

Ευρωβαρόμετρο Flash 576 | Επιτόπια έρευνα: Απρίλιος – Μάιος 2026

Κυβερνοασφάλεια στον χώρο εργασίας: ενημέρωση και ετοιμότητα των εργαζομένων

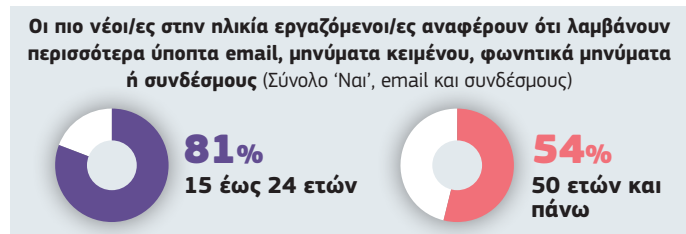
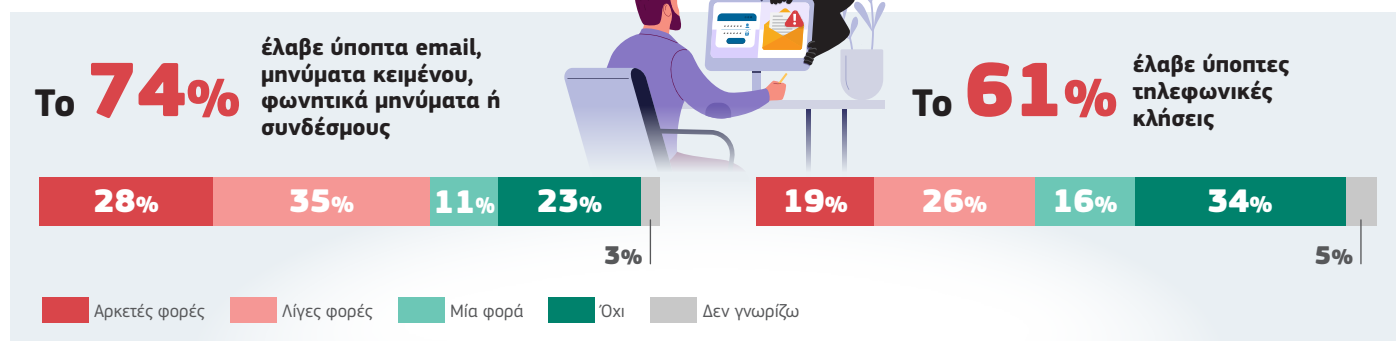


Εκτεταμένη έκθεση σε κυβερνοαπειλές στην εργασία

Τα τρία τέταρτα των εργαζομένων έχουν εκτεθεί σε ύποπτα email, μηνύματα ή συνδέσμους στην εργασία τους, κατά τους τελευταίους έξι μήνες

Βάση: ΕΕ των 27 (%)

Q6. Κατά τους τελευταίους έξι μήνες, λάβατε εσείς προσωπικά κάποιο από τα ακόλουθα στη δουλειά σας;



Το ηλεκτρονικό ψάρεμα παραμένει η πιο διαδεδομένη απειλή, αλλά οι εργαζόμενοι/ες αναφέρουν και άλλες κακόβουλες απόπειρες

Βάση: ΕΕ των 27 (%) | Q7. Κατά τους τελευταίους έξι μήνες, απ' όσο γνωρίζετε, αντιμετώπισε ο οργανισμός όπου εργάζεστε ένα ή περισσότερα από τα ακόλουθα;



Νεοεμφανιζόμενες απειλές μέσω τεχνητής νοημοσύνης

Οι απάτες μέσω χρήσης τεχνητής νοημοσύνης (15%) και άλλα περιστατικά στο κυβερνοχώρο (7%) είναι ανάμεσα στα περιστατικά που αναφέρονται.

Μόνο το 18%

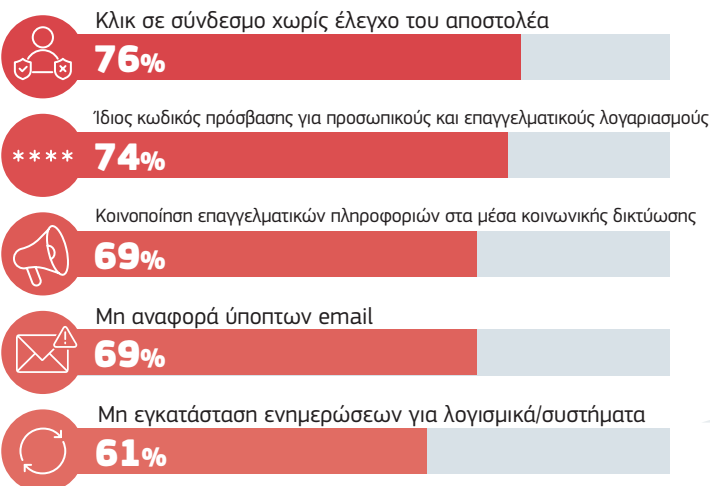
των εργαζομένων αναφέρει ότι δεν έχει αντιμετωπίσει κανένα περιστατικό στην εργασία.



