



Κοινή Χρήση Πόρων

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

ΠΕΡΙΕΧΟΜΕΝΟ

ΕΙΣΑΓΩΓΗ.....	2
ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΣΥΛΛΟΓΗΣ.....	4
ΣΥΛΛΟΓΗ ΠΟΡΩΝ.....	8
3.1 Κυβερνοαπειλές και κυβερνοασφάλεια	8
3.2 Ψευδείς Ειδήσεις Και Παραπληροφόρηση.....	11
3.3 Ψηφιακές Δεξιότητες Και Εκπαίδευση.....	13
3.4 Πολιτική & Κανονισμοί.....	14
3.5 Τεχνολογία & Εργαλεία	15
3.6 Τουρισμός Και Πόροι Για Συγκεκριμένους Τομείς.....	16
3.7 Άλλα / Διατομεακά Θέματα	19
ΠΡΟΣΑΡΜΟΓΗ ΚΑΙ ΤΟΠΟΘΕΤΗΣΗ ΤΗΣ ΨΗΦΙΑΚΗΣ ΒΙΒΛΙΟΘΗΚΗΣ ΣΤΟΝ ΙΣΤΟΤΟΠΟ ΤΟΥ TREADS	21
ΣΥΜΠΕΡΑΣΜΑΤΑ	24

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Σχήμα 1: Ψηφιακή βιβλιοθήκη πόρων: Διαδικασία ανάπτυξης.....	6
Σχήμα 2: Ψηφιακή βιβλιοθήκη στον ιστότοπο του TREADS.....	22
Σχήμα 3: Παράδειγμα αρχείου PDF για κάθε κατηγορία	23

«Το έγκλημα στον κυβερνοχώρο αποτελεί τη μεγαλύτερη απειλή για κάθε εταιρεία στον κόσμο.»

— Ginni Rometty, πρώην Διευθύνουσα Σύμβουλος της¹

Στην ψηφιακή εποχή, όπου οι τουριστικές εταιρείες βασίζονται όλο και περισσότερο σε διαδικτυακές πλατφόρμες, ψηφιακές κρατήσεις και εφαρμογές για κινητά, η ασφάλεια στον κυβερνοχώρο έχει αναδειχθεί σε θεμελιώδη πυλώνα της λειτουργικής ακεραιότητας. Ακόμη και μία παραβίαση δεδομένων μπορεί να θέσει σε κίνδυνο ευαίσθητες πληροφορίες, να βλάψει τη φήμη σας και να οδηγήσει σε δαπάνη.

Πέρα από τις κυβερνοεπιθέσεις, ο τουρισμός αντιμετωπίζει μια αυξανόμενη απειλή από την παραπληροφόρηση, δηλαδή ψευδείς ή παραπλανητικές πληροφορίες που διαδίδονται γρήγορα στο διαδίκτυο. Ένα γνωστό παράδειγμα συνέβη μεταξύ 2015 και 2017, όταν διεθνή μέσα ενημέρωσης και διαδικτυακές πηγές διέδωσαν ψευδείς ισχυρισμούς σχετικά με τις λεγόμενες «απαγορευμένες ζώνες» στο Παρίσι, περιοχές που υποτίθεται ότι ελέγχονταν από εξτρεμιστές και δεν ήταν ασφαλείς για τους τουρίστες²³. Αν και διαψεύστηκε ευρέως, η φήμη αυτή διήρκεσε αρκετά ώστε να επηρεάσει αρνητικά την αντίληψη για την ασφάλεια, να μειώσει τον αριθμό των τουριστών και να βλάψει τις τοπικές επιχειρήσεις. Περιπτώσεις όπως αυτή υπογραμμίζουν τον τρόπο με τον οποίο οι ψευδείς ειδήσεις, ακόμη και όταν δεν στοχεύουν άμεσα μια συγκεκριμένη εταιρεία, μπορούν να διαταράξουν ολόκληρους προορισμούς και να προκαλέσουν μακροπρόθεσμη ζημιά στη φή.

Το έργο TREADS ανταποκρίνεται στην επείγουσα ανάγκη βελτίωσης **της ψηφιακής ανθεκτικότητας** στον τομέα του τουρισμού, με ιδιαίτερη έμφαση στις μικρές και πολύ μικρές επιχειρήσεις, οι οποίες είναι από τις πιο ευάλωτες στις κυβερνοαπειλές και τις ψηφιακές διαταραχές. Στο πλαίσιο των προτεραιοτήτων του έργου — ενίσχυση της ψηφιακής ετοιμότητας, της ανθεκτικότητας και της ικανότητας, καθώς και ευθυγράμμιση της επαγγελματικής εκπαίδευσης και

¹ Rometty, G. (2015). Το έγκλημα στον κυβερνοχώρο αποτελεί τη μεγαλύτερη απειλή για κάθε εταιρεία στον κόσμο. *Forbes*.
<https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>

κατάρτισης (ΕΕΚ) με τις τρέχουσες απαιτήσεις της αγοράς εργασίας— το παρόν παραδοτέο παρουσιάζει την ανάπτυξη ενός ολοκληρωμένου συνόλου πόρων.

Η δεξαμενή πόρων, η οποία αναπτύχθηκε στο πλαίσιο του πακέτου εργασίας 2, δραστηριότητα A4, και υπό την ηγεσία της ARCTUR, είναι μια πρακτική, δομημένη συλλογή υλικών που έχει σχεδιαστεί για να υποστηρίζει εκπαιδευτικούς, μαθητές και επαγγελματίες στους τομείς του τουρισμού και της ΕΕΚ. Περιλαμβάνει επιμελημένο περιεχόμενο σε βασικούς θεματικούς τομείς, όπως η κυβερνοασφάλεια, η παραπληροφόρηση, οι ψηφιακές δεξιότητες και τα πλαίσια πολιτικής.

Το παρόν παραδοτέο περιγράφει τη μεθοδολογία που χρησιμοποιήθηκε, την οργάνωση της τελικής ψηφιακής βιβλιοθήκης και τα αποτελέσματα της συνεργασίας μεταξύ των εταίρων του έργου για τη δημιουργία ενός υψηλής ποιότητας, φιλικού προς τον χρήστη και προσβάσιμου εκπαιδευτικού πόρου. Η ψηφιακή βιβλιοθήκη δίνει τη δυνατότητα στους επαγγελματίες του τουρισμού, τους εκπαιδευτικούς και τους μαθητές να παραμένουν ενημερωμένοι, να συμμορφώνονται με τους κανονισμούς και να είναι ψηφιακά ασφαλείς.

Στο πλαίσιο της εργασίας WP2/A4, αναλήφθηκε η ανάπτυξη ενός κοινού πόρου, ο οποίος σχεδιάστηκε ως μια δομημένη ψηφιακή βιβλιοθήκη με σκοπό την υποστήριξη της διδασκαλίας, της μάθησης και της έρευνας στο πλαίσιο της επαγγελματικής εκπαίδευσης και κατάρτισης (EEK).

Ο πρωταρχικός στόχος ήταν η συλλογή και η επιμέλεια ενός ευρέος φάσματος σχετικών υλικών — συμπεριλαμβανομένων εκπαιδευτικού περιεχομένου, ακαδημαϊκής έρευνας, μελετών περιπτώσεων, προγραμμάτων σπουδών EEK, αποτελεσμάτων από έργα που χρηματοδοτήθηκαν από την ΕΕ και κανονιστικών πλαισίων— που αφορούν τους βασικούς θεματικούς τομείς του έργου TREADS.

