

ΜΑΙΟΣ 2026

ΕΝΗΜΕΡΩΤΙΚΟ ΔΕΛΤΙΟ ΝΟ 3

GO CLOUD GO SECURE

Ανακαλύψτε νέο περιεχόμενο και εργαλεία ασφάλειας με το Go Cloud! Go Secure!

Αγαπητέ αναγνώστη,

Χαιρόμαστε που είμαστε ξανά μαζί! Διαβάζετε το 3ο Newsletter του έργου μας Go Cloud! Go Secure!

Έχουμε σημαντικά νέα να μοιραστούμε μαζί σας: τρία βασικά αποτελέσματα του έργου είναι πλέον διαθέσιμα στην ιστοσελίδα μας:

- Το εργαλείο αυτοαξιολόγησης CSI επιτρέπει στους χρήστες να αξιολογήσουν τις γνώσεις τους και να εντοπίσουν σημεία που μπορούν να βελτιώσουν.
- Το εκπαιδευτικό πρόγραμμα CSI προσφέρει πρακτικό και εύχρηστο εκπαιδευτικό υλικό για την ασφάλεια στο cloud.
- Το Μοντέλο CSI βοηθά τις ΜΜΕ να κατανοήσουν πώς να χρησιμοποιούν τις υπηρεσίες cloud με μεγαλύτερη ασφάλεια και ποια βήματα μπορούν να ακολουθήσουν για να βελτιωθούν.

Προς το παρόν, και οι τρεις πόροι είναι διαθέσιμοι στα αγγλικά, ενώ οι μεταφρασμένες εκδόσεις θα είναι σύντομα έτοιμες.

Σε αυτό το τεύχος θα βρείτε χρήσιμες ενημερώσεις, νέο υλικό και πρακτικές πληροφορίες που θα σας βοηθήσουν να ενισχύσετε το επίπεδο κυβερνοασφάλειάς σας.

Ευχαριστούμε που είστε μαζί μας!
Η ομάδα του Go Cloud!



Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Κύρια θέματα

Μήνυμα από την ομάδα του Go Cloud!
– σελίδα 1

Η διαδρομή προς την ασφάλεια στο Cloud
– σελίδα 2

Εργαλείο αυτοαξιολόγησης CSI
– σελίδα 3

Εκπαιδευτικό πρόγραμμα CSI
– σελίδα 4

Μοντέλο Εφαρμογής CSI
– σελίδα 5

Ενδιαφέροντα στοιχεία για την κυβερνοασφάλεια
– σελίδα 8

Αναζητούμε δοκιμαστές!
– σελίδα 6

Σύντομα οι εκδηλώσεις διάδοσης!
– σελίδα 7



www.gocloudsecure.eu



[@gocloudgosecure](https://www.instagram.com/gocloudgosecure)



[gocloudgosecure](https://www.facebook.com/gocloudgosecure)



[gocloudgosecure](https://www.linkedin.com/company/gocloudgosecure)



GO CLOUD GO SECURE

Η διαδρομή προς την ασφάλεια στο Cloud

A practical pathway for SMEs and VET providers:
assess your current situation, build cloud-
security skills, and turn knowledge into action.

Πώς μπορεί ο οργανισμός μου
να βελτιώσει την ασφάλεια στο
cloud βήμα προς βήμα;



1 Ξεκινήστε με την αυτοαξιολόγηση

Χρησιμοποιήστε το εργαλείο αυτοαξιολόγησης CSI για να αξιολογήσετε το επίπεδο ενημέρωσής σας για την ασφάλεια στο cloud, τις καθημερινές πρακτικές και τη λήψη αποφάσεων. Σας βοηθά να εντοπίσετε δυνατά σημεία, κενά και τομείς προτεραιότητας.

2 Εντοπίστε ανάγκες και κενά

Αξιοποιήστε τα αποτελέσματα για να δείτε πού χρειάζεται περισσότερη υποστήριξη - από τις βασικές αρχές του cloud και την κοινή ευθύνη έως τις συνηθισμένες απειλές και τα αδύναμα σημεία.



3 Αναπτύξτε δεξιότητες μέσω του εκπαιδευτικού προγράμματος

Μάθετε να κατανοείτε τους κινδύνους του cloud, να αναγνωρίζετε συνηθισμένες απειλές, να σχεδιάζετε ασφαλέστερα περιβάλλοντα cloud και να εφαρμόζετε αποτελεσματικές πρακτικές διακυβέρνησης.



