

Ανάπτυξη Ψηφιακών Δεξιοτήτων



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Coordinator:

MMC Mediterranean
Management Centre

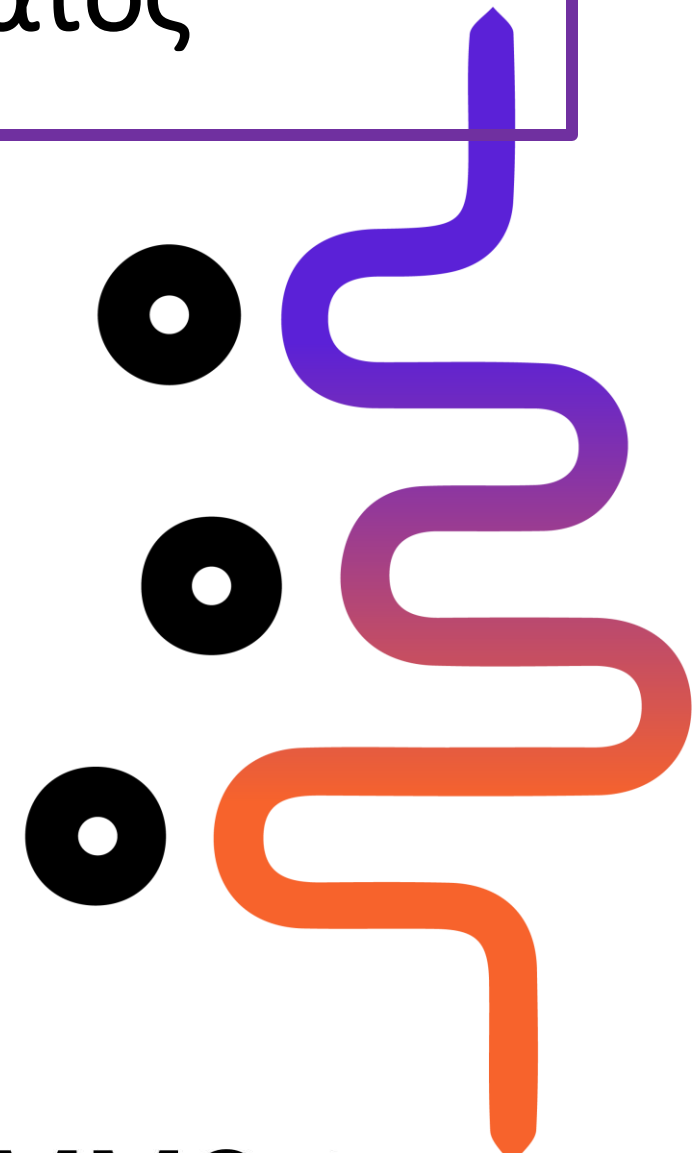
Partners:



Στόχοι του Μαθήματος

Σε επίπεδο γνώσεων:

- Να εντοπίζουν τους συνηθισμένους ψηφιακούς κινδύνους στον χώρο εργασίας και να εξηγούν τις επιπτώσεις τους στον οργανισμό.
- Να κατανοούν και να εφαρμόζουν τις βασικές αρχές του GDPR σε καθημερινές εργασιακές καταστάσεις.
- Να διακρίνουν και να επιλέγουν δομημένους τρόπους για τη διαχείριση ψηφιακών πληροφοριών και δεδομένων.
- Να αναγνωρίζουν και να συγκρίνουν κατάλληλα ψηφιακά εργαλεία και εφαρμογές ΑΙ ανάλογα με τις ανάγκες της εργασίας.
- Να εξηγούν τα επαγγελματικά πρότυπα για ψηφιακή επικοινωνία και συνεργασία.
- Να περιγράφουν και να εφαρμόζουν βήματα επίλυσης τεχνικών προβλημάτων.
- Να κατανοούν γιατί είναι απαραίτητη η συνεχής αναβάθμιση ψηφιακών δεξιοτήτων.



Στόχοι του Μαθήματος

Σε επίπεδο δεξιοτήτων:

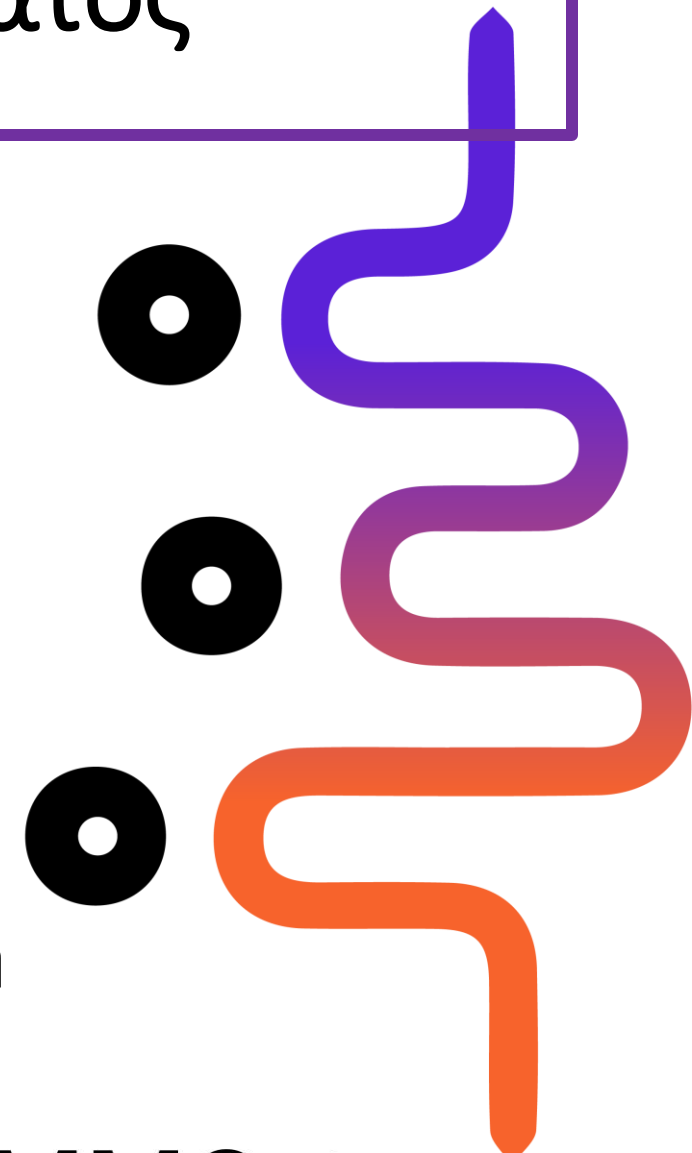
- Να εφαρμόζουν κατάλληλα μέτρα ψηφιακής προστασίας για τη μείωση κινδύνων κυβερνοασφάλειας και προστασίας δεδομένων στην καθημερινή εργασία.
- Να αξιολογούν κριτικά ψηφιακές πληροφορίες και πηγές, ώστε να διαπιστώνουν την αξιοπιστία και την καταλληλότητά τους για επαγγελματική χρήση.
- Να οργανώνουν, να κατηγοριοποιούν και να διαχειρίζονται ψηφιακά αρχεία και πληροφορίες με δομημένα συστήματα που βελτιώνουν την αποδοτικότητα της εργασίας.
- Να επιλέγουν και να χρησιμοποιούν κατάλληλα ψηφιακά εργαλεία παραγωγικότητας για την δημιουργία παραδοτέων.
- Να χρησιμοποιούν εργαλεία τεχνητής νοημοσύνης με υπευθυνότητα και στρατηγική, διασφαλίζοντας την προστασία ευαίσθητων δεδομένων και αξιολογώντας κριτικά τα αποτελέσματά τους.
- Να συνεργάζονται αυτόνομα μέσω ψηφιακών τεχνολογιών, διαχειριζόμενοι σωστά τις ρυθμίσεις κοινοποίησης, τη συν-επεξεργασία και τα δικαιώματα πρόσβασης.
- Να εντοπίζουν και να επιλύουν συνηθισμένα τεχνικά προβλήματα χρησιμοποιώντας δομημένη λογική επίλυσης προβλήματος και να καταγράφουν τη διαδικασία επίλυσης όπου απαιτείται.
- Να αξιολογούν το προσωπικό τους επίπεδο ψηφιακών δεξιοτήτων και να σχεδιάζουν ένα οργανωμένο πλάνο βελτίωσης για την κάλυψη των κενών που εντοπίζουν.



Στόχοι του Μαθήματος

Σε επίπεδο στάσεων:

- Να επιδεικνύουν αυστηρότητα στην προστασία δεδομένων, επίγνωση θεμάτων κυβερνοασφάλειας και ηθική συμπεριφορά στη χρήση ψηφιακών τεχνολογιών στον επαγγελματικό χώρο.
- Να δείχνουν υπευθυνότητα και επαγγελματισμό στην ψηφιακή επικοινωνία και στις συνεργατικές πρακτικές.
- Να έχουν ενεργητική και προληπτική στάση στον εντοπισμό και την αντιμετώπιση ψηφιακών προβλημάτων στο εργασιακό περιβάλλον.
- Να υιοθετούν νοοτροπία δια βίου μάθησης, επιδιώκοντας τη συνεχή ανάπτυξη των ψηφιακών τους δεξιοτήτων ως απάντηση στις τεχνολογικές εξελίξεις.



Δομή του μαθήματος

Ψηφιακή Ασφάλεια
και Υπεύθυνη
Διαχείριση
Δεδομένων

Ψηφιακός και
Πληροφοριακός
Γραμματισμός

Ψηφιακά Εργαλεία και
Τεχνητή Νοημοσύνη για
καθημερινές
επαγγελματικές εργασίες

Ψηφιακή Επικοινωνία,
Συνεργασία και
Επαγγελματική
Ταυτότητα στο
διαδίκτυο

Δημιουργία και
Επεξεργασία Ψηφιακού
Περιεχομένου για
επαγγελματικές ανάγκες

Επίλυση βασικών
τεχνικών
προβλημάτων

Ψηφιακή Ασφάλεια & Υπεύθυνη Διαχείριση Δεδομένων

Ενότητα 1



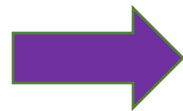
Γιατί είναι σημαντική αυτή η ενότητα;

Αυτή η ενότητα παρουσιάζει τις βασικές αρχές και πρακτικές που υποστηρίζουν την ασφαλή, υπεύθυνη και αποτελεσματική συμμετοχή σε ψηφιακά εργασιακά περιβάλλοντα.

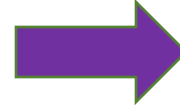
Εστιάζει στην αναγνώριση κινδύνων, στη σωστή διαχείριση πληροφοριών, στη λήψη σωστών αποφάσεων στην καθημερινή εργασία.

Στο σύγχρονο εργασιακό περιβάλλον, η ψηφιακή ασφάλεια αποτελεί βασική επαγγελματική απαίτηση. Η μη ασφαλής ψηφιακή συμπεριφορά μπορεί να οδηγήσει σε διαρροή δεδομένων, διακοπή λειτουργιών, απώλεια εμπιστοσύνης, νομικά ή κανονιστικά προβλήματα και χαμηλότερη ποιότητα εργασίας. Επομένως, η υπεύθυνη ψηφιακή συμπεριφορά δεν είναι κάτι δευτερεύον, αλλά βασικό στοιχείο της επαγγελματικής απόδοσης.

ΕΝΕΡΓΕΙΑ

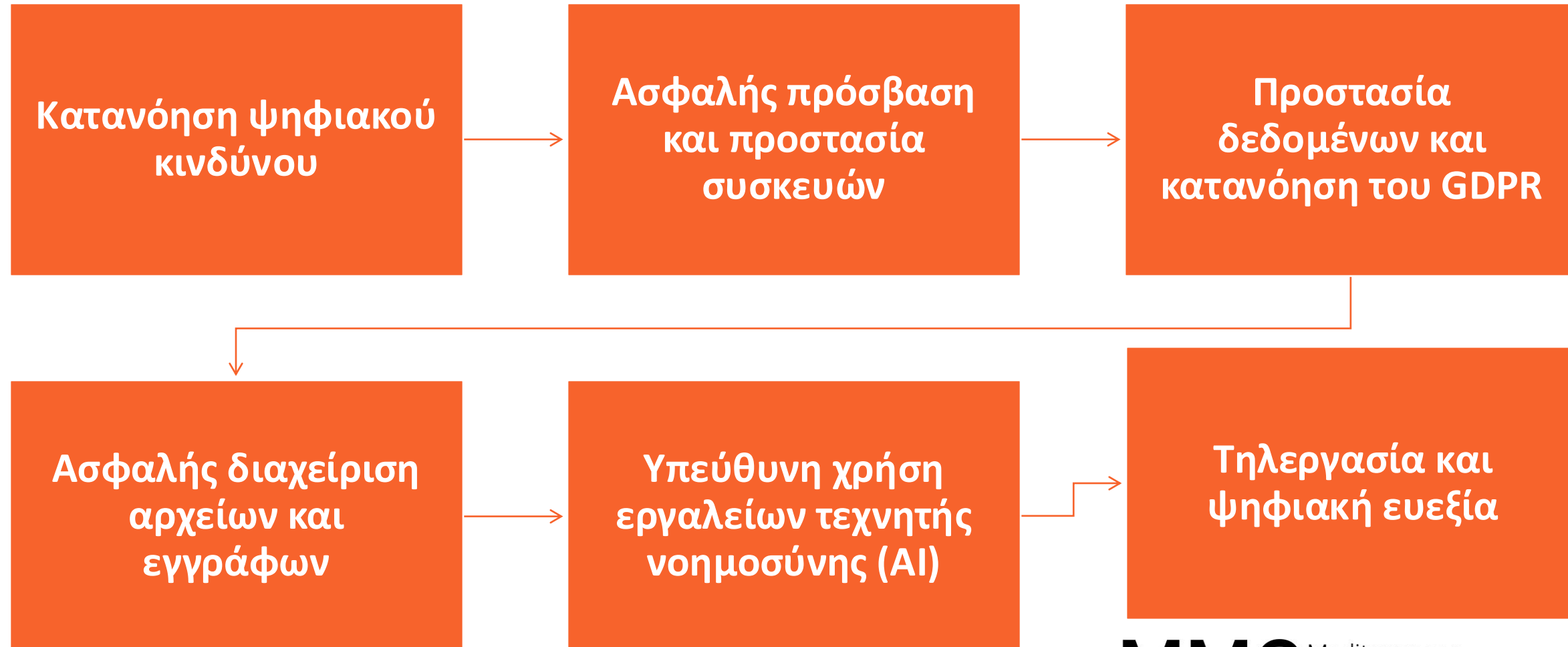


ΚΙΝΔΥΝΟΣ



ΕΠΙΠΤΩΣΕΙΣ

Δομή Ενότητας



Υποενότητα 1 – Κατανόηση Ψηφιακού Κινδύνου



Τι είναι η ψηφιακή ασφάλεια;

Η **ψηφιακή ασφάλεια** αναφέρεται στο σύνολο των συμπεριφορών, ελέγχων και αποφάσεων που βοηθούν άτομα και οργανισμούς να χρησιμοποιούν τις ψηφιακές τεχνολογίες χωρίς να εκθέτουν άσκοπα δεδομένα, συστήματα, ιδιωτικότητα, ευημερία ή την εργασία τους σε κινδύνους.

Περιλαμβάνει:

- την προστασία συσκευών και λογαριασμών
- την προσεκτική διαχείριση πληροφοριών
- την ασφαλή επικοινωνία
- την επίγνωση του ψηφιακού περιβάλλοντος
- την υπεύθυνη λήψη αποφάσεων



Ψηφιακή ασφάλεια στην πράξη (στον χώρο εργασίας)

Η **ψηφιακή ασφάλεια** δεν αφορά μόνο έκτακτα περιστατικά ή σοβαρές επιθέσεις. Εμφανίζεται καθημερινά, μέσα από απλές και συνηθισμένες δραστηριότητες, όπως:

- έλεγχος email
- διαμοιρασμός αρχείων
- αποθήκευση εγγράφων
- χρήση online πλατφορμών
- σύνδεση σε συστήματα
- εργασία εξ αποστάσεως
- χρήση εργαλείων τεχνητής νοημοσύνης

Ακόμη και οι πιο απλές καθημερινές εργασίες μπορούν να δημιουργήσουν σημαντικούς κινδύνους, αν δεν γίνονται με προσοχή και έλεγχο.

Τι είναι ο ψηφιακός κίνδυνος;

Ο **ψηφιακός κίνδυνος** είναι οποιαδήποτε κατάσταση, γεγονός ή συμπεριφορά που μπορεί να επηρεάσει αρνητικά:

- την εμπιστευτικότητα των πληροφοριών
- την ακεραιότητα των δεδομένων
- τη διαθεσιμότητα των συστημάτων
- την ιδιωτικότητα
- την εμπιστοσύνη
- την ποιότητα της εργασίας

Οι ψηφιακοί κίνδυνοι μπορεί να προκύψουν τόσο από τεχνικές αδυναμίες όσο και από ανθρώπινη συμπεριφορά.

Παράδειγμα: Αποστολή αρχείου σε λάθος παραλήπτη.

Πρόκειται για μια συνηθισμένη περίπτωση όπου ο κίνδυνος οφείλεται σε ανθρώπινο λάθος και μπορεί να οδηγήσει σε διαρροή εμπιστευτικών δεδομένων.



Ψηφιακός κίνδυνος = κάθε απειλή προς δεδομένα, συστήματα, ιδιωτικότητα ή ροή εργασίας που προκύπτει από ψηφιακή δραστηριότητα.

Quiz1

Παρακαλούμε επιλέξτε τη σωστή απάντηση.

Ποια κατάσταση αντιπροσωπεύει έναν τυπικό ψηφιακό κίνδυνο στον χώρο εργασίας;

- ☐ 2. Αποστολή αρχείου σε λάθος παραλήπτη
- ☐ 4. Συμμετοχή σε μια σύσκεψη
- ☐ 3. Χρήση υπολογιστικού φύλλου (spreadsheet)
- ☐ 1. Συγγραφή μιας μακροσκελούς αναφοράς

Τύποι Ψηφιακών Κινδύνων στον Χώρο Εργασίας

Οι ψηφιακοί κίνδυνοι στον χώρο εργασίας συνήθως κατηγοριοποιούνται σε συγκεκριμένες ομάδες, καθεμία από τις οποίες αντιπροσωπεύει διαφορετικό τύπο απειλής για τα δεδομένα, τις συσκευές και τα συστήματα.

Οι περισσότερες απειλές ανήκουν σε προβλέψιμες κατηγορίες, κάτι που μας βοηθά να τις αναγνωρίζουμε και να τις προλαμβάνουμε πιο εύκολα.

Συνηθισμένοι ψηφιακοί κίνδυνοι:

- **Phishing (Ηλεκτρονικό “ψάρεμα”)**: Παραπλανητικά μηνύματα που έχουν στόχο να αποσπάσουν πληροφορίες ή να οδηγήσουν σε επικίνδυνες ενέργειες.
- **Malware (Κακόβουλο λογισμικό)**: Λογισμικό που προκαλεί ζημιά, κλέβει δεδομένα ή διαταράσσει τη λειτουργία συστημάτων.
- **Social Engineering (Κοινωνική μηχανική)**: Χειραγώγηση ανθρώπων για την απόκτηση πρόσβασης ή ευαίσθητων πληροφοριών.
- **Αδύναμη ταυτοποίηση (Weak Authentication)**: Κακές πρακτικές σε κωδικούς και συνδέσεις (π.χ. εύκολοι ή επαναλαμβανόμενοι κωδικοί).
- **Μη ασφαλής διαμοιρασμός (Unsafe Sharing)**: Μη ελεγχόμενη πρόσβαση σε αρχεία και δεδομένα.

Οι οδηγίες [ENISA's cyber hygiene guidance](#) επικεντρώνονται ακριβώς σε τέτοιες καθημερινές πρακτικές πρόληψης. Η γρήγορη αναγνώριση της κατηγορίας του κινδύνου βοηθά στον σωστό και άμεσο χειρισμό του.

Phishing (Ηλεκτρονικό “ψάρεμα”)

Το **Phishing** είναι μια μορφή κυβερνοεπίθεσης κατά την οποία οι επιτιθέμενοι προσποιούνται νόμιμους οργανισμούς (ή παρουσιάζονται ως αξιόπιστη οντότητα) με σκοπό να κλέψουν ευαίσθητες πληροφορίες, όπως στοιχεία σύνδεσης, στοιχεία πιστωτικών καρτών ή εταιρικά μυστικά.

Οι επιθέσεις phishing χρησιμοποιούν συχνά τεχνικές κοινωνικής μηχανικής για να εξαπατήσουν τον παραλήπτη, ώστε να πιστέψει ότι το μήνυμα προέρχεται από αξιόπιστη πηγή και να ενεργήσει χωρίς κατάλληλη επαλήθευση.



Παράδειγμα:

Ένας εργαζόμενος λαμβάνει ένα email που φαίνεται να προέρχεται από την τράπεζά του, το οποίο αναφέρει ότι ο λογαριασμός του έχει παραβιαστεί και ότι πρέπει να πατήσει σε έναν σύνδεσμο για να ενημερώσει τα στοιχεία του. Αυτός ο σύνδεσμος οδηγεί σε μια ψεύτικη ιστοσελίδα που έχει σχεδιαστεί για να κλέψει τα στοιχεία σύνδεσης.

Ο βασικός κίνδυνος είναι η **κλοπή ταυτότητας ή η οικονομική απάτη**. Το phishing μπορεί επίσης να δώσει στους επιτιθέμενους πρόσβαση σε εσωτερικά συστήματα, οδηγώντας σε μεγαλύτερες διαρροές δεδομένων ή μολύνσεις από κακόβουλο λογισμικό.

Quiz2

Παρακαλούμε επιλέξτε τη σωστή απάντηση.

Ποια είναι η πιο επαγγελματική αντίδραση σε ένα επείγον μήνυμα μέσω ηλεκτρονικού ταχυδρομείου που ζητά μια άμεση ενέργεια;

- ☐ 4. Προώθηση του μηνύματος σε συναδέλφους
- ☐ 3. Επαλήθευση του αποστολέα πριν από οποιαδήποτε ενέργεια
- ☐ 1. Άμεση ανταπόκριση για την αποφυγή προβλημάτων
- ☐ 2. Κλικ στον σύνδεσμο για επαλήθευση

Εντοπισμός phishing

Ενδείξεις ενός ύποπτου μηνύματος μπορεί να περιλαμβάνουν:

- **ασυνήθιστη διεύθυνση αποστολέα** → μπορεί να μιμείται έναν αξιόπιστο οργανισμό αλλά περιέχει μικρές ασυνέπειες (π.χ. επιπλέον γράμματα ή διαφορετικά domains)
- **αίτημα εκτός κανονικής διαδικασίας** → παρακάμπτει καθιερωμένες ροές εργασίας ή διαδικασίες έγκρισης
- **μη αναμενόμενο συνημμένο ή σύνδεσμο** → μπορεί να οδηγεί σε κακόβουλες ιστοσελίδες ή να εγκαθιστά κακόβουλο λογισμικό
- **επείγων ή απειλητικός τόνος** → μειώνει την κριτική σκέψη, πιέζοντας τον χρήστη να ενεργήσει γρήγορα χωρίς έλεγχο
- **γραμματικά λάθη ή ασυνήθιστη μορφοποίηση**
- **αίτημα για εμπιστευτικά δεδομένα ή κωδικούς** → παραβιάζει τις πολιτικές ασφάλειας του οργανισμού

Ένα μήνυμα μπορεί να φαίνεται επαγγελματικό και παρόλα αυτά να είναι επικίνδυνο.

Πρακτικός Κανόνας:

Μην κάνετε κλικ σε συνδέσμους και μην ανοίγετε συνημμένα από άγνωστα ή ύποπτα emails. Να επαληθεύετε πάντα τη διεύθυνση email του αποστολέα και να μην ενεργείτε άμεσα σε επείγοντα ψηφιακά αιτήματα χωρίς προηγούμενη επιβεβαίωση.

Μελέτη Περίπτωσης: Ανάλυση Phishing Email

Παράδειγμα ύποπτου email

Θέμα: Επείγον: Εντοπίστηκε ζήτημα ασφάλειας στον υπολογιστή σας

Από: Margaret Doe, IT Supervisor m.doe@ourcompany.com

Προς: John Sample

Περιεχόμενο email:

John,

Η ομάδα ασφάλειας IT έχει εντοπίσει ασυνήθιστη δραστηριότητα στον υπολογιστή σας κατά τις βραδινές ώρες. Πιστεύουμε ότι η συσκευή σας ενδέχεται να έχει επηρεαστεί από ένα πρόσφατα εντοπισμένο ζήτημα ασφάλειας.

Παρακαλώ ελέγξτε τα συνημμένα αρχεία καταγραφής και επιβεβαιώστε αν αυτές οι ενέργειες πραγματοποιήθηκαν από εσάς. Εάν όχι, παρακαλώ πατήστε στον παρακάτω σύνδεσμο για να ενημερώσετε άμεσα το λογισμικό προστασίας από ιούς:

 Ενημέρωση λογισμικού ασφάλειας
Ενημερώστε με μόλις ολοκληρωθεί.

Margaret
IT Supervisor

Ανάλυση του Email

1. Εξατομίκευση

Το μήνυμα χρησιμοποιεί το όνομα του εργαζομένου ("John") → αυξάνει την εμπιστοσύνη

2. Ψεύτικος αλλά ρεαλιστικός αποστολέας

Το domain φαίνεται σωστό αλλά έχει μικρή αλλοίωση → ourcompany.com αντί για ourcompany.com

3. Εξουσία

Το μήνυμα φαίνεται να προέρχεται από το τμήμα IT → αυξάνει τη συμμόρφωση

4. Δημιουργία φόβου

"Η συσκευή σας μπορεί να έχει επηρεαστεί" → δημιουργεί αίσθημα επείγοντος και ανησυχίας

5. Ενέργεια χαμηλού ρίσκου

"Ελέγξτε τα συνημμένα αρχεία" → χτίζει εμπιστοσύνη πριν την κύρια ενέργεια

6. Ενέργεια υψηλού ρίσκου

"Πατήστε στον σύνδεσμο για ενημέρωση λογισμικού" → το πραγματικό σημείο επίθεσης (malware ή κλοπή στοιχείων)

Malware

Ο όρος Malware (κακόβουλο λογισμικό) αναφέρεται σε λογισμικό που έχει δημιουργηθεί για να παραβιάσει ή να επηρεάσει αρνητικά μια συσκευή, ένα σύστημα ή ένα σύνολο δεδομένων. Μπορεί να εισέλθει μέσω μη ασφαλών λήψεων, κακόβουλων συνημμένων, ψεύτικων ενημερώσεων ή παραβιασμένων ιστοσελίδων.

Παράδειγμα: Άνοιγμα ενός μολυσμένου συνημμένου αρχείου.

Πιθανές συνέπειες περιλαμβάνουν:

- απώλεια αρχείων
- μείωση της απόδοσης του συστήματος
- μη εξουσιοδοτημένη πρόσβαση
- διακοπή λειτουργιών
- εξάπλωση σε άλλα συστήματα

Πρακτικός Κανόνας:

- Βεβαιωθείτε ότι το λογισμικό προστασίας από ιούς είναι εγκατεστημένο και ενημερωμένο σε όλες τις συσκευές.
- Μην κατεβάζετε λογισμικό ή ενημερώσεις από μη αξιόπιστες πηγές και χρησιμοποιείτε μόνο έγκυρες πλατφόρμες για εφαρμογές που σχετίζονται με την εργασία.



Βασικοί τύποι Κακόβουλου Λογισμικού

1. Ransomware

- κρυπτογραφεί τα δεδομένα του οργανισμού και απαιτεί πληρωμή (συχνά σε κρυπτονόμισμα)
- στοχεύει στη διαθεσιμότητα των δεδομένων

2. Spyware

- παρακολουθεί κρυφά τη δραστηριότητα του χρήστη (πληκτρολογήσεις, οθόνη, στοιχεία σύνδεσης)
- στοχεύει στην εμπιστευτικότητα

3. Δούρειοι Ίπποι (Trojan Horses)

- εμφανίζονται ως νόμιμα εργαλεία (π.χ. μετατροπέας PDF, αρχείο ενημέρωσης)
- εγκαθιστούν κακόβουλο λογισμικό όταν εκτελούνται

Social engineering: η ανθρώπινη διάσταση του ψηφιακού κινδύνου

Η κοινωνική μηχανική (social engineering) αναφέρεται στη χειραγώγηση ανθρώπων αντί για συστήματα. Περιλαμβάνει την εξαπάτηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες, εκμεταλλευόμενη ψυχολογικές τεχνικές και όχι τεχνικά μέσα.

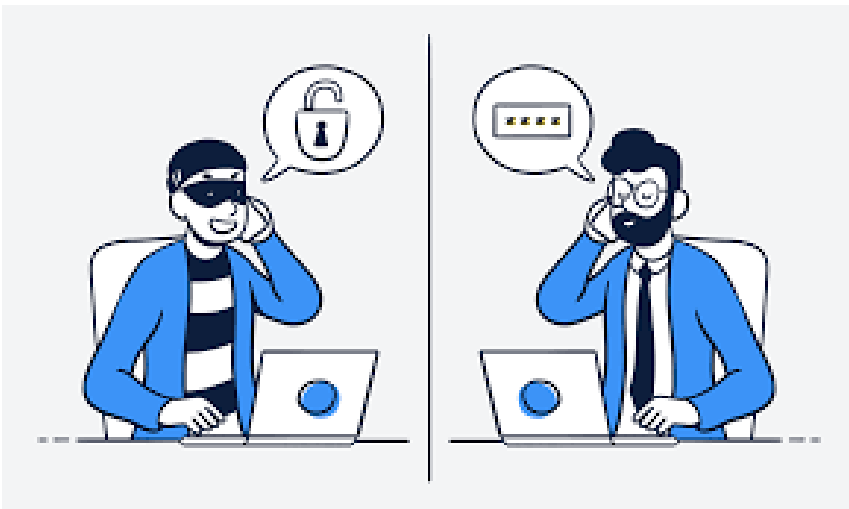
Οι επιτιθέμενοι μπορεί να προσποιηθούν νόμιμους εργαζομένους, προμηθευτές ή πελάτες, ώστε να κερδίσουν εμπιστοσύνη και να πείσουν το θύμα να αποκαλύψει ευαίσθητα δεδομένα ή να δώσει πρόσβαση σε συστήματα.

Παράδειγμα:

Ένας επιτιθέμενος τηλεφωνεί σε έναν εργαζόμενο προσποιούμενος ότι είναι από το τμήμα HR και τον πείθει να μοιραστεί τα εσωτερικά στοιχεία σύνδεσης της εταιρείας ή διαπιστευτήρια πρόσβασης.

Πρακτικός κανόνας:

Επαληθεύετε όλα τα μη αναμενόμενα αιτήματα για ευαίσθητες πληροφορίες επικοινωνώντας με τον αποστολέα μέσω επίσημων καναλιών επικοινωνίας. Να είστε προσεκτικοί όταν λαμβάνετε απρόσμενες κλήσεις ή emails που ζητούν στοιχεία σύνδεσης ή πρόσβαση σε εταιρικά συστήματα.



Γιατί η καθημερινή εργασία είναι συχνά ευάλωτη

Οι εργαζόμενοι συχνά έχουν πολλαπλές ευθύνες, εργάζονται υπό πίεση χρόνου και βασίζονται σε σχετικά ανεπίσημες πρακτικές επικοινωνίας. Αυτό αυξάνει την πιθανότητα για μη ασφαλείς «συντομεύσεις», ανεπαρκή έλεγχο και ασυνεπή διαχείριση δεδομένων και πρόσβασης.

Πολλά ψηφιακά περιστατικά δεν συμβαίνουν επειδή οι χρήστες δεν γνωρίζουν. Συμβαίνουν επειδή οι χρήστες είναι:

- βιαστικοί
- απασχολημένοι ή αφηρημένοι
- εκτελούν πολλές εργασίες ταυτόχρονα
- υπερβολικά σίγουροι
- λειτουργούν από συνήθεια χωρίς κριτική ικανότητα

Ο κίνδυνος, επομένως, προκύπτει συχνά από τις συνθήκες της καθημερινής εργασίας.
Η ψηφιακή ασφάλεια εξαρτάται σε μεγάλο βαθμό από τη συμπεριφορά.

Μελέτη Περίπτωσης: Το κόστος ενός κλικ

Αυτή η μελέτη περίπτωσης δείχνει πώς η κοινωνική μηχανική μπορεί να οδηγήσει σε τεχνική παραβίαση ασφάλειας μέσω μιας απλής ενέργειας του χρήστη.

Σενάριο

Ένας εργαζόμενος λαμβάνει ένα email με τίτλο:
«Τιμολόγιο – Απαιτείται άμεση εξέταση»

- Φαίνεται να προέρχεται από νόμιμο προμηθευτή
- Είναι επαγγελματικό και σχετικό με την εργασία
- Ζητά το άνοιγμα ενός συνημμένου τιμολογίου

Το αίτημα φαίνεται συνηθισμένο και ασφαλές.

Γιατί λειτουργεί (Κοινωνική μηχανική)

- **Εμπιστοσύνη** → οικείο επαγγελματικό πλαίσιο (τιμολόγιο)
- **Σχετικότητα** → μέρος καθημερινών εργασιών
- **Επείγον** → ενθαρρύνει άμεση ενέργεια
- **Χαμηλός αντιλαμβανόμενος κίνδυνος** → το άνοιγμα αρχείων φαίνεται φυσιολογικό

Εξέλιξη Επίθεσης, Αποτέλεσμα & Επιπτώσεις

Αφού ο εργαζόμενος ανοίξει το συνημμένο, εκτελείται κακόβουλος κώδικας, ο οποίος μολύνει το σύστημα και επιτρέπει την εξάπλωση του κακόβουλου λογισμικού στο εσωτερικό δίκτυο. Ως αποτέλεσμα, τα αρχεία του οργανισμού κρυπτογραφούνται μέσω επίθεσης ransomware, καθιστώντας όλα τα δεδομένα πελατών μη προσβάσιμα και διακόπτοντας τη λειτουργία της επιχείρησης. Ο οργανισμός αντιμετωπίζει σημαντικές συνέπειες, όπως κόστος αποκατάστασης που υπερβαίνει τις 50.000€, διακοπή λειτουργιών και απώλεια παραγωγικότητας. Το πιο κρίσιμο αποτέλεσμα, ωστόσο, είναι η απώλεια εμπιστοσύνης των πελατών, η οποία μπορεί να έχει μακροπρόθεσμες ή ακόμη και μη αναστρέψιμες επιπτώσεις.

Υποενότητα 2 – Ασφαλής Πρόσβαση & Προστασία Συσκευών



Co-funded by
the European Union

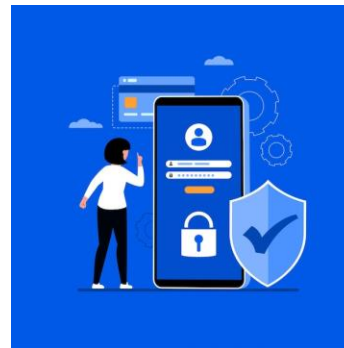
Γιατί είναι σημαντική η ταυτοποίηση

Η ταυτοποίηση (authentication) είναι η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη, μιας συσκευής ή μιας οντότητας πριν δοθεί πρόσβαση σε ένα σύστημα ή σε δεδομένα.

Η αποτελεσματική ταυτοποίηση αποτελεί την πρώτη γραμμή άμυνας ενάντια στη μη εξουσιοδοτημένη πρόσβαση. Περιλαμβάνει τη χρήση κωδικών πρόσβασης, βιομετρικών στοιχείων, έξυπνων καρτών και άλλων μεθόδων, ώστε να διασφαλίζεται ότι το σωστό άτομο αποκτά πρόσβαση στα συστήματα.

Παράδειγμα:

Κατά τη σύνδεση σε μια ασφαλή πλατφόρμα, οι χρήστες πρέπει να εισάγουν έναν κωδικό πρόσβασης και να επιβεβαιώσουν την ταυτότητά τους χρησιμοποιώντας έναν σαρωτή δακτυλικού αποτυπώματος ή έναν δεύτερο παράγοντα ταυτοποίησης, όπως έναν κωδικό που αποστέλλεται στο κινητό.



Κωδικοί πρόσβασης ως πρώτη γραμμή άμυνας

Οι **κωδικοί πρόσβασης** παραμένουν ένας από τους πιο συνηθισμένους μηχανισμούς ελέγχου πρόσβασης. Η αποτελεσματικότητά τους δεν εξαρτάται μόνο από την πολυπλοκότητα, αλλά και από το μήκος, τη μοναδικότητα και τη συμπεριφορά του χρήστη.

Οι επιθέσεις brute-force μπορούν να «σπάσουν» κωδικούς 8 χαρακτήρων μέσα σε λίγα λεπτά. Οι κακές πρακτικές στη χρήση κωδικών αποδυναμώνουν ακόμη και τα πιο καλά σχεδιασμένα συστήματα.

Choose a password: Password strength: Too short
Minimum of 8 characters in length.

Choose a password: Password strength: Weak
Minimum of 8 characters in length.

Choose a password: Password strength: Fair
Minimum of 8 characters in length.

Choose a password: Password strength: Good
Minimum of 8 characters in length.

Choose a password: Password strength: Strong
Minimum of 8 characters in length.

From google.com

Αρχές ισχυρών κωδικών πρόσβασης

1. Το μήκος είναι η βασική προτεραιότητα

- Χρησιμοποιείτε τουλάχιστον 16 χαρακτήρες.
- Οι μεγαλύτεροι κωδικοί είναι πιο δύσκολο να «σπάσουν» μέσω επιθέσεων brute-force

2. Μοναδικότητα

- Μην επαναχρησιμοποιείτε κωδικούς σε διαφορετικές πλατφόρμες.
- Μια παραβίαση σε μία υπηρεσία δεν πρέπει να επηρεάζει άλλες

3. Πολυπλοκότητα / Τυχαιότητα

- Συνδυάζετε διαφορετικούς τύπους χαρακτήρων: γράμματα, αριθμούς και σύμβολα
- Παράδειγμα: 6MonkeysRLooking^.

4. Χρήση φράσεων πρόσβασης (passphrases)

- Συνδυάστε 4–7 άσχετες μεταξύ τους λέξεις (π.χ. "BlueSkyCoffee*2024")
- Είναι πιο ασφαλείς και πιο εύκολο να θυμάστε

5. Αποφυγή προσωπικών πληροφοριών

- Μην χρησιμοποιείτε ονόματα, ημερομηνίες γέννησης, λέξεις λεξικού ή κοινές ακολουθίες όπως "123456" ή "password123"

Οι κωδικοί πρέπει να είναι μεγάλοι, μοναδικοί και να μην βασίζονται σε προσωπικά στοιχεία. Να αποθηκεύονται με ασφάλεια και να μην επαναχρησιμοποιούνται σε διαφορετικούς λογαριασμούς,

Μη ασφαλείς πρακτικές κωδικών πρόσβασης

1. Επαναχρησιμοποίηση κωδικών πρόσβασης

- Χρήση του ίδιου κωδικού πρόσβασης σε πολλαπλές πλατφόρμες.
- Μία παραβίαση μπορεί να θέσει σε κίνδυνο όλους τους λογαριασμούς.

2. Αδύναμοι / απλοί κωδικοί πρόσβασης

- Προβλέψιμες λέξεις, ημερομηνίες γέννησης, ονόματα κατοικίδιων ή σύντομες ακολουθίες.
- Σπάζονται εύκολα από αυτοματοποιημένα εργαλεία.

3. Μη ασφαλής αποθήκευση κωδικών πρόσβασης

- Καταγραφή κωδικών σε σημειώσεις (π.χ. αυτοκόλλητα χαρτάκια), αποθήκευση σε απλά αρχεία κειμένου ή χρήση μη κρυπτογραφημένης αυτόματης συμπλήρωσης στον browser.

4. Κοινοποίηση διαπιστευτηρίων

- Κοινοποίηση κωδικών μέσω μη κρυπτογραφημένων email, μηνυμάτων ή σε άλλα άτομα.

6. Μη ενημέρωση κωδικών μετά από παραβάσεις

- Συνέχιση χρήσης ενός κωδικού πρόσβασης αφού έχει εκτεθεί σε παραβίαση δεδομένων

Συνέπειες κακής ασφάλειας κωδικών πρόσβασης

Credential Stuffing: Οι χάκερ αποκτούν πρόσβαση σε άλλες υπηρεσίες χρησιμοποιώντας κλεμμένα στοιχεία σύνδεσης.

Κλοπή ταυτότητας: Μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες.

Οικονομική απώλεια: Άμεση κλοπή χρημάτων ή δόλιες αγορές από τραπεζικούς λογαριασμούς.

Συνηθισμένες κακές πρακτικές και λάθη στη δημιουργία κωδικών πρόσβασης

5 Συνηθισμένα λάθη στις συνήθειες χρήσης κωδικών

- Επαναχρησιμοποίηση κωδικών πρόσβασης
- Φυσική αποθήκευση κωδικών (π.χ. σε χαρτί)
- Μη αλλαγή κωδικών μετά από παραβίαση
- Αποθήκευση κωδικών στον browser
- Μη ασφαλής κοινοποίηση κωδικών

6 Συνηθισμένα λάθη στη δημιουργία κωδικών

- Χρήση ονομάτων οικογένειας
- Χρήση προσωπικών πληροφοριών
- Χρήση προσωπικών προτιμήσεων
- Χρήση απλών ακολουθιών όπως "56789"
- Χρήση προβλέψιμων χαρακτήρων ή λέξεων λεξικού
- Δημιουργία σύντομων και απλών κωδικών

Πολυπαραγοντική ταυτοποίηση (Multi-factor authentication MFA)

Η πολυπαραγοντική ταυτοποίηση (MFA) ενισχύει την προστασία πρόσβασης απαιτώντας περισσότερες από μία μορφές επαλήθευσης. Θεωρείται «Το χρυσό πρότυπο προστασίας».

Συνήθως συνδυάζει:

- κάτι που γνωρίζει ο χρήστης (π.χ. κωδικός πρόσβασης / PIN)
- κάτι που έχει ο χρήστης (π.χ. smartphone / κλειδί ασφαλείας)
- ή κάτι που είναι ο χρήστης (π.χ. βιομετρικά στοιχεία, δακτυλικό αποτύπωμα / FaceID)

Δεν εξαλείφει πλήρως τον κίνδυνο, αλλά τον μειώνει σημαντικά σε περίπτωση που εκτεθούν τα στοιχεία σύνδεσης. Ακόμη και αν ένας παράγοντας παραβιαστεί, η πρόσβαση παραμένει προστατευμένη.

Παράδειγμα: Χρήση κωδικού πρόσβασης σε συνδυασμό με σάρωση δακτυλικού αποτυπώματος ή κωδικό που αποστέλλεται μέσω SMS.



Πώς λειτουργεί η πολυπαραγοντική ταυτοποίηση (Βήμα προς βήμα διαδικασία)

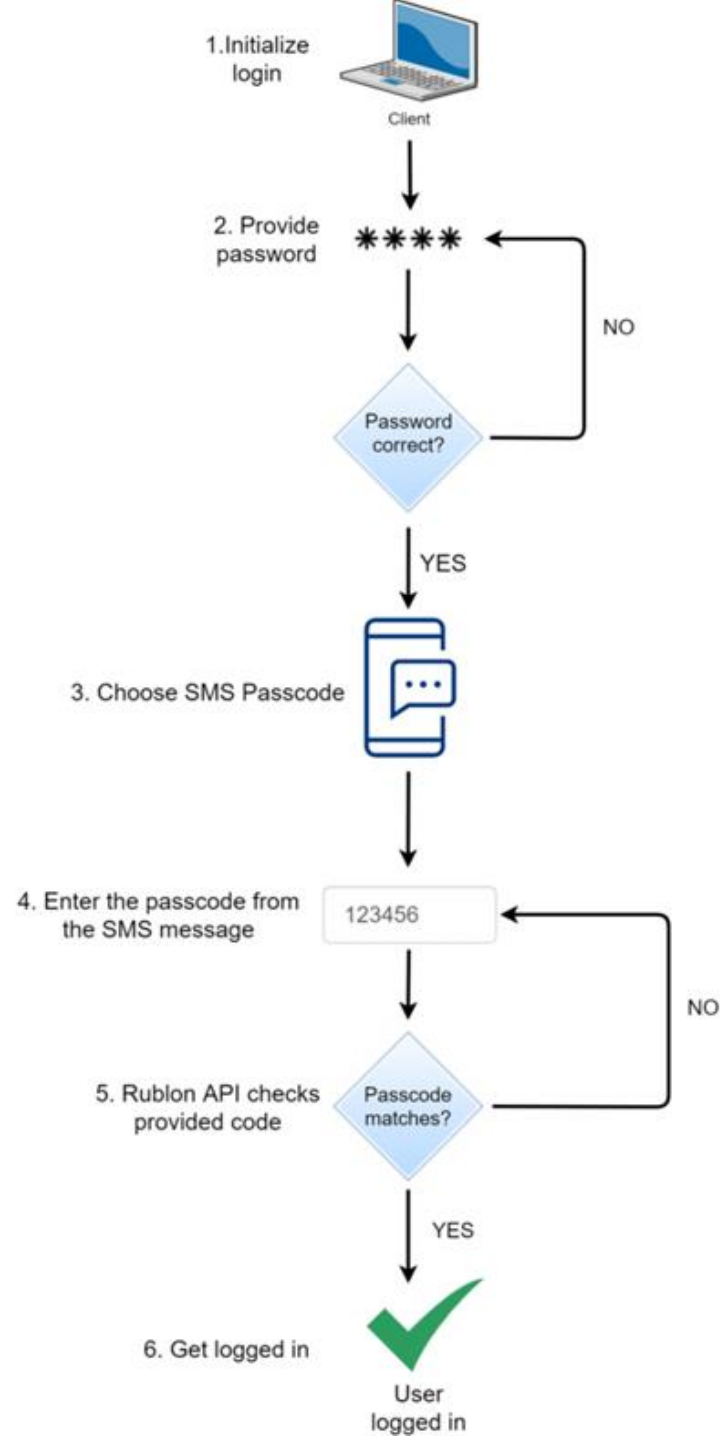
Κατά την πρόσβαση σε ένα ασφαλές σύστημα, η ταυτοποίηση πραγματοποιείται σε πολλαπλά στάδια:

1. Ο χρήστης εισάγει το όνομα χρήστη και τον κωδικό πρόσβασης
2. Το σύστημα επαληθεύει τα στοιχεία σύνδεσης
3. Ενεργοποιείται ένα δεύτερο αίτημα ταυτοποίησης
4. Ο χρήστης λαμβάνει έναν κωδικό