τι είναι ο GDPR;

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ, που εφαρμόζεται από τις 25 Μαΐου 2018, θέτει κανόνες για την επεξεργασία προσωπικών δεδομένων και παρέχει στα άτομα δικαιώματα επί αυτών [1].

Q3: Τι είναι ο CCPA;

Ο νόμος της Καλιφόρνιας για το απόρρητο των καταναλωτών (CCPA), όπως τροποποιήθηκε από τον CPRA, παρέχει στους κατοίκους το δικαίωμα να γνωρίζουν, να διαγράφουν, να διορθώνουν και να εξαιρούνται από την πώληση ή την κοινοποίηση δεδομένων [4].

Q4: Τι σημαίνει ελαχιστοποίηση δεδομένων;

Χρήση μόνο προσωπικών δεδομένων που είναι επαρκή, σχετικά και περιορισμένα σε ό,τι είναι απαραίτητο για έναν σκοπό· ως χρήστης, μπορείς να το εφαρμόσεις κοινοποιώντας λιγότερα [1].

Q5: Τι είναι τα δικαιώματα εφαρμογών (app permissions);

Ρυθμίσεις που επιτρέπουν στις εφαρμογές να έχουν πρόσβαση στην τοποθεσία, τις επαφές ή τις φωτογραφίες σου· η εξέτασή τους και η απενεργοποίηση όσων δεν χρειάζονται μπορεί να περιορίσει τη συλλογή δεδομένων [8].

Σημείο ελέγχου 10: Συχνές ερωτήσεις για το απόρρητο δεδομένων – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για την προστασία των προσωπικών σου δεδομένων.

Q6: Τι κάνει το HTTPS για το απόρρητό μου;

Το HTTPS κρυπτογραφεί τα δεδομένα μεταξύ του προγράμματος περιήγησής σου και ενός ιστότοπου, αλλά και οι ιστότοποι απάτης μπορούν να χρησιμοποιούν HTTPS, επομένως το λουκέτο δεν αποδεικνύει ότι ένας ιστότοπος είναι αξιόπιστος [10].

Q7: Τι είναι το Δικαίωμα Διαγραφής (Right to Erasure);

Βάσει του άρθρου 17 του GDPR μπορείς να ζητήσεις από έναν οργανισμό να διαγράψει τα δεδομένα σου σε ορισμένες περιπτώσεις· το δικαίωμα δεν είναι απόλυτο και έχει εξαιρέσεις [1].

Q8: Τι θεωρείται έγκυρη συγκατάθεση;

Μια σαφής θετική ενέργεια, όπως η επιλογή ενός μη προεπιλεγμένου πλαισίου μετά από σαφή ενημέρωση· τα προεπιλεγμένα πλαίσια, η σιωπή ή η κύλιση δεν λογίζονται [2].

Q9: Τι κάνει έναν κωδικό πρόσβασης ισχυρό;

Το μήκος μετράει περισσότερο: το NIST ζητά από τους ιστότοπους να απαιτούν τουλάχιστον 15 χαρακτήρες για κωδικούς πρόσβασης που χρησιμοποιούνται μόνοι τους και να επιτρέπουν διαχειριστές κωδικών πρόσβασης [11].

Q10: Τι πρέπει να κάνω μετά από παραβίαση δεδομένων;

Άλλαξε τους κωδικούς πρόσβασης που επηρεάστηκαν, ενεργοποίησε την MFA, παρακολούθησε τους λογαριασμούς σου και εξέτασε το ενδεχόμενο δωρεάν παγώματος πίστωσης· το IdentityTheft.gov παραθέτει βήματα ανάκαμψης [9].

Σημείο ελέγχου 10: Συχνές ερωτήσεις για το απόρρητο – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε βαθύτερες ερωτήσεις για τις νομικές βάσεις, τα cookies, την παρακολούθηση, τους μεσίτες δεδομένων και τα δικαιώματά σου στο διαδίκτυο.

Q1: Χρειάζεται η συγκατάθεσή μου για κάθε επεξεργασία δεδομένων σύμφωνα με τον GDPR;

Όχι. Η συγκατάθεση είναι μία από τις έξι νόμιμες βάσεις του Άρθρου 6· άλλες περιλαμβάνουν τη σύμβαση, τη νομική υποχρέωση και τα έννομα συμφέροντα [1].

Q2: Πού εφαρμόζεται ο GDPR;

Σε οργανισμούς που είναι εγκατεστημένοι στην ΕΕ, καθώς και σε οργανισμούς εκτός ΕΕ που προσφέρουν αγαθά ή υπηρεσίες σε άτομα στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους [1].