4 Εφαρμόστε το Μοντέλο CSI

Χρησιμοποιήστε το Μοντέλο CSI για να μετατρέψετε τη γνώση σε πράξη. Καταγράψτε υπηρεσίες, κινδύνους και απαιτήσεις συμμόρφωσης και στη συνέχεια καθορίστε προτεραιότητες, ρόλους, πολιτικές και κατάλληλα μέτρα ασφάλειας.



5 Βελτιωθείτε και αναπτυχθείτε με ασφάλεια

Παρακολουθήστε την πρόοδο, βελτιώστε τις πρακτικές σας και ενισχύετε συνεχώς την ανθεκτικότητά σας. Τα εργαλεία μας υποστηρίζουν τη συνεχή βελτίωση, την ευαισθητοποίηση του προσωπικού και έναν πιο ασφαλή ψηφιακό μετασχηματισμό.

Success!





ΕΡΓΑΛΕΙΟ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ CSI

ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ CLOUD

**ΑΠΑΝΤΗΣΤΕ ΣΕ 15 ΕΡΩΤΗΣΕΙΣ – ΔΕΙΤΕ ΑΜΕΣΑ ΤΑ
ΑΠΟΤΕΛΕΣΜΑΤΑ**

CLICK HERE >

ΤΩΡΑ ΔΙΑΘΕΣΙΜΟ ONLINE



Ελέγξτε το επίπεδο ασφάλειας στο Cloud

Πόσο ασφαλής είναι η προσέγγισή σας στη χρήση του cloud; Το εργαλείο αυτοαξιολόγησης CSI βοηθά ΜΜΕ, εκπαιδευτές και εκπαιδευόμενους να εξετάσουν πραγματικές καταστάσεις ασφάλειας στο cloud με απλό και πρακτικό τρόπο.

Το ερωτηματολόγιο καλύπτει βασικά θέματα όπως τα μοντέλα υπηρεσιών cloud, η κοινή ευθύνη, η προστασία δεδομένων, η πρόληψη ransomware, το Zero Trust, ο έλεγχος πρόσβασης, η διακυβέρνηση και η αντιμετώπιση περιστατικών.

Δεν πρόκειται για «τρομακτική εξέταση» – μόνο για χρήσιμες ερωτήσεις που σας βοηθούν να δείτε τι ήδη γνωρίζετε και σε ποια σημεία μπορείτε να βελτιωθείτε.

Από τους καθημερινούς κινδύνους σε καλύτερες αποφάσεις

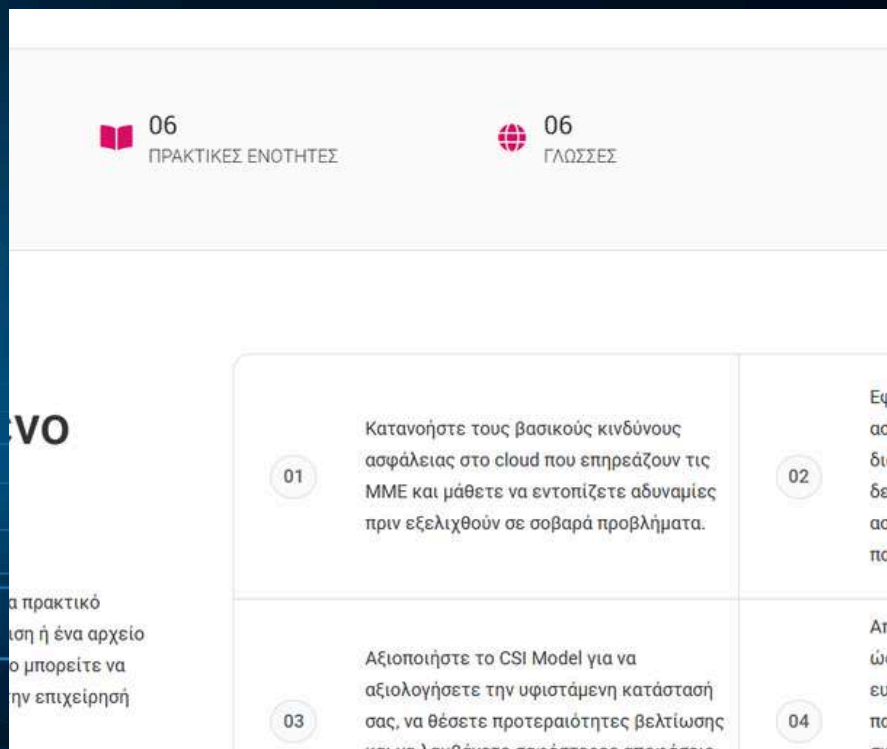
Η ασφάλεια στο cloud μπορεί να φαίνεται σύνθετη, ειδικά για μικρές επιχειρήσεις με περιορισμένους πόρους. Το εργαλείο αυτοαξιολόγησης CSI τη μετατρέπει σε απλές, πρακτικές ερωτήσεις που συνδέονται με καθημερινές αποφάσεις. Καλύπτει θέματα όπως κωδικοί πρόσβασης, έλεγχος ταυτότητας πολλαπλών παραγόντων, αντίγραφα ασφαλείας, διαρροές δεδομένων, σχεδιασμός cloud και κατανομή ευθυνών, βοηθώντας τις ΜΜΕ να εντοπίσουν τα βασικά σημεία που χρειάζονται βελτίωση.