Η βάση δεδομένων δημιουργήθηκε με γνώμονα τις ακόλουθες **βασικές ανάγκες**:

1. **Ευαισθητοποίηση και ανθεκτικότητα στον τομέα της κυβερνοασφάλειας** – Προώθηση της κατανόησης και της ετοιμότητας έναντι των κυβερνοπειλών στον τομέα του τουρισμού.
2. **Κρίσιμη πληροφοριακή παιδεία** – Ενίσχυση της ικανότητας αξιολόγησης της αξιοπιστίας των πληροφοριών στην ψηφιακή εποχή.
3. **Αντιμετώπιση έκτακτων καταστάσεων και μετρίασμός κινδύνων** – Παροχή εργαλείων και στρατηγικών για τη διαχείριση κινδύνων και τον σχεδιασμό έκτακ.
4. **Εκπαίδευση στη γνώση των μέσων ενημέρωσης** – Υποστήριξη των επαγγελματιών στον εντοπισμό της παραπληροφόρησης και στη διατήρηση της ακεραιότητας.
5. **Αντιμετώπιση του χάσματος δεξιοτήτων** – Βοήθεια στις ΜΜΕ και τις πολύ μικρές επιχειρήσεις να προσαρμοστούν στην ψηφιακή και πράσινη μετάβαση μέσω της αναβάθμισης των δεξιοτήτων τους.
6. **Ασφάλεια δεδομένων και ηθική χρήση** – Διασφάλιση της νόμιμης και ηθικής διαχείρισης των δεδομένων των πελατών σε όλες τις τουριστικές δραστηριότητες.

ΟΙ Ομάδες-στόχοι για αυτόν τον πόρο περιλαμβάνουν εκπαιδευτικούς ΕΕΚ, μαθητές ΕΕΚ, επαγγελματίες του τουρισμού (ειδικά ΜΜΕ), ταξιδιώτες και το ευρύτερο κοινό.

Για να εξασφαλιστεί η συνέπεια και η θεματική συνάφεια, όλοι οι εταίροι του έργου συνέβαλαν στη συλλογή υλικού ακολουθώντας ένα κοινό σύνολο κατευθυντήριων γραμμών. Ζητήθηκε από κάθε εταίρο να συνεισφέρει τουλάχιστον 10 στοιχεία πόρων, καλύπτοντας 2-3 διαφορετικούς τύπους από τις διάφορες κατηγορίες, όπως εκπαιδευτικό υλικό (π.χ. σχέδια μαθήματος, εγχειρίδια, ενότητες ηλεκτρονικής μάθησης), ερευνητικές εργασίες (π.χ. άρθρα που έχουν αξιολογηθεί από ομοτίμους ή έγγραφα πολιτικής), μελέτες περιπτώσεων (π.χ. εφαρμοσμένα παραδείγματα που αναδεικνύουν βέλτιστες πρακτικές), προγράμματα σπουδών ΕΕΚ (π.χ. ενότητες σχετικές με την ασφάλεια στον κυβερνοχώρο, τις ψηφιακές δεξιότητες κ.λπ.), έργα που χρηματοδοτούνται από την ΕΕ (π.χ. αποτελέσματα, εκθέσεις ή περιλήψεις σχετικών πρωτοβουλιών) και κανονιστικά πλαίσια (π.χ. νομικά κείμενα, έγγραφα πολιτικής ή κατευθυντήριες γραμμές συμμόρφωσης). Όλοι οι πόροι έπρεπε να είναι άμεσα σχετικοί με το θεματικό επίκεντρο του TREADS, προσβάσιμοι (ανοικτής πρόσβασης ή με τα κατάλληλα δικαιώματα χρήσης) και εφαρμόσιμοι για εκπαιδευτικούς ή/και ερευνητικούς σκοπούς.

Οι πόροι υποβλήθηκαν με την εισαγωγή πληροφοριών σε ένα κοινόχρηστο φύλλο Excel, συνοδευόμενα από σύντομα μεταδεδομένα (συμπεριλαμβανομένου του τίτλου, του συγγραφέα/πηγής, του έτους έκδοσης και της συνάφειας), μαζί με έναν σύνδεσμο προς το υλικό ή μια άμεση μεταφόρτωση σε ψηφιακή μορφή (π.χ. PDF). Όλα τα υλικά συγκεντρώθηκαν και αποθηκεύτηκαν μέσω ενός κοινόχρηστου δίσκου. Αυτή η συστηματική και συνεργατική προσέγγιση εξασφάλισε την ποιότητα, την ποικιλομορφία και τη χρηστικότητα της Συλλογής Πόρων.



Σχήμα 1: Ψηφιακή βιβλιοθήκη πόρων: Διαδικασία ανάπτυξης

Μετά τη φάση συλλογής, όλα τα υλικά που υποβλήθηκαν εξετάστηκαν προσεκτικά για να διασφαλιστεί η θεματική ευθυγράμμιση, η ποιότητα και η συμμόρφωση με τις απαιτήσεις προσβασιμότητας και χρήσης. Αυτή η διαδικασία εξέτασης είχε ως στόχο τη διατήρηση ενός υψηλού επιπέδου συνάφειας και χρησιμότητας σε όλες τις συνεισφορές.

Στη συνέχεια, τα υλικά οργανώθηκαν συστηματικά σε τελικές θεματικές κατηγορίες, ώστε να εξασφαλιστεί η εύκολη πρόσβαση και η φιλική προς τον χρήστη πλοήγηση. Αυτή η δομή επιτρέπει την στοχευμένη εξερεύνηση βασικών θεμάτων και βοηθά τους χρήστες να εντοπίζουν γρήγορα το πιο σχετικό περιεχόμενο για τις συγκεκριμένες ανάγκες τους Ομαδοποιώντας τους πόρους σε συνεκτικά θέματα — όπως Κυβερνοαπειλές και Κυβερνοασφάλεια, Ψευδείς ειδήσεις και παραπληροφόρηση, Ψηφιακές δεξιότητες και εκπαίδευση, Πολιτική και κανονισμοί, Τεχνολογία και εργαλεία, Τουρισμός και πόροι για συγκεκριμένους τομείς, καθώς και Άλλα/Διατομεακά θέματα — η Ψηφιακή Βιβλιοθήκη βελτιώνει

την εμπειρία του χρήστη και αποτελεί ένα πρακτικό εργαλείο για εκπαιδευτικούς ΕΕΚ, μαθητές και επαγγελματίες του τουρισμού.

Η τελική έκδοση του Resource Pool, με τίτλο Digital Library, είναι διαθέσιμη [στο διαδίκτυο](#). Ενσωματώνει επιλεγμένους συνδέσμους, περιγραφές και υλικό που μπορεί να μεταφορτωθεί, προσφέροντας μια κεντρική πλατφόρμα που υποστηρίζει τη συνεχή μάθηση και την επαγγελματική ανάπτυξη στον τομέα του τουρισμού.

Η Συλλογή Πόρων συγκεντρώνει προσεκτικά επιλεγμένους πόρους που αφορούν βασικά θέματα σχετικά με τον ψηφιακό μετασχηματισμό στον τομέα του τουρισμού. Οργανωμένη σε θεματικές κατηγορίες, προσφέρει εύκολη πρόσβαση σε πολύτιμο υλικό που υποστηρίζει την εκπαίδευση, την έρευνα και την επαγγελματική ανάπτυξη. Αυτή η δομή βοηθά τους χρήστες να βρουν γρήγορα σχετικό περιεχόμενο προσαρμοσμένο στις ανάγκες των εκπαιδευτικών ΕΕΚ, των φοιτητών, των επαγγελματιών του τουρισμού και των ΜΜΕ.