Q3: Χρειάζονται οι ιστότοποι συγκατάθεση για όλα τα cookies;

Όχι πάντα. Τα απολύτως απαραίτητα cookies εξαιρούνται συνήθως, ενώ τα μη απαραίτητα, όπως τα cookies παρακολούθησης, απαιτούν προηγούμενη έγκυρη συγκατάθεση [3].

Q4: Ποιος είναι ο κίνδυνος για το απόρρητο από τους trackers τρίτων;

Οι ιχνηλάτες τρίτων μπορούν να σε ακολουθούν σε πολλούς ιστότοπους για να σου εμφανίζουν στοχευμένες διαφημίσεις· η διαγραφή των cookies και η προσαρμογή των ρυθμίσεων ιδιωτικότητας μπορεί να βοηθήσει [8].

Q5: Τι είναι ένας μεσίτης δεδομένων (data broker);

Μια επιχείρηση που συλλέγει προσωπικές πληροφορίες από διάφορες πηγές και τις πουλά σε άλλες εταιρείες· οι κάτοικοι της Καλιφόρνιας μπορούν να χρησιμοποιήσουν την πλατφόρμα DROP της πολιτείας για να ζητήσουν διαγραφή [5].

Σημείο ελέγχου 10: Συχνές ερωτήσεις για το απόρρητο – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε βαθύτερες ερωτήσεις για τις νομικές βάσεις, τα cookies, την παρακολούθηση, τους μεσίτες δεδομένων και τα δικαιώματά σου στο διαδίκτυο.

Q6: Τι είναι ο σύνδεσμος «Do Not Sell or Share» του CCPA;

Οι επιχειρήσεις που πωλούν ή μοιράζονται δεδομένα πρέπει γενικά να προσφέρουν έναν σύνδεσμο «Do Not Sell or Share My Personal Information» και να σέβονται σήματα εξαίρεσης όπως το GPC [4].

Q7: Με κάνει ένα VPN ανώνυμο;

Όχι. Ένα VPN κρυπτογραφεί την κίνηση προς τον διακομιστή VPN και κρύβει την IP σου από τους ιστότοπους, αλλά ο πάροχος μπορεί να τη δει, και τα cookies και το fingerprinting μπορούν ακόμη να σε παρακολουθούν [12].

Q8: Πώς μπορώ να εντοπίσω ένα μήνυμα ηλεκτρονικού ψαρέματος (phishing);

Πρόσεχε τα επείγοντα αιτήματα να πατήσεις συνδέσμους, να επιβεβαιώσεις στοιχεία πληρωμής ή να διορθώσεις προβλήματα λογαριασμού· επικοινώνησε με την εταιρεία χρησιμοποιώντας έναν αριθμό ή έναν ιστότοπο που ξέρεις ότι είναι αληθινός [7].

Q9: Είναι ασφαλές το δημόσιο Wi-Fi;

Μπορεί να είναι επικίνδυνο. Οι περισσότεροι ιστότοποι χρησιμοποιούν κρυπτογράφηση, γι' αυτό έλεγξε για HTTPS, κράτα το λογισμικό ενημερωμένο και χρησιμοποίησε MFA [10]· ένα VPN μπορεί να προσθέσει προστασία σε μη αξιόπιστα δίκτυα [12].

Q10: Ποιες είναι οι μέγιστες οικονομικές κυρώσεις βάσει του GDPR;

Για τις πιο σοβαρές παραβιάσεις, τα πρόστιμα μπορούν να φτάσουν τα 20 εκατ. ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών, όποιο από τα δύο είναι υψηλότερο [1].

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την ιδιωτικότητα δεδομένων

Εξέτασε πραγματικά στοιχεία για τους νόμους περί ιδιωτικότητας, τους μεσίτες δεδομένων, τις απάτες, τις παραβιάσεις και τις ασφαλέστερες διαδικτυακές συνήθειες.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Ο GDPR εφαρμόζεται από τις 25 Μαΐου 2018 και παρέχει στα άτομα δικαιώματα πρόσβασης, διόρθωσης και διαγραφής των προσωπικών τους δεδομένων [1].

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Βάσει του GDPR, οι σοβαρότερες παραβάσεις μπορούν να επιφέρουν πρόστιμα έως 20 εκατομμύρια ευρώ ή 4% του παγκόσμιου κύκλου εργασιών [1].