Ένα απλό πρώτο βήμα για ισχυρότερη ασφάλεια στο Cloud

Το εργαλείο αυτοαξιολόγησης CSI δεν στοχεύει να σας πιέσει, αλλά να ενισχύσει την επίγνωση. Σας βοηθά να ελέγχετε γρήγορα τις γνώσεις σας, να εντοπίσετε κενά και να αποκτήσετε μεγαλύτερη αυτοπεποίθηση στην ασφάλεια cloud. Για ΜΜΕ, εκπαιδευτές και εκπαιδευόμενους, αποτελεί ένα απλό σημείο εκκίνησης για καλύτερες πρακτικές κυβερνοασφάλειας και ασφαλέστερη χρήση του cloud.

ΕΝΙΣΧΥΣΤΕ ΤΙΣ ΔΕΞΙΟΤΗΤΕΣ ΣΑΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ CLOUD

Το εκπαιδευτικό πρόγραμμα CSI βοηθά τις ΜΜΕ να ενισχύσουν τις γνώσεις τους στην ασφάλεια cloud μέσα από πρακτική και εύκολη εκπαίδευση. Δείχνει πώς να αναγνωρίζουν κινδύνους, να προστατεύουν τα δεδομένα, να λαμβάνουν ασφαλέστερες καθημερινές αποφάσεις και να εφαρμόζουν το Μοντέλο CSI με μεγαλύτερη σιγουριά.



CLICK HERE >

ΕΚΠΑΙΔΕΥΤΙΚΟ ΠΡΟΓΡΑΜΜΑ CSI

Έξι ενότητες, σχεδιασμένες για πολυάσχολους επιχειρηματίες

- Ενότητα 1 – Βασικές αρχές ασφάλειας Cloud για ΜΜΕ:
 - Παρουσιάζει το cloud computing, τα μοντέλα υπηρεσιών και ανάπτυξης, τα οφέλη και τις προκλήσεις για τις ΜΜΕ, καθώς και τις βασικές αρχές ασφαλούς υιοθέτησης του cloud και της κοινής ευθύνης.
- Ενότητα 2 – Κυβερνοαπειλές και προκλήσεις για τις ΜΜΕ:
 - Εξετάζει συνήθεις απειλές για τις ΜΜΕ, όπως phishing, ransomware, εσωτερικές απειλές και shadow IT, μαζί με πρακτικά και οικονομικά μέτρα πρόληψης.
- Ενότητα 3 – Σχεδιασμός ασφαλών περιβαλλόντων Cloud:
 - Παρουσιάζει τις βασικές αρχές και τα μέτρα για ασφαλείς υποδομές cloud, όπως διαχείριση ταυτότητας και πρόσβασης, κρυπτογράφηση, πολυεπίπεδη άμυνα, τμηματοποίηση, παρακολούθηση και ασφαλής σχεδιασμός.
- Ενότητα 4 – Διακυβέρνηση ασφάλειας Cloud:
 - Καλύπτει βασικά θέματα διακυβέρνησης, όπως κρυπτογράφηση και διαχείριση κλειδιών, προστασία δεδομένων, αξιολόγηση κινδύνων, συμμόρφωση, ιδιωτικότητα, επιχειρησιακή συνέχεια και βασικά πλαίσια κυβερνοασφάλειας.
- Ενότητα 5 – Το Μοντέλο CSI: Από τη θεωρία στην πράξη:
 - Παρουσιάζει πώς οι ΜΜΕ εφαρμόζουν το Μοντέλο CSI για αξιολόγηση κινδύνων, ιεράρχηση ενεργειών, υλοποίηση μέτρων ασφάλειας και συνεχή παρακολούθηση και βελτίωση.
- Ενότητα 6 – Ανάπτυξη ικανοτήτων για παρόχους ΕΕΚ:
 - Υποστηρίζει παρόχους ΕΕΚ στη δημιουργία εκπαίδευσης cloud security για ΜΜΕ, με κατάλληλα προφίλ εκπαιδευομένων, πρακτικές μεθόδους, ψηφιακά εργαλεία και συνεργασία με επιχειρήσεις.



Δομή του Εκπαιδευτικού Προγράμματος

Το εκπαιδευτικό πρόγραμμα CSI καθοδηγεί τους εκπαιδευόμενους στις βασικές αρχές ασφάλειας cloud, την αναγνώριση απειλών, τον ασφαλή σχεδιασμό cloud, τη διακυβέρνηση, το Μοντέλο CSI και την ανάπτυξη ικανοτήτων. Συμβάλλει σε ασφαλέστερες αποφάσεις, μεγαλύτερη ευαισθητοποίηση του προσωπικού, καλύτερη προετοιμασία για συμμόρφωση και έναν πιο σίγουρο ψηφιακό μετασχηματισμό.

ΜΟΝΤΕΛΟ ΕΦΑΡΜΟΓΗΣ CSI

ΠΡΑΚΤΙΚΟΣ ΟΔΙΚΟΣ ΓΙΑ ΑΣΦΑΛΕΣΤΕΡΗ ΧΡΗΣΗ ΤΟΥ CLOUD

Οι υπηρεσίες cloud μπορούν να κάνουν τις ΜΜΕ πιο γρήγορες, ευέλικτες και ανταγωνιστικές — αρκεί να χρησιμοποιούνται με ασφάλεια. Το Μοντέλο Εφαρμογής CSI βοηθά τις επιχειρήσεις να κατανοήσουν τους κινδύνους του cloud, να θέσουν σαφείς προτεραιότητες και να κάνουν πρακτικά βήματα για ισχυρότερη κυβερνοασφάλεια.

Μοντέλο Εφαρμογής CSI

Φάση 1: ΑΝΑΛΥΣΗ

Φάση 2: ΚΑΘΟΡΙΣΜΟΣ

Φάση 3: ΣΧΕΔΙΑΣΜΟΣ

Φάση 4: ΕΦΑΡΜΟΓΗ

Φάση 5: ΕΠΑΛΗΘΕΥΣΗ

Από τους κινδύνους στην πράξη

Το Μοντέλο CSI ξεκινά με σαφή ανάλυση των υπηρεσιών cloud, των πιθανών κινδύνων και των απαιτήσεων συμμόρφωσης. Έτσι, οι ΜΜΕ μπορούν να εντοπίσουν πού είναι πιο ευάλωτες και τι πρέπει να βελτιώσουν πρώτα.

Σχεδιασμένο για ΜΜΕ

Το μοντέλο είναι πρακτικό και εύκολο στην εφαρμογή. Βοηθά μικρότερους οργανισμούς να δημιουργήσουν πολιτικές, να καθορίσουν αρμοδιότητες και να επιλέξουν ρεαλιστικά μέτρα ασφάλειας, χωρίς περιττή πολυπλοκότητα.

Πέντε στάδια για ισχυρότερη ασφάλεια στο Cloud

Το Μοντέλο Εφαρμογής CSI καθοδηγεί τους οργανισμούς μέσα από πέντε βασικά στάδια: Ανάλυση, Καθορισμός, Σχεδιασμός, Εφαρμογή και Επαλήθευση. Βήμα προς βήμα, βοηθά τις επιχειρήσεις να περάσουν από την κατανόηση των κινδύνων στην εφαρμογή πραγματικών μέτρων ασφάλειας.

Το μοντέλο τονίζει επίσης τη σημασία της εκπαίδευσης, της παρακολούθησης και της ανατροφοδότησης. Η ασφάλεια στο cloud δεν σταματά μετά την εφαρμογή — γίνεται μια συνεχής διαδικασία μάθησης, ελέγχου και βελτίωσης.

[CLICK HERE](#)



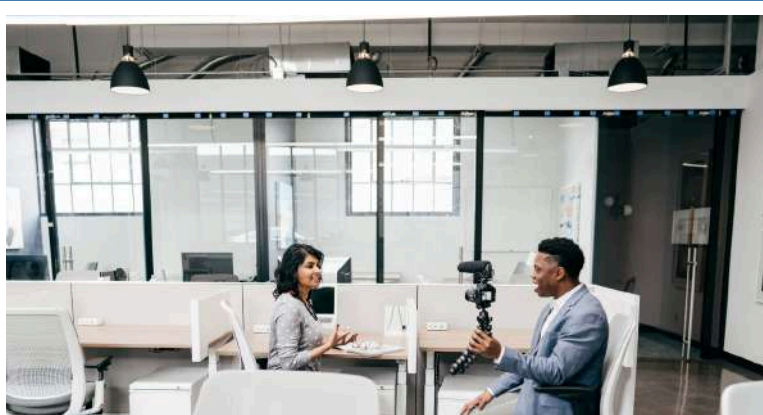
Με το Μοντέλο CSI, οι ΜΜΕ αποκτούν ένα πρακτικό πλαίσιο για ασφαλέστερες αποφάσεις, προστασία δεδομένων, καλύτερη συμμόρφωση και μεγαλύτερη μακροπρόθεσμη εμπιστοσύνη στις τεχνολογίες cloud.

ΑΝΑΖΗΤΟΥΜΕ ΔΟΚΙΜΑΣΤΕΣ!



GO CLOUD! GO SECURE ΤΟ ΕΡΓΟ ΠΕΡΝΑΣΤΗ ΦΑΣΗ ΔΟΚΙΜΩΝ

Το έργο Go Cloud! Go Secure! έφτασε σε ακόμη ένα σημαντικό ορόσημο: ξεκινά η δοκιμή του Μοντέλου Εφαρμογής Cloud Security και του σχετικού εκπαιδευτικού προγράμματος. Στόχος αυτής της φάσης είναι να αξιολογηθεί πόσο χρήσιμα, κατανοητά και σχετικά είναι τα εργαλεία που αναπτύχθηκαν για επιχειρήσεις, εκπαιδευτές και επαγγελματίες ασφάλειας cloud.



ΑΝΑΤΡΟΦΟΔΟΤΗΣΗ ΕΙΔΙΚΩΝ ΓΙΑ ΠΡΑΚΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Η διαδικασία δοκιμών και η αξιολόγηση των αποτελεσμάτων αναμένεται να ολοκληρωθούν έως τον Σεπτέμβριο του 2026. Μετά τις τελικές βελτιώσεις, το Μοντέλο Εφαρμογής Cloud Security και το εκπαιδευτικό πρόγραμμα θα είναι διαθέσιμα και στις πέντε γλώσσες του έργου.

WE WANT YOUR
FEEDBACK!

Εξωτερικοί εμπειρογνώμονες συμμετέχουν στις δοκιμές

Μαζί με το προσωπικό των εταιρών του έργου, θα συμμετάσχουν εξωτερικοί εμπειρογνώμονες και εκπρόσωποι των ομάδων-στόχων. Η ανατροφοδότησή τους θα βοηθήσει την κοινοπραξία να βελτιώσει το μοντέλο και το εκπαιδευτικό υλικό, ώστε να ανταποκρίνονται όσο το δυνατόν καλύτερα στις πρακτικές ανάγκες των μικρομεσαίων επιχειρήσεων.

Αναμενόμενα αποτελέσματα έως τον Σεπτέμβριο 2026

Ολοκλήρωση πιλοτικών
δοκιμών

Βελτίωση του μοντέλου και
του εκπαιδευτικού
προγράμματος

Διαθεσιμότητα σε πέντε
γλώσσες



Συμβάλετε στις τελικές εκδόσεις των αποτελεσμάτων του Go Cloud,
μοιράζοντας μαζί μας τις πολύτιμες απόψεις σας παρακάτω:

[Σύνδεσμος για τη δοκιμή](#)

ΣΥΝΤΟΜΑ ΟΙ ΕΚΔΗΛΩΣΕΙΣ ΔΙΑΔΟΣΗΣ!

Σεπτέμβριος – Οκτώβριος 2026
Σε 5 ευρωπαϊκές χώρες

ΣΕΠΤΕΜΒΡΙΟΣ –
ΟΚΤΩΒΡΙΟΣ 2026

ΕΚΔΗΛΩΣΕΙΣ ΔΙΑΔΟΣΗΣ ΣΕ:
ΑΥΣΤΡΙΑ
ΟΥΓΓΑΡΙΑ
ΙΤΑΛΙΑ
ΒΟΥΛΓΑΡΙΑ
ΚΥΠΡΟ

Τι να περιμένετε;

- Γνωρίστε τα αποτελέσματα του έργου και καινοτόμα εργαλεία
- Μάθετε πρακτικές στρατηγικές για την ασφάλεια cloud
- Ανταλλάξτε απόψεις με ειδικούς και τοπικούς φορείς
- Εμπνευστείτε και δημιουργήστε χρήσιμες επαφές

Λάβετε μέρος στην τοπική εκδήλωση εάν είστε:

- ιδιοκτήτης ή διευθυντής ΜΜΕ
- επαγγελματίας πληροφορικής
- επαγγελματίας κυβερνοασφάλειας
- σύμβουλος
- εκπαιδευτής
- άτομο που ενδιαφέρεται για την ασφάλεια cloud

Μείνετε συντονισμένοι!

Το αναλυτικό πρόγραμμα, οι ημερομηνίες και οι πληροφορίες εγγραφής θα ανακοινωθούν σύντομα στην ιστοσελίδα και στα μέσα κοινωνικής δικτύωσης του έργου.

Μην χάσετε την ευκαιρία να γίνετε μέρος μιας ισχυρότερης και ασφαλέστερης ψηφιακής Ευρώπης!

Ο ΣΥΝΑΡΠΑΣΤΙΚΟΣ ΚΟΣΜΟΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Η κυβερνοασφάλεια χρησιμοποιεί... μέλι ως παγίδα!

Ένα «honeypot» είναι ένα εσκεμμένα ελκυστικό ψεύτικο σύστημα που έχει σχεδιαστεί για να προσελκύει κυβερνοεπιτιθέμενους. Ενώ οι εισβολείς πιστεύουν ότι βρήκαν έναν πολύτιμο στόχο, οι ειδικοί ασφάλειας μπορούν να παρακολουθούν τις μεθόδους τους και να μαθαίνουν πώς να προστατεύουν καλύτερα τα πραγματικά συστήματα.

Κάθε αρχείο έχει το δικό του ψηφιακό αποτύπωμα!

Ένα κρυπτογραφικό hash λειτουργεί σαν μοναδικό αποτύπωμα ενός αρχείου. Ακόμη και η αλλαγή ενός μόνο γράμματος μπορεί να δημιουργήσει εντελώς διαφορετικό αποτύπωμα, επιτρέποντας να εντοπιστεί εάν τα δεδομένα έχουν τροποποιηθεί κρυφά.

Μια φωτογραφία μπορεί να κρύβει έναν μυστικό «επιβάτη»!

Η στεγανογραφία είναι η τεχνική απόκρυψης πληροφοριών μέσα σε μια φαινομενικά συνηθισμένη εικόνα, ηχογράφηση ή βίντεο. Το αρχείο μπορεί να φαίνεται απολύτως φυσιολογικό, ενώ στην πραγματικότητα περιέχει ένα κρυφό μήνυμα ή κακόβουλο κώδικα.

Κάποιοι υπολογιστές ζουν σε ψηφιακά «νησιά»!

Οι υπολογιστές που περιέχουν ιδιαίτερα ευαίσθητα δεδομένα είναι μερικές φορές «air-gapped», δηλαδή φυσικά αποσυνδεδεμένοι από το διαδίκτυο και άλλα δίκτυα. Ωστόσο, ακόμη και ένα ψηφιακό «νησί» μπορεί να προσβληθεί μέσω ενός μολυσμένου USB ή άλλης αφαιρούμενης συσκευής.

did

you

know

?



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093



**Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης**

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.