3.1 Κυβερνοαπειλές και κυβερνοασφάλεια

Λέξεις-κλειδιά: κυβερνοεπιθέσεις, κυβερνοασφάλεια, κυβερνοέγκλημα, phishing.

Οι κυβερνοαπειλές, όπως το phishing, το κυβερνοέγκλημα και οι παραβιάσεις δεδομένων, αποτελούν σημαντικούς κινδύνους για τον τουριστικό τομέα, καθώς οι ψηφιακές πλατφόρμες γίνονται όλο και πιο αναπόσπαστο μέρος των επιχειρηματικών δραστηριοτήτων. Η αυξανόμενη συχνότητα των κυβερνοεπιθέσεων απαιτεί ενισχυμένα μέτρα κυβερνοασφάλειας για την προστασία ευαίσθητων δεδομένων και συστημάτων πελατών. Η εκπαίδευση και η ευαισθητοποίηση είναι καθοριστικής σημασίας για την καταπολέμηση αυτών των απειλών, με πρωτοβουλίες όπως το Σχέδιο Δράσης της ΕΕ για την Κυβερνοασφάλεια (2025) και το Πρόγραμμα AWARE (2024) να τονίζουν τη σημασία της κατάρτισης εξειδικευμένου εργατικού δυναμικού. Επιπλέον, η υιοθέτηση πλαισίων κυβερνοασφάλειας και η συμμόρφωση με κανονισμούς όπως ο ΓΚΠΔ είναι ζωτικής σημασίας για την προστασία της ιδιωτικής ζωής και τη διασφάλιση της επιχειρηματικής συνέχειας στον τομέα του τουρισμού και της φιλοξενίας.

Τα άρθρα και οι πρωτοβουλίες που ασχολούνται με αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- Agenda Digitale. (30 Ιανουαρίου 2025). Cybersecurity Italia: la mappa dei rischi 2025. Agenda Digitale.

<https://www.agendadigitale.eu/sicurezza/allarme-cyber-la-mappe-dei-rischi-per-imprese-e-istituzioni-nel-2025/>

- Blažič, B. J. (2021). Αλλαγή του τοπίου της εκπαίδευσης στον τομέα της κυβερνοασφάλειας στην ΕΕ: Θα παράγει η νέα προσέγγιση τις απαιτούμενες δεξιότητες στον τομέα της κυβερνοασφάλειας; Εκπαίδευση και τεχνολογίες πληροφοριών, 27. <https://doi.org/10.1007/s10639-021-10704-y>
- *Cyber Blueprint - Σχέδιο σύστασης του Συμβουλίου. (2025). Διαμορφώνοντας το ψηφιακό μέλλον της Ευρώπης.* <https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation>
- EFVET. (2024, 23 Ιανουαρίου). Διασφάλιση του μέλλοντος: Ο ρόλος του προγράμματος AWARE στην εκπαίδευση στην κυβερνοασφάλεια για την EEK - Ευρωπαϊκό Φόρουμ Τεχνικής και Επαγγελματικής Εκπαίδευσης και Κατάρτισης. EFVET - Ευρωπαϊκό Φόρουμ Επαγγελματικής Εκπαίδευσης και Κατάρτισης. <https://efvet.org/securing-the-future-the-aware-projects-role-in-cybersecurity-education-for-vet/>
- Ghaderi, Z., Beal, L., & L'Hocine Houanti. (2024). Απειλές για την ασφάλεια στον κυβερνοχώρο στον τουρισμό και τη φιλοξενία: προοπτικές από τουρίστες που χρησιμοποιούν υπηρεσίες κοινής οικονομίας. Τρέχοντα ζητήματα στον τουρισμό, 1-16. <https://doi.org/10.1080/13683500.2024.2353327>
- Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Πλαίσιο, εργαλεία και ορθές πρακτικές για προγράμματα σπουδών στον τομέα της κυβερνοασφάλειας. *IEEE Access*, 9, 94723-94747. <https://doi.org/10.1109/access.2021.3093952>
- *Εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια στο Διαδίκτυο.* (27 Ιανουαρίου 2022). Wikipedia. https://en.wikipedia.org/wiki/Internet_Security_Awareness_Training
- Ismail, S., Hattingh, M., & Matthee, M. (2024). Κατανόηση των προκλήσεων των ψευδών ειδήσεων στον τομέα του τουρισμού και των ταξιδιών: Μια συστηματική ανασκόπηση της βιβλιογραφίας. *Lecture Notes in Computer Science*, 371-382. https://doi.org/10.1007/978-3-031-72234-9_31

- Kumar, P. (2021). Τεχνολογία πληροφοριών για τη φιλοξενία και τον τουρισμό. USF M3 Publishing, LLC. <https://doi.org/10.5038/9781732127593>
- Labs, K. (23 Ιανουαρίου 2024). Καταπολέμηση των απειλών στον κυβερνοχώρο με εκπαίδευση σε θέματα ασφάλειας. Keepnet Labs. <https://keepnetlabs.com/blog/cybersecurity-and-the-tourism-sector-combatting-cyber-threats-with-security-awareness-training-and-human-risk-management>
- Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., & Ioannidis, S. (2020). Η κυβερνοασφάλεια στην εποχή της ψηφιακής μεταμόρφωσης: Η περίπτωση της Ελλάδας. Διεθνής Διάσκεψη για το Διαδίκτυο των Πραγμάτων και τις Έξυπνες Εφαρμογές (ITIA). <https://doi.org/10.1109/itia50152.2020.9312297>
- Magliulo, A. (2016). Κυβερνοασφάλεια και ανταγωνιστικότητα στον τουρισμό. Ευρωπαϊκό Περιοδικό Τουρισμού, Φιλοξενίας και Αναψυχής, 7(2), 128–134. <https://doi.org/10.1515/ejthr-2016-0015>
- Maria, & Giglio, C. (2024). Η ΚΥΒΕΡΝΗΤΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΡΕΥΝΑ ΓΙΑ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΤΟΥΡΙΣΜΟΥ ΚΑΙ ΤΗΣ ΦΙΛΟΞΕΝΙΑΣ: ΤΡΕΧΟΝΤΑ ΘΕΜΑΤΑ, ΤΑΣΕΙΣ ΚΑΙ ΑΓΕΝΔΑ ΓΙΑ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ. *Cuadernos de Turismo*, 53, 243–260. <https://doi.org/10.6018/turismo.616471>
- Martín, C. (2024, Νοέμβριος). Συμμόρφωση με τον ΓΚΠΔ στον τομέα του τουρισμού - LetsLaw. LetsLaw. <https://letslaw.es/en/compliance-gdpr-tourism-sector/>
- Panai, E. (2018). Ένα πλαίσιο κυβερνοασφάλειας για ανεξάρτητα ξενοδοχεία. 4η Ετήσια Διάσκεψη της EATSA – *Euro-Asia Tourism Studies Association*. https://www.researchgate.net/publication/325780143_A_Cyber_Security_Framework_for_Independent_Hotels
- Pankaj, H. (2025). Κυβερνοασφάλεια και προστασία δεδομένων στον κλάδο της φιλοξενίας και του τουρισμού: Αποκαλύπτοντας τις προκλήσεις και τη στρατηγική μετριασμού των κινδύνων: Μια επισκόπηση της έρευνας. Διεθνές Περιοδικό Επιστήμης και Έρευνας (IJSR), 14(2), 354–362. <https://doi.org/10.21275/sr25205142950>