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Οι τροποποιήσεις CPRA στον CCPA της Καλιφόρνιας τέθηκαν σε ισχύ την 1η Ιανουαρίου 2023, προσθέτοντας δικαιώματα διόρθωσης δεδομένων και περιορισμού της χρήσης ευαίσθητων δεδομένων [4].

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Οι καταναλωτές δήλωσαν ότι έχασαν 15,9 δισ. δολάρια από απάτες το 2025, από πάνω από 12 δισ. την προηγούμενη χρονιά, σύμφωνα με την FTC [6].

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Από την 1η Ιανουαρίου 2026, οι κάτοικοι της Καλιφόρνιας μπορούν να χρησιμοποιούν τη δωρεάν πλατφόρμα DROP για να ζητούν από μεσίτες δεδομένων να διαγράψουν τα προσωπικά τους δεδομένα [5].

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Σύμφωνα με τους κανόνες προστασίας δεδομένων της ΕΕ, τα προεπιλεγμένα τσεκαρισμένα πλαίσια, η σιωπή ή η αδράνεια δεν θεωρούνται έγκυρη συναίνεση [2].

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ

Στο HB, οι ιστότοποι πρέπει να σου παρέχουν τρόπο να συναινέσεις σε κάθε cookie που δεν είναι απολύτως απαραίτητο για τον ιστότοπο [3].

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ

Ο GDPR απαιτεί ορισμένες παραβιάσεις προσωπικών δεδομένων να δηλώνονται στην αρχή εντός 72 ωρών, όπου είναι εφικτό [1].

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ

Το NIST λέει ότι οι ιστότοποι δεν πρέπει να επιβάλλουν περιοδικές αλλαγές κωδικού πρόσβασης και πρέπει να ελέγχουν τους νέους κωδικούς έναντι λιστών παραβιασμένων κωδικών [11].

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΟ ΑΠΟΡΡΗΤΟ

Ένα VPN κρύβει τη διεύθυνση IP σου από τους ιστότοπους, αλλά ο πάροχος του VPN μπορεί και πάλι να βλέπει την κίνησή σου, γι' αυτό επίλεξε προσεκτικά [12].

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα παζλ βασίζονται σε επίσημες οδηγίες ιδιωτικότητας της ΕΕ, του Ηνωμένου Βασιλείου, της Καλιφόρνιας, της FTC, του NIST και του EFF.

ΕΠΙΣΗΜΕΣ ΚΑΙ ΕΙΔΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[3] Information Commissioner's Office. (n.d.). Cookies. ICO for the public.

https://ico.org.uk/for-the-public/online/cookies/

[4] California Privacy Protection Agency. (n.d.). Frequently asked questions (FAQs).

https://cppa.ca.gov/faq.html

[5] California Privacy Protection Agency. (2025). Delete Request and Opt-out Platform (DROP).

https://privacy.ca.gov/drop/

[6] Federal Trade Commission. (2026, March 25). FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud [Press release].

https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[7] Federal Trade Commission. (2022). How to recognize and avoid phishing scams. Consumer Advice.

https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] Federal Trade Commission. (2023). How websites and apps collect and use your information. Consumer Advice.

https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

[9] Federal Trade Commission. (2024). What to know about identity theft. Consumer Advice.

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

[10] Federal Trade Commission. (2023). Are public Wi-Fi networks safe? What you need to know. Consumer Advice.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[11] National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4).

https://csrc.nist.gov/pubs/sp/800/63/b/4/final

[12] Electronic Frontier Foundation. (2026). Choosing the VPN that's right for you. Surveillance Self-Defense.

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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ελαχιστοποίηση δεδομένων** ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το άρθρο 5 του GDPR απαιτεί τα προσωπικά δεδομένα να είναι πρόσφορα, συναφή και περιορισμένα σε ό,τι είναι απαραίτητο· οι χρήστες μπορούν να το μιμηθούν μοιράζοντας λιγότερα δεδομένα [1].

2 **Αντιμετώπιση παραβίασης** ΔΙΑΡΡΗΞΗ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Μετά από παραβίαση, άλλαξε τους εκτεθειμένους κωδικούς πρόσβασης, ενεργοποίησε το MFA και παρακολούθησε τους λογαριασμούς· το IdentityTheft.gov προσφέρει εξατομικευμένα βήματα ανάκαμψης [9].

3 **Έγκυρη συναίνεση** ΣΥΓΚΑΤΑΘΕΣΗ ΓΙΑ COOKIES — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η έγκυρη συναίνεση απαιτεί σαφή θετική ενέργεια μετά από σαφή ενημέρωση· τα προεπιλεγμένα τσεκαρισμένα πλαίσια και η συνεχής κύλιση δεν πληρούν τις προϋποθέσεις [2].