Καλή ενημέρωση σχετικά με τους κινδύνους κυβερνοασφάλειας και τις συνέπειές τους

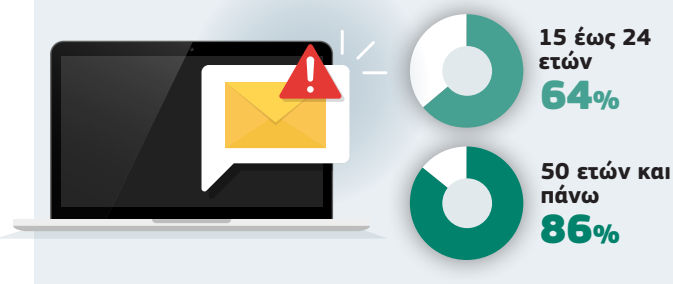
Οι εργαζόμενοι/ες είναι γενικά ενημερωμένοι/ες για ριψοκίνδυνες συμπεριφορές, ειδικά όσον αφορά το ηλεκτρονικό ψάρεμα και τη διαχείριση των κωδικών πρόσβασης

Βάση: ΕΕ των 27 (%) | Q1. Κατά τη γνώμη σας, πόσο ριψοκίνδυνες είναι οι ακόλουθες ενέργειες όταν χρησιμοποιείτε ψηφιακά συστήματα και εργαλεία στη δουλειά; (Σύνολο 'Ριψοκίνδυνο')



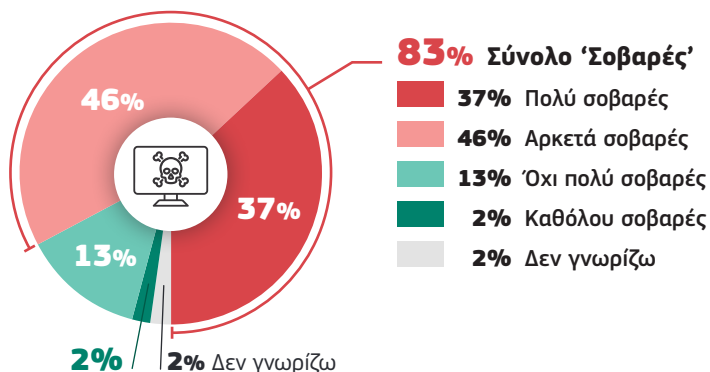
Η ενημέρωση σχετικά με τους κινδύνους αυξάνεται κατακόρυφα στις μεγαλύτερες ηλικίες

'Κλικ σε σύνδεσμο χωρίς έλεγχο του αποστολέα' - Σύνολο 'Ριψοκίνδυνο'



Οι πιθανές συνέπειες από μια κυβερνοεπίθεση θεωρούνται σε συντριπτικό βαθμό σοβαρές

Βάση: ΕΕ των 27 (%) | Q3. Πόσο σοβαρές πιστεύετε ότι θα ήταν οι συνέπειες από μια κυβερνοεπίθεση στον οργανισμό όπου εργάζεστε;

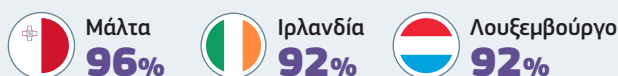


'Πολύ σοβαρές' Το 48% των οργανισμών με 250 και πάνω εργαζόμενους/ες, έναντι το 29% εκείνων με 1 έως 9 εργαζόμενους/ες

Το **83%**

θεωρεί ότι οι συνέπειες από μια κυβερνοεπίθεση θα ήταν σοβαρές για τον οργανισμό όπου εργάζεται

Υψηλότερες βαθμολογίες χώρας (Σύνολο 'Σοβαρές')



Η κυβερνοασφάλεια αναγνωρίζεται ευρέως ως σημαντική, και αυτό ισχύει περισσότερο για τους εργαζόμενους παρά για τη διοίκηση

Βάση: ΕΕ των 27 (%) | Q4. Πόσο σημαντική είναι η κυβερνοασφάλεια για τον οργανισμό όπου εργάζεστε, τόσο κατά την άποψή σας όσο και κατά την άποψη της διοίκησης; (Σύνολο 'Σημαντική')

Σημασία της κυβερνοασφάλειας (Σύνολο 'Σημαντική')

Κατά την άποψη των εργαζομένων



Κατά την άποψη της διοίκησης, σύμφωνα με τους εργαζόμενους



Σύμφωνα με την άποψη των εργαζομένων σε οργανισμούς με 250 και πάνω άτομα προσωπικό, το 62% θεωρεί την κυβερνοασφάλεια πολύ σημαντική, σε σχέση με το 47% σε οργανισμούς με 1 έως 9 εργαζόμενους/ες

Η ενημέρωση για τους κινδύνους είναι υψηλή, αλλά οι καθημερινές πρακτικές δεν συμβαδίζουν ακόμα

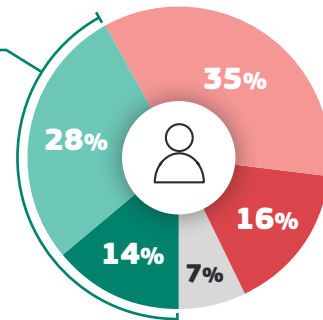
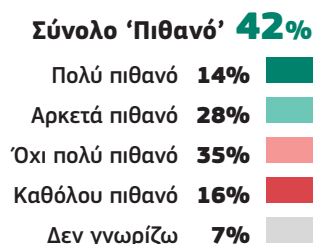
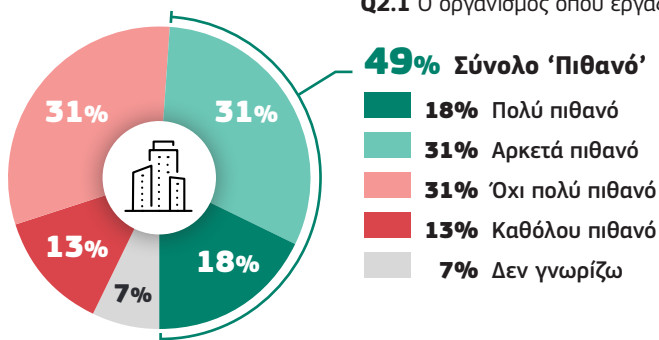
Οι κυβερνοεπιθέσεις εκλαμβάνονται ως ένας υπαρκτός κίνδυνος για τον οργανισμό όπου εργάζονται, αλλά οι εργαζόμενοι/ες νιώθουν οι ίδιοι/ες λιγότερο εκτεθειμένοι/ες

Βάση: ΕΕ των 27 (%) | Q2. Πόσο πιθανό πιστεύετε ότι είναι να αντιμετωπίσετε εσείς ή ο οργανισμός όπου εργάζεστε κάποια κυβερνοεπίθεση μέσα στους επόμενους έξι μήνες;



Q2.1 Ο οργανισμός όπου εργάζεστε

Q2.2 Οι ίδιοι/ες εργαζόμενοι/ες εν ώρα εργασίας



Το 49% σε σχέση με το 42%

των εργαζομένων θεωρεί ότι ο οργανισμός όπου εργάζονται κινδυνεύει περισσότερο από τους ίδιους/τις ίδιες

Ο θεωρούμενος κίνδυνος για τον οργανισμό αυξάνεται με το μέγεθος
(Σύνολο 'Πιθανό')

250+ εργαζόμενοι/ες



56%

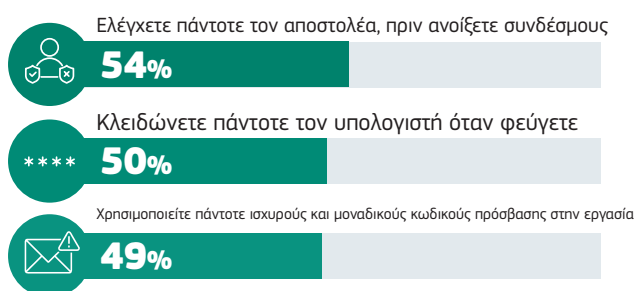
1 έως 9 εργαζόμενοι/ες



35%

Οι βασικές υγιείς συνήθειες στον κυβερνοχώρο είναι κοινές, αλλά όχι συστηματικές

Βάση: ΕΕ των 27 (%) | Q11. Πόσο συχνά κάνετε εσείς προσωπικά κάθε ένα από τα ακόλουθα στη δουλειά; ('Πάντοτε')



Οι συστηματικές πρακτικές αυξάνονται εντόνως με την ηλικία

'Χρησιμοποιεί ισχυρούς και μοναδικούς κωδικούς πρόσβασης' — % 'Πάντοτε'



Οι περισσότεροι/ες εργαζόμενοι/ες πιστεύουν ότι ο οργανισμός όπου εργάζονται είναι αποτελεσματικός στην προστασία από κυβερνοεπιθέσεις

Βάση: ΕΕ των 27 (%) | Q5. Πόσο αποτελεσματικά είναι τα ψηφιακά συστήματα και εργαλεία που παρέχει οργανισμός όπου εργάζεστε; / Q9. Γενικά, πόσο εκτεθειμένα σε κυβερνοεπιθέσεις είναι κάθε ένα από τα ακόλουθα;



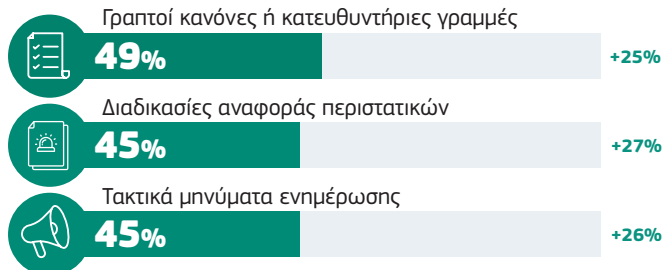
Το **82%**

αξιολογεί ότι τα ψηφιακά συστήματα και εργαλεία του οργανισμού όπου εργάζονται είναι αποτελεσματικά απέναντι σε κυβερνοεπιθέσεις

Άνιση ετοιμότητα των εργατικού δυναμικού εντός του οργανισμού

Περίπου οι μισοί οργανισμοί έχουν λάβει βασικά μέτρα κυβερνοασφάλειας, ενώ το ένα τέταρτο σχεδιάζει να τα υιοθετήσει

Βάση: ΕΕ των 27 (%) | Q10. Αν' όσο γνωρίζετε, έχει λάβει ο οργανισμός όπου εργάζεστε κάποιο από τα ακόλουθα μέτρα σχετικά με την κυβερνοασφάλεια;

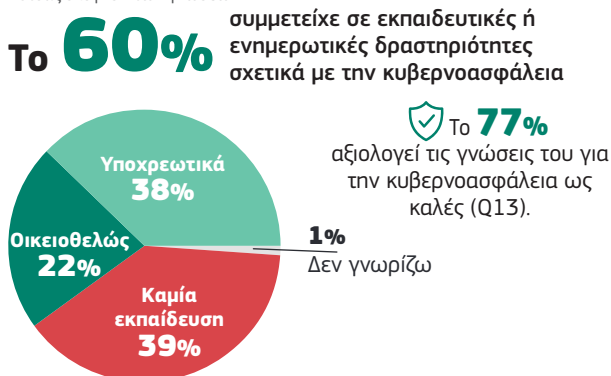
**Η επισημοποίηση εντείνεται με το μέγεθος του οργανισμού**

‘Γραπτοί κανόνες ή κατευθυντήριες γραμμές’ — % Ναι



Το 60% των εργαζομένων έχει λάβει εκπαίδευση σχετικά με την κυβερνοασφάλεια το περασμένο έτος, αλλά αυτό το ποσοστό πέφτει απότομα σε μικρότερους οργανισμούς

Βάση: ΕΕ των 27 (%) | Q12. Κατά τους τελευταίους 12 μήνες, συμμετείχατε σε κάποια εκπαιδευτική ή ενημερωτική δραστηριότητα σχετικά με την κυβερνοασφάλεια; / Q13. Αυτοαξιολόγηση των γνώσεων

**Χάσμα στην εκπαίδευση ανάλογα με το μέγεθος του οργανισμού (Σύνολο ‘Ναι’)**
... και τη θέση εργασίας**Η ζήτηση για δεξιότητες στον κυβερνοχώρο είναι έντονη, αλλά υπάρχουν εμπόδια στην εκπαίδευση**

Οι εργαζόμενοι/ες νιώθουν πολύ μεγαλύτερη σιγουριά να αναγνωρίζουν ύποπτα email, παρά ψεύτικα βίντεο φτιαγμένα με τεχνητή νοημοσύνη

Βάση: ΕΕ των 27 (%) | Q8. Πόσο σίγουρος/σίγουρη νιώθετε για την ικανότητά σας να αναγνωρίζετε...;

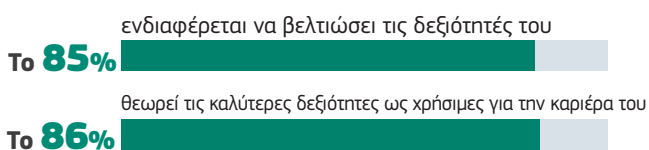


-24 πόντοι



Υπάρχει μεγάλη όρεξη για βελτίωση των δεξιοτήτων, ωστόσο, η έλλειψη χρόνου παραμένει το κύριο εμπόδιο

Βάση: ΕΕ των 27 (%) | Q14. Ενδιαφέρον για βελτίωση των δεξιοτήτων / Q15. Χρησιμότητα για το επαγγελματικό μέλλον / Q16. Κύρια εμπόδια (Πρώτων)

Κίνητρα για βελτίωση των δεξιοτήτων**Κύρια εμπόδια στην εκπαίδευση**