- Paraskevas, A. (ανουάριος 2020). (PDF) Κυβερνοασφάλεια στον τομέα των ταξιδιών και του τουρισμού: Μια προσέγγιση βασισμένη στον κίνδυνο. ResearchGate.
https://www.researchgate.net/publication/342123867_Cybersecurity_in_Travel_and_Tourism_A_Risk-based_Approach
- Πιπίρος, Κ. & Λιασίδου, Σ. (2025). Ένα νέο πλαίσιο αξιολόγησης κινδύνων κυβερνοασφάλειας για τον κλάδο της φιλοξενίας: τεχνικές και μέθοδοι για ενισχυμένη προστασία δεδομένων και μετριασμό απειλών. Παγκόσμια θέματα φιλοξενίας και τουρισμού. <https://doi.org/10.1108/whatt-12-2024-0296>
- Rajendra Kumar SETHIA. (27 Ιουνίου 2024). Προσαρμογή της εκπαίδευσης στον τομέα της κυβερνοασφάλειας στις ευρωπαϊκές τάξεις EEK στις τρέχουσες ανάγκες των ΜΜΕ. EPALE - Ευρωπαϊκή Επιτροπή; EPALE - Ηλεκτρονική Πλατφόρμα για Εκπαίδευσης Εκπαίδευσης στην. <https://epale.ec.europa.eu/en/content/aligning-cybersecurity-education-european-vet-classrooms-current-needs-smes>
- RED TANDEM PLUS, & CYBER.VET.EU. (2018). *Εγχειρίδιο CYBER.VET.EU*. Cybervet.eu. https://cybervet.eu/es/outputs/io4-the-cybersecurity-handbook-for-vet-institutions/?get_page=fileviewer&file=https://cybervet.eu/openfile/MTY3NTYxMDQwM19DWUJFU5WRVQuRVUgSGFuZGJvb2sgU1BBTk1TSC5wZGY=?PHPSESSID=oacsqkhkak3tphon033mgv050i&PHPSESSID=oacsqkhkak3tphon033mgv050i
- Shabani, N., & Munir, A. (2020). Μια ανασκόπηση των ζητημάτων κυβερνοασφάλειας στον κλάδο της φιλοξενίας. *Advances in Intelligent Systems and Computing*, 1230, 482–493. Researchgate. https://doi.org/10.1007/978-3-030-52243-8_35
- Šilak, G., & Bobek, S. (2025). Kibernetiska varnost. *Dk.um.si*. <https://dk.um.si/Dokument.php?lang=slv&id=168548&dn=>

3.2 Ψευδείς Ειδήσεις Και Παραπληροφόρηση

Λέξεις-κλειδιά: παραπληροφόρηση, ψευδείς ειδήσεις, πόλεμος πληροφοριών, χειραγώγηση των κοινωνικών μέσων.

Οι ψευδείς ειδήσεις και η παραπληροφόρηση αποτελούν σημαντικές προκλήσεις στον τομέα του τουρισμού, επηρεάζοντας συχνά τις αποφάσεις των καταναλωτών και τη φήμη των εμπορικών σημάτων. Η αύξηση της χειραγώγησης των κοινωνικών μέσων και του πληροφοριακού πολέμου επιδεινώνει αυτά τα ζητήματα, με την ψευδή διαφήμιση και τις παραπλανητικές αφηγήσεις να γίνονται όλο και πιο διαδεδομένες (Abdallah, 2021; Anton et al., 2020). Ο αντίκτυπος των ψευδών ειδήσεων στη συμπεριφορά των πελατών, όπως η αλλαγή των ταξιδιωτικών σχεδίων ή η διάδοση αρνητικών κριτικών, μπορεί να βλάψει τις επιχειρήσεις, ιδίως στον τομέα της φιλοξενίας (Nassar et al., 2023). Οι ερευνητές τονίζουν την ανάγκη για πιο αποτελεσματικά μοντέλα επαλήθευσης των γεγονότων και crowdsourcing για την καταπολέμηση της παραπληροφόρησης (Lamprou et al., 2021). Καθώς η ψηφιακή παραπληροφόρηση αυξάνεται, η αντιμετώπιση των συνεπειών της είναι ζωτικής σημασίας για τη διατήρηση της εμπιστοσύνης και της σταθερότητας στον τουριστικό κλάδο.

Τα άρθρα και οι πρωτοβουλίες που συζητούν αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- Abdallah, A. (2021). ΨΕΥΤΙΚΕΣ ΕΙΔΗΣΕΙΣ, ΨΕΥΤΙΚΗ ΔΙΑΦΗΜΙΣΗ, ΚΟΙΝΩΝΙΚΑ ΜΕΣΑ ΚΑΙ Η ΤΟΥΡΙΣΤΙΚΗ ΒΙΟΜΗΧΑΝΙΑ. Διεθνές Περιοδικό Έρευνας για την Ανάπτυξη, 11(7), 48999–49003. <https://doi.org/10.37118/ijdr.xxxxx.05.2021>
- Anton, E., Teodorescu, C. A., & Vargas, V. M. (2020) Προοπτικές και ανασκοπήσεις στη χρήση αφηγηματικών στρατηγικών για την επικοινωνία ψευδών ειδήσεων στον τουριστικό κλάδο. Πρακτικά του Διεθνούς Συνεδρίου για την Επιχειρηματική Αριστεία, 14(1), 728–734. <https://doi.org/10.2478/picbe-2020-0069>
- Fedeli, G. (2019). Οι «ψευδείς ειδήσεις» συναντούν τον τουρισμό: μια προτεινόμενη ερευνητική ατζέντα. Annals of Tourism Research, 102684. <https://doi.org/10.1016/j.annals.2019.02.002>
- Lamprou, E., Antonopoulos, N., Anomeritou, I., & Apostolou, C. (2021). Χαρακτηριστικά των ψευδών ειδήσεων και της παραπληροφόρησης στην Ελλάδα: Η άνοδος των νέων μοντέλων δημοσιογραφικής επαλήθευσης των γεγονότων με βάση το crowdsourcing. Journalism and Media, 2(3), 417–439. <https://doi.org/10.3390/journalmedia2030025>
- MedDMO. (28 Μαρτίου 2023). Το MedDMO με μια ματιά - MEDDMO. MEDDMO. <https://meddmo.eu/about-us/meddmo-at-a-glance/>

- Nassar, M. A., Elsaqqa, M., & Hagra, S. (2023). Επίδραση της ψηφιακής παραπληροφόρησης στην ανταπόκριση των πελατών ξενοδοχείων: Επισκόπηση και μελλοντικές κατευθύνσεις έρευνας. *Pharos International Journal of τουρισμού και Φιλοξενίας*, 2(2), 61–71. <https://doi.org/10.21608/pijth.2023.332020>
- Stupavský, I., Dakić, P., & Vranić, V. (2023). Η επίδραση των ψευδών ειδήσεων στα ταξίδια και την αντικοινωνική συμπεριφορά στις διαδικτυακές κοινότητες: Επισκόπηση. *Εφαρμοσμένες Επιστήμες*, 13(21), 11719–11719. <https://doi.org/10.3390/app132111719>

3.3 Ψηφιακές Δεξιότητες Και Εκπαίδευση

Λέξεις-κλειδιά: κατάρτιση, εκπαίδευση, ανάπτυξη ικανοτήτων, ψηφιακή παιδεία.

Οι ψηφιακές δεξιότητες και η εκπαίδευση είναι απαραίτητες για το εργατικό δυναμικό του τουρισμού, ώστε να συμβαδίζει με τις τεχνολογικές εξελίξεις και να ανταποκρίνεται στις απαιτήσεις των σύγχρονων ταξιδιωτών. Ο τουριστικός τομέας απαιτεί συνεχή ανάπτυξη ικανοτήτων σε τομείς όπως η ψηφιακή παιδεία, η διαχείριση δεδομένων και το διαδικτυακό μάρκετινγκ. Εκθέσεις όπως αυτή του Υπουργείου Τουρισμού της Ελλάδας (2021) υπογραμμίζουν τον κρίσιμο ρόλο των ψηφιακών δεξιοτήτων στη βελτίωση της παροχής υπηρεσιών και στην ενίσχυση της ανταγωνιστικότητας του κλάδου.

Επιπλέον, πρωτοβουλίες που εστιάζουν στον αειφόρο τουρισμό και τον χωροταξικό σχεδιασμό, όπως το SPOT (2021) και το Low Carbon Travel (2021), τονίζουν τη σημασία της ψηφιακής κατάρτισης για την προώθηση πρακτικών οικολογικού τουρισμού. Καθώς ο κλάδος προσαρμόζεται στον ψηφιακό μετασχηματισμό, η επένδυση στην εκπαίδευση και την κατάρτιση είναι ζωτικής σημασίας τόσο για τους εργαζομένους όσο και για τις επιχειρήσεις, προκειμένου να ευδοκμήσουν σε ένα ταχέως εξελισσόμενο περιβάλλον.

Τα άρθρα και οι πρωτοβουλίες που ασχολούνται με αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων. (30 Ιανουαρίου 2024). Δημοσιεύσεις και δεδομένα. Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων. https://www.ecdc.europa.eu/en/publications-data?f%5B0%5D=output_types%3A1244

- Ταξίδια με χαμηλές εκπομπές άνθρακα. (2021). Ταξίδια με χαμηλές εκπομπές άνθρακα - ATRE. Ταξίδια με χαμηλές εκπομπές άνθρακα. <https://www.lowcarbontravel.net/en>
- Υπουργείο Τουρισμού της Ελλάδας. (2021). Έκθεση σχετικά με τις ψηφιακές δεξιότητες του εργατικού δυναμικού στον τομέα του τουρισμού στην Ελλάδα: Κρίσιμα ζητήματα και πολιτικές απαντήσεις. Υπουργείο Τουρισμού της Ελλάδας.
- SPOT (2 Δεκεμβρίου 2021). SPOT. Βιώσιμη χωροταξική σχεδιασμός τουριστικών προορισμών. Βιώσιμη χωροταξική σχεδιασμός τουριστικών προορισμών. <https://spot-erasmus.eu/>

3.4 Πολιτική & Κανονισμοί

Λέξεις-κλειδιά: νομοθεσία, πλαίσια, στρατηγικές, διακυβέρνηση.

Η αποτελεσματική πολιτική και η ρύθμιση είναι ζωτικής σημασίας για τη διαχείριση των προκλήσεων του ψηφιακού μετασχηματισμού και της κυβερνοασφάλειας στον τομέα του τουρισμού. Η οδηγία NIS2 (2023) της Ευρωπαϊκής Επιτροπής τονίζει την ανάγκη για κοινά πρότυπα κυβερνοασφάλειας σε όλα τα κράτη μέλη της ΕΕ, εξασφαλίζοντας υψηλό επίπεδο προστασίας για τις κρίσιμες υποδομές σε διάφορους τομείς, συμπεριλαμβανομένου του τουρισμού. Τα εθνικά πλαίσια, όπως οι νέοι νόμοι της Ελλάδας για την κυβερνοασφάλεια (Νόμος 5086/2024), ενισχύουν περαιτέρω τη διακυβέρνηση και την ανταπόκριση στις κυβερνοαπειλές. Νομοθεσίες όπως ο κανονισμός 2019/881 της ΕΕ και ο κανονισμός 2025/37 εστιάζουν στην ανάπτυξη και την εφαρμογή ισχυρών ψηφιακών υποδομών για την αντιμετώπιση των αναδυόμενων κινδύνων. Αυτές οι ρυθμιστικές προσπάθειες διαδραματίζουν καθοριστικό ρόλο στη διασφάλιση της ασφάλειας, της ιδιωτικότητας και της βιωσιμότητας των ψηφιακών πλατφορμών στον τουριστικό κλάδο.

Η νομοθεσία που αφορά τα θέματα αυτά είναι διαθέσιμη παρακάτω.

- Ευρωπαϊκή Επιτροπή. (14 Σεπτεμβρίου 2023). Οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας στον κυβερνοχώρο σε ολόκληρη την Ένωση (Οδηγία NIS2) | Διαμορφώνοντας το ψηφιακό μέλλον της Ευρώπης. Digital-Strategy.ec.europa.eu. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

- *Gazzetta Ufficiale*. (2024). *Gazzettaufficiale.it*. <https://www.gazzettaufficiale.it/eli/id/2024/07/02/24G00108/SG>
- Mariotti, G., Panai, E., & Camerada, M. (n.d.). Ανακτήθηκε στις 6 Μαΐου 2025, από https://www.ageiweb.it/geotema/wp-content/uploads/2019/10/Suppl2018_7_Mariotti_Panai_Camerada.pdf
- *Νόμος 5086/2024 - Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις*. (2024). Taxheaven | Φορολογικό αρχείο. <https://www.taxheaven.gr/law/5086/2024>
- *Κανονισμός - 2019/881 - EN - EUR-Lex*. (2019). Europa.eu. <https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng>
- *Κανονισμός - EE - 2025/37 - EN - EUR-Lex*. (2025). Europa.eu. <https://eur-lex.europa.eu/eli/reg/2025/37/oj/eng>

3.5 Τεχνολογία & Εργαλεία

Λέξεις-κλειδιά: τεχνητή νοημοσύνη, αλυσίδα μπλοκ, ψηφιακές πλατφόρμες, τεχνικές.

Οι τεχνολογικές καινοτομίες, όπως η τεχνητή νοημοσύνη, η αλυσίδα μπλοκ και οι ψηφιακές πλατφόρμες, μετασχηματίζουν τον τουριστικό κλάδο, βελτιώνοντας την εμπειρία των πελατών και την επιχειρησιακή αποδοτικότητα. Η πρωτοβουλία Tourism Digital Hub (2022) υπογραμμίζει τον ρόλο της ψηφιακής υποδομής στην υποστήριξη των τουριστικών επιχειρήσεων με προηγμένες τεχνικές λύσεις. Εργαλεία όπως η τεχνητή νοημοσύνη (AI) επιτρέπουν εξατομικευμένες ταξιδιωτικές εμπειρίες, ενώ η τεχνολογία blockchain προσφέρει ασφαλείς συναλλαγές και διαφανή συστήματα κρατήσεων. Η έρευνα των Pencarelli et al. (2021) εξετάζει πώς τα ψηφιακά εργαλεία, ιδίως μεταξύ των Ιταλών της γενιάς των millennials, αναδιαμορφώνουν τη συμπεριφορά και τις προσδοκίες των ταξιδιωτών. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, θα διαδραματίσει καθοριστικό ρόλο στην προώθηση της καινοτομίας και της βιωσιμότητας.

Τα άρθρα που αναλύουν αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- *M1C3 Investimento 4.1: Τουριστικός ψηφιακός κόμβος*. (11 Μαΐου 2022). -. <https://www.ministeroturismo.gov.it/tourism-digital-hub/>

- PENCARELLI, T., GABBIANELLI, L., & SAVELLI, E. (2021). Η τουριστική εμπειρία στην ψηφιακή εποχή: η περίπτωση των Ιταλών της γενιάς των millennials. *Sinergie Italian Journal of Management*, 38(3), 165–190. <https://doi.org/10.7433/s113.2020.10>
- ΟΟΣΑ (2024), Τεχνητή νοημοσύνη και τουρισμός: έγγραφο πολιτικής G7/ΟΟΣΑ, Έγγραφο τουρισμού ΟΟΣΑ, αρ. 2024/02, Εκδόσεις ΟΟΣΑ, Παρίσι. <https://doi.org/10.1787/3f9a4d8d-en>
- Balasubramanian, S., Sethi, J.S., Ajayan, S. et al. (2022). Ένα ευνοϊκό πλαίσιο για την αλυσίδα μπλοκ στον τουρισμό. *Τεχνολογία πληροφοριών και τουρισμός* 24, 165–179. <https://doi.org/10.1007/s40558-022-00229-6>
- Zeqiri A, Ben Youssef A, Maherzi Zahar T. (2025). Ο ρόλος των ψηφιακών τουριστικών πλατφορμών στην προώθηση των στόχων βιώσιμης ανάπτυξης στην εποχή της Βιομηχανίας 4.0. *Βιωσιμότητα*. 17(8): 3482. <https://doi.org/10.3390/su17083482>

3.6 Τουρισμός Και Πόροι Για Συγκεκριμένους Τομείς

Πόροι ειδικά για τον τουρισμό, τα ταξίδια και τη φιλοξενία.

Οι κλάδοι του τουρισμού και της φιλοξενίας αντιμετωπίζουν μοναδικές προκλήσεις στον τομέα της κυβερνοασφάλειας, με αυξανόμενη ανάγκη προστασίας των δεδομένων των πελατών και των ψηφιακών υποδομών. Οι πόροι που αφορούν συγκεκριμένα αυτούς τους κλάδους εστιάζουν στη βελτίωση της ανθεκτικότητας στον κυβερνοχώρο και στην ασφάλεια των διαδικτυακών πλατφορμών. Μελέτες όπως αυτές των Ghaderi et al. (2024) και Divya (2022) υπογραμμίζουν τη σημασία της προστασίας των δεδομένων των χρηστών στις έξυπνες πόλεις και στον κλάδο της φιλοξενίας. Η ανάπτυξη στρατηγικών ανθεκτικότητας στον κυβερνοχώρο για τις τουριστικές επιχειρήσεις τονίζεται σε πόρους όπως το Codes to Resilience (2025) και το Cybersecurity in Tourism & Hospitality (2020), τα οποία περιγράφουν τις βέλτιστες πρακτικές για τον μετριασμό των κινδύνων και τη διατήρηση της εμπιστοσύνης των πελατών.

Διάφορες πρωτοβουλίες του κλάδου, όπως το Deploytour (2024) και οι κατευθυντήριες γραμμές της ισπανικής κυβέρνησης για την ασφάλεια στον κυβερνοχώρο στον τομέα του τουρισμού (2024), παρέχουν πλαίσια και εργαλεία για τη βελτίωση της ασφάλειας στον κυβερνοχώρο στον κλάδο. Η ενσωμάτωση

μέτρων ασφάλειας στον κυβερνοχώρο σε διαδικτυακά ταξιδιωτικά γραφεία και ξενοδοχεία, όπως συζητήθηκε από τον Florido-Benítez (2024), είναι απαραίτητη για την προστασία των προσωπικών δεδομένων των χρηστών. Καθώς οι τουριστικοί προορισμοί εξελίσσονται σε έξυπνες πόλεις, η διασφάλιση της ανθεκτικότητάς τους στον κυβερνοχώρο είναι κρίσιμη για τη διατήρηση της ανάπτυξης και.

Τα άρθρα και οι πρωτοβουλίες που συζητούν αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- Aljohani, W., & Elfadil. (2020). Μέτρηση της ευαισθητοποίησης των φοιτητών σε θέματα κυβερνοασφάλειας: Μια μελέτη περίπτωσης στο Πανεπιστήμιο Fahad Bin Sultan. Διεθνές Περιοδικό Επιστήμης Υπολογιστών και Κινητής Πληροφορικής, 9(6), 141–155. <https://ijcsmc.com/docs/papers/June2020/V9I6202038.pdf>
- Carreira, D. (11 Νοεμβρίου 2022). Κυβερνοανθεκτικότητα, μια έρευνα μελετών περίπτωσης. Academia.edu. [https://www.academia.edu/90518927/Cyber Resilience a Survey of Case Studies](https://www.academia.edu/90518927/Cyber_Resilience_a_Survey_of_Case_Studies)
- Κώδικες ανθεκτικότητας: Κυβερνοανθεκτικότητα στον τομέα των ταξιδιών και του τουρισμού. (2025). Thinkdigital.travel. <https://www.thinkdigital.travel/research-directory/codes-to-resilience-cyber-resilience-in-travel-and-tourism>
- Κυβερνοασφάλεια στον τουρισμό και τη φιλοξενία: η ανάγκη προστασίας των δεδομένων των πελατών. (13 Φεβρουαρίου 2020). NTG. <https://nexttourismgeneration.eu/cybersecurity-in-tourism-hospitality-the-urge-of-protecting-customer-data/>
- Deploytour. (2024). Deploytour. <https://deploytour.eu/>
- Divya. (21 Φεβρουαρίου 2022). Η σημασία της προστασίας των δεδομένων στον τομέα του τουρισμού και της φιλοξενίας. OmniCyber Security. <https://www.omnicybersecurity.com/importance-of-protecting-data-tourism-hospitality-industry/>
- Ενδυναμωμένες ζωές. Ανθεκτικές χώρες. Έξυπνος τουρισμός: Ο δρόμος προς πιο ασφαλείς και ανθεκτικούς προορισμούς. (n.d.). Ανακτήθηκε Μάιος 6 2025,

από https://www.itu.int/en/publications/Documents/tsb/2022-U4SSC-Smart-tourism/files/downloads/22-00512-U4SSC_Smart%20tourism-E.pdf

- Florido-Benítez, L. (2024). Η ασφάλεια στον κυβερνοχώρο που εφαρμόζουν τα διαδικτυακά ταξιδιωτικά πρακτορεία και τα ξενοδοχεία για την προστασία των προσωπικών δεδομένων των χρηστών στις έξυπνες πόλεις. Έξυπνες πόλεις, 7(1), 475–495. <https://www.mdpi.com/2624-6511/7/1/19>
- Fragnière, E., & Yagci, K. (Eds.). (n.d.). Ασφάλεια δικτύων και κυβερνοχώρου στον τομέα της φιλοξενίας και του τουρισμού. Τεχνολογία πληροφοριών φιλοξενίας και τουρισμού. <https://arodes.hes-so.ch/record/9164?v=pdf>
- Ghaderi, Z., Beal, L., Hall, C. M., Zaman, M., Rather, R. A., & Puad, A. (2024). Κυβερνοασφάλεια και ανθεκτικότητα έξυπνων τουριστικών προορισμών. Έρευνα για τον τουρισμό και την αναψυχή, 1–17. <https://doi.org/10.1080/02508281.2024.2434791>
- Kumar, P. (2021). Τεχνολογία πληροφοριών για τη φιλοξενία και τον τουρισμό. USF M3 Publishing, LLC. <https://doi.org/10.5038/9781732127593>
- Maria, & Giglio, C. (2024). ΕΡΕΥΝΑ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΗΤΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΤΟΥΡΙΣΜΟ ΚΑΙ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΦΙΛΟΞΕΝΙΑΣ: ΤΡΕΧΟΝΤΑ ΘΕΜΑΤΑ, ΤΑΣΕΙΣ ΚΑΙ ΑΓΕΝΔΑ ΓΙΑ ΤΟ ΜΕΛΛΟΝ ΕΡΕΥΝΑ. *Cuadernos de Turismo*, 53, 243–260. <https://doi.org/10.6018/turismo.616471>
- Palou, N. (21 Οκτωβρίου 2024). Κυβερνοανθεκτικότητα του τουριστικού τομέα: προκλήσεις και βέλτιστες πρακτικές. Telefónica Tech; Telefónica Tech S.L.U. <https://telefonicatech.com/en/blog/cyber-resilience-tourism-sector>
- Sanger, D. E. (12 Δεκεμβρίου 2018). Κυβερνοεπίθεση κατά της Marriott: Παραβίαση δεδομένων ξενοδοχείου που έπληξε 500 εκατομμύρια επισκέπτες συνδέθηκε με κινεζική υπηρεσία κατασκοπείας| The Independent. <https://www.independent.co.uk/tech/marriott-cyber-attack-starwood-hotel-data-breach-china-spy-agency-guests-a8679006.html>
- Scollo, J. (18 Ιουνίου 2024). Ciberseguridad, un desafío vital para las empresas turísticas en la era. Ladevi; Ladevi Medios y Soluciones. <https://espana.ladevi.info/ciberseguridad/ciberseguridad-un-desafio-vital-las-empresas-turisticas-la-era-digital-n67450>

- Ισπανική κυβέρνηση, INCIBE και Segittur. (2024). *Cyberseguridad en el sector turístico y de ocio*. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-turismo-ocio.pdf>

3.7 Άλλα / Διατομεακά Θέματα

Τα διατομεακά ζητήματα στον τομέα του τουρισμού συχνά διασταυρώνονται με την κυβερνοασφάλεια, την ψηφιακή παιδεία και τη διαχείριση δεδομένων. Μια βασική πρωτοβουλία είναι το έργο DATES (n.d.), το οποίο επικεντρώνεται στη δημιουργία ενός Ευρωπαϊκού Χώρου Δεδομένων για τον Τουρισμό, με στόχο την ενίσχυση της ανταλλαγής δεδομένων και της συνεργασίας σε ολόκληρο τον τουριστικό κλάδο. Η ενσωμάτωση τεχνολογιών όπως η τεχνητή νοημοσύνη (Karoo, 2024) διαδραματίζει σημαντικό ρόλο στη βελτίωση της κυβερνοασφάλειας και της παροχής υπηρεσιών, ιδίως στον τομέα της φιλοξενίας και του τουρισμού. Επιπλέον, η παιδεία στα μέσα επικοινωνίας και την πληροφορία (YouTube, 2023) αποκτά όλο και μεγαλύτερη σημασία τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις, προκειμένου να πλοηγούνται με ασφάλεια στον ψηφιακό κόσμο.

Οι παραβιάσεις δεδομένων παραμένουν ένα επείγον ζήτημα, όπως επισημαίνει ο Tariq (2024), ο οποίος διερευνά στρατηγικές πρόληψης στον κλάδο της φιλοξενίας. Καθώς αυτά τα διατομεακά θέματα συνεχίζουν να εξελίσσονται, υπογραμμίζουν την ανάγκη για μια ολοκληρωμένη προσέγγιση στη διαχείριση των δεδομένων, της ασφάλειας και της τεχνολογίας στον τομέα του τουρισμού.

Τα άρθρα και οι πρωτοβουλίες που συζητούν αυτά τα θέματα είναι διαθέσιμα παρακάτω.

- Έργο DATES Χώρος δεδομένων τουρισμού Ευρωπαϊκός χώρος δεδομένων τουρισμού - Έργο DATES Έργο Dates. (χ.χ.). Έργο DATES. <https://www.tourismdataspace-csa.eu/>
- Karoo, V. (2024). Τεχνητή νοημοσύνη και κυβερνοασφάλεια στον τομέα των υπηρεσιών. Apple Academic Press EBooks, 265–303. <https://doi.org/10.1201/9781003432951-17>

- Πολίτες με γνώση των μέσων ενημέρωσης και της πληροφορίας: Σκεφτείτε κριτικά, κάντε κλικ με σύνεση! (χ.χ.). Wwww.youtube.com. Ανακτήθηκε στις 3 Αυγούστου 2023, από <https://youtu.be/bjYhmTC3lrc>
- Tariq, M. U. (2024). Περιστατικά παραβίασης δεδομένων και πρόληψη στον κλάδο της φιλοξενίας. Σειρά βιβλίων Advances in Hospitality, Tourism and the Services Industry (AHTSI), 181–199. <https://doi.org/10.4018/979-8-3693-2715-9.ch010>

ΠΡΟΣΑΡΜΟΓΗ ΚΑΙ ΤΟΠΟΘΕΤΗΣΗ ΤΗΣ ΨΗΦΙΑΚΗΣ ΒΙΒΛΙΟΘΗΚΗΣ ΣΤΟΝ ΙΣΤΟΤΟΠΟ ΤΟΥ TREADS

Σε συμφωνία με τη δομή και τις τεχνικές δυνατότητες του ιστότοπου του έργου TREADS, η συλλογή πόρων με τίτλο «Ψηφιακή βιβλιοθήκη» προσαρμόστηκε και καταστάθηκε προσβάσιμη στο διαδίκτυο. Σε συνεργασία με την GAIA, τον εταίρο που είναι υπεύθυνος για την ανάπτυξη και τη συντήρηση του ιστότοπου του έργου, κάθε θεματική κατηγορία των συλλεγμένων υλικών συγκεντρώθηκε σε ένα ειδικό έγγραφο PDF. Αυτά τα έγγραφα περιλαμβάνουν επιλεγμένους συνδέσμους προς σχετικούς πόρους και εξασφαλίζουν μια φιλική προς τον χρήστη παρουσίαση του περιεχομένου.

Η προσαρμογή αυτή εξασφαλίζει τη μακροπρόθεσμη προσβασιμότητα και πρακτική χρήση των αποτελεσμάτων του έργου, υποστηρίζοντας τους επαγγελματίες του τουρισμού, τους εκπαιδευτικούς και τις ΜΜΕ στην ανάπτυξη σχετικών ψηφιακών δεξιοτήτων. Η δομημένη παρουσίαση των υλικών επιτρέπει τη στοχευμένη πλοήγηση σε βασικούς θεματικούς τομείς και προάγει την ευρύτερη διάδοση και τον αντίκτυπο των αποτελεσμάτων του έργου.

Η Ψηφιακή Βιβλιοθήκη είναι διαθέσιμη στο κοινό και μπορείτε να την επισκεφθείτε μέσω του ακόλουθου συνδέσμου: <https://treadsproject.eu/resource-pool/>.



[PROJECT DESCRIPTION](#)
[PARTNERS](#)
[RESOURCES ▾](#)
[NEWS AND EVENTS](#)
[CONTACT](#)

English ▾

Digital Library



The tourism sector is changing rapidly, and staying ahead means being well informed. The Digital Library of **TREADS** brings together essential knowledge, tools, and key ideas to help you and your organization thrive in a digital world. Explore a curated collection of articles, frameworks, and best practices addressing topics such as cybersecurity, digital skills, policies, and more, all tailored to the needs of tourism professionals, educators, and SMEs.

Whether you're looking to improve your digital capabilities, protect your business from cyber threats, or build a smarter, more resilient tourism future, this is your starting point.

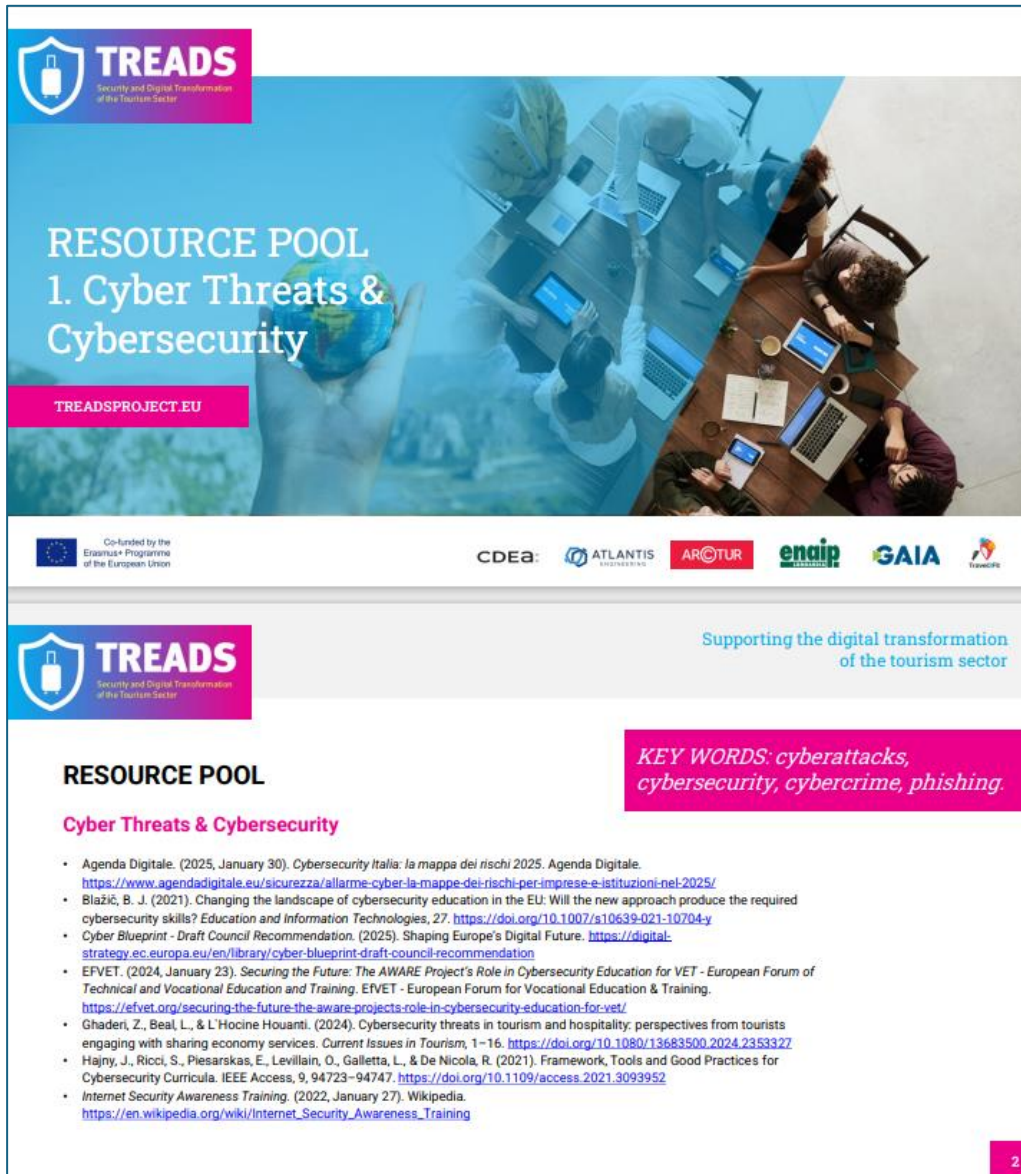
Discover knowledge. Develop skills. Shape the future.

▼ **Cyber Threats and Cybersecurity**
Keywords : cyberattacks, cybersecurity, cybercrime, phishing
 Cyberthreats, such as phishing, cybercrime, and data breaches, pose significant risks to the tourism sector, especially as digital platforms become more essential to business operations. The increased frequency of cyberattacks calls for strengthened cybersecurity measures to protect sensitive customer data and systems. Education and awareness are key to combating these threats, with initiatives such as the **EU Cyber Blueprint (2025)** and **Project AWARE (2024)** highlighting the importance of developing a skilled workforce. Furthermore, adopting cybersecurity frameworks and complying with regulations such as the **GDPR** are critical to protecting privacy and ensuring business continuity in the tourism and hospitality industries.

Articles and initiatives addressing these topics are available [here](#).

► **Fake News and Disinformation**
Keywords : disinformation, fake news, information warfare, social media manipulation.

Σχήμα 2: Ψηφιακή βιβλιοθήκη στον ιστότοπο του TREADS



Σχήμα 3: Παράδειγμα αρχείου PDF για κάθε κατηγορία

Οι τουριστικές εταιρείες διαχειρίζονται τεράστιες ποσότητες προσωπικών και οικονομικών δεδομένων, από στοιχεία διαβατηρίων έως πληροφορίες πιστωτικών καρτών. Μια μόνο παραβίαση μπορεί να βλάψει τη φήμη, να υπονομεύσει την εμπιστοσύνη των πελατών και να οδηγήσει σε σοβαρές νομικές και οικονομικές συνέπειες. Σε μια εποχή όπου οι ψηφιακές κρατήσεις, οι διαδικτυακές κριτικές και οι εφαρμογές για κινητά καθορίζουν την ταξιδιωτική εμπειρία, η κυβερνοασφάλεια πρέπει να μετακινηθεί από το παρασκήνιο στο προσκήνιο της επιχειρηματικής στρατηγικής. Η προστασία των επισκεπτών ξεκινά με την προστασία των δεδομένων τους. Αυτός είναι ακριβώς ο λόγος για τον οποίο δημιουργήθηκε η Ψηφιακή Βιβλιοθήκη: για να ενημερώσει τις τουριστικές εταιρείες σχετικά με τους κινδύνους, τις βέλτιστες πρακτικές και τις λύσεις στον τομέα της κυβερνοασφάλειας, όλα σε μία κεντρική και εύκολα προσβάσιμη πλατφόρμα. Δίνει τη δυνατότητα στις επιχειρήσεις να παραμένουν ενημερωμένες, συμμορφωμένες και ασφαλείς σε έναν όλο και πιο ψηφιακό κόσμο.



 treadsproject.eu

 [treads-project](https://www.linkedin.com/company/treads-project)

 [Treads Project](https://www.facebook.com/Treads-Project)

 [treadsprojecteu](https://www.instagram.com/treadsprojecteu)



Co-funded by the
European Union

Co-funded by the European Union. The opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union nor the granting authority can be held responsible for them