4 **Δικαιώματα βάσει CCPA** ΝΟΜΟΣ CCPA — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι καταναλωτές στην Καλιφόρνια μπορούν να εξαιρεθούν από την πώληση ή την κοινοποίηση προσωπικών πληροφοριών, μεταξύ άλλων μέσω σημάτων Global Privacy Control [4].

5 **Προστασία VPN** ΣΗΡΑΓΓΑ VPN — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα VPN κρυπτογραφεί την κίνηση προς τον διακομιστή VPN και κρύβει την IP σου από τους ιστότοπους, αλλά τα cookies και το fingerprinting μπορούν και πάλι να σε παρακολουθούν [12].

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ιδιωτικότητα και ασφάλεια** ΙΔΙΩΤΙΚΟΤΗΤΑ — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Συναφή αλλά διαφορετικά: Το άρθρο 5 του GDPR θέτει κανόνες για τον τρόπο χρήσης των δεδομένων, ενώ το άρθρο 32 απαιτεί ξεχωριστά μέτρα ασφαλείας [1].

7 **Εδαφικό πεδίο εφαρμογής του GDPR** ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ GDPR — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το άρθρο 3(2) καλύπτει οργανισμούς εκτός ΕΕ που προσφέρουν αγαθά ή υπηρεσίες σε άτομα στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους [1].

8 **Τα VPN και τα cookies** ΟΡΙΑ VPN — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένα VPN κρύβει τη διεύθυνση IP σου, αλλά τα cookies, τα εικονοστοιχεία παρακολούθησης και το fingerprinting μπορούν και πάλι να σε ακολουθούν σε διάφορους ιστότοπους [12].

9 **Λιγότερο μοίρασμα** ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η απενεργοποίηση αχρείαστων αδειών εφαρμογών και η κοινοποίηση λιγότερων στοιχείων περιορίζει όσα μπορούν να συλλεχθούν και να εκτεθούν αργότερα σε μια παραβίαση [8].

10 **Εξαίρεση από πώληση ή κοινοποίηση** ΝΟΜΟΣ CCPA — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι επιχειρήσεις που πωλούν ή μοιράζονται δεδομένα πρέπει να προσφέρουν έναν σαφή σύνδεσμο εξαίρεσης, όπως το «Do Not Sell or Share My Personal Information» [4].

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

B 1. Δικαίωμα διαγραφής	A 2. Δικαίωμα εξαίρεσης (opt-out)	E 3. Ελαχιστοποίηση δεδομένων	G 4. Κρυπτογράφηση
H 5. Μεσίτης δεδομένων	D 6. Συναίνεση	F 7. Phishing	C 8. Cookie παρακολούθησης

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΣΥΓΚΑΤΑΘΕΣΗ	2 ΜΕΣΙΤΗΣ ΔΕΔΟΜΕΝΩΝ	3 ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	4 ΚΡΥΠΤΟΓΡΑΦΗΣΗ
5 ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ	6 ΔΙΑΓΡΑΦΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 B – ΑΠΟΕΓΓΡΑΦΗ	2 F – ΣΥΓΚΑΤΑΘΕΣΗ	3 E – ΜΕΣΙΤΗΣ	4 A – ΔΙΑΓΡΑΦΗ
5 C – ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ	6 G – ΨΑΡΕΜΑ	7 H – ΜΠΙΣΚΟΤΟ	8 D – ΚΡΥΠΤΟΓΡΑΦΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Δικαίωμα διαγραφής, Δικαίωμα εξαίρεσης (opt-out) και Ελαχιστοποίηση δεδομένων και να δώσουν ένα παράδειγμα για τον καθένα.

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

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

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: ΜΠΙΣΚΟΤΟ Μικρό αρχείο του προγράμματος περιήγησης που μπορεί να ακολουθεί τη δραστηριότητά σου σε διάφορους ιστότοπους (8 γράμματα)

3 οριζόντια: ΣΥΓΚΑΤΑΘΕΣΗ Ελεύθερα δοσμένη, συγκεκριμένη, ενημερωμένη και σαφής συμφωνία για τη χρήση των δεδομένων (11 γράμματα)

7 οριζόντια: ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ Ελαχιστοποίηση δεδομένων: συλλογή μόνο όσων χρειάζονται για έναν δηλωμένο σκοπό (14 γράμματα)

8 οριζόντια: ΨΑΡΕΜΑ Ψεύτικα μηνύματα που σε εξαπατούν ώστε να αποκαλύψεις στοιχεία σύνδεσης ή κάρτας (6 γράμματα)

ΚΑΘΕΤΑ

2 κάθετα: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Αλλοίωση των δεδομένων ώστε να τα διαβάσει μόνο όποιος έχει το σωστό κλειδί (13 γράμματα)

4 κάθετα: ΑΠΟΕΓΓΡΑΦΗ Δικαίωμα του CCPA να σταματήσεις την πώληση ή την κοινοποίηση των δεδομένων σου (10 γράμματα)

5 κάθετα: ΜΕΣΙΤΗΣ Εταιρεία που συγκεντρώνει και πουλά προφίλ ανθρώπων (7 γράμματα)

6 κάθετα: ΔΙΑΓΡΑΦΗ Δικαίωμα που σου επιτρέπει να ζητήσεις από έναν οργανισμό να διαγράψει τα προσωπικά σου δεδομένα (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. ΦΓΡΔΑΙΗΑ — **ΔΙΑΓΡΑΦΗ**
2. ΙΛΣΑΤΣΕΗΟΗΟΙΠΧ — **ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ**
3. ΙΜΤΣΣΗΕ — **ΜΕΣΙΤΗΣ**
4. ΑΕΡΜΨΑ — **ΨΑΡΕΜΑ**
5. ΑΓΗΠΕΡΓΑΦΟ — **ΑΠΟΕΓΓΡΑΦΗ**
6. ΤΦΓΟΗΥΣΑΚΡΡΗΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
7. ΘΑΣΥΑΗΕΣΓΤΚ — **ΣΥΓΚΑΤΑΘΕΣΗ**
8. ΣΠΚΟΜΤΟΙ — **ΜΠΙΣΚΟΤΟ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΣΚΕΨΟΥ ΠΡΙΝ ΜΟΙΡΑΣΤΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Αίτημα διαγραφής δεδομένων από έναν ιστότοπο

Οδηγίες για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Η Μάγια, που ζει στη Γαλλία, έκλεισε πριν από δύο χρόνια τον λογαριασμό της σε μια εφαρμογή αγορών, αλλά εξακολουθεί να λαμβάνει τα διαφημιστικά της μηνύματα. Θέλει η εφαρμογή να διαγράψει τα προσωπικά της δεδομένα βάσει του δικαιώματος διαγραφής του GDPR.
- Προτεινόμενες προσεγγίσεις: Επιλογή 1: Η Maya στέλνει γραπτό αίτημα διαγραφής και αντιτίθεται στο άμεσο μάρκετινγκ, το οποίο πρέπει τότε να σταματήσει· η εφαρμογή θα πρέπει γενικά να απαντήσει εντός ενός μηνός [1]. Επιλογή 2: πρώτα διαγράφεται από τη λίστα αποδεκτών για άμεση ανακούφιση. Αιτιολόγηση: η διαγραφή δεν είναι απόλυτη, οπότε η εφαρμογή μπορεί να κρατήσει δεδομένα που χρειάζονται για νομικές υποχρεώσεις ή νομικές αξιώσεις [1]. Αν δεν απαντήσει, μπορεί να υποβάλει καταγγελία στην αρχή προστασίας δεδομένων της [1].

B Μελέτη περίπτωσης 2: Μια εφαρμογή κουίζ και τα δικαιώματά της

Οδηγίες για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια δωρεάν εφαρμογή κουίζ προσωπικότητας ζητά από τον Leo την τοποθεσία, τις επαφές, το μικρόφωνο και την ημερομηνία γέννησής του πριν μπορέσει να ξεκινήσει.
- Προτεινόμενες προσεγγίσεις: Επιλογή 1: αρνείται την πρόσβαση στην τοποθεσία, στις επαφές και στο μικρόφωνο και μετά ελέγχει αν το κουίζ εξακολουθεί να λειτουργεί [8]. Επιλογή 2: αν η εφαρμογή επιμένει, επιλέγει άλλη εφαρμογή ή τη διαγράφει [8]. Αιτιολόγηση: ένα κουίζ σπάνια χρειάζεται αυτά τα δεδομένα και η κοινοποίηση λιγότερων δεδομένων περιορίζει ό,τι μπορεί να συλλεχθεί, να πωληθεί ή να εκτεθεί. Ο Leo μπορεί επίσης να ελέγχει τακτικά τα δικαιώματα στις ρυθμίσεις απορρήτου του κινητού του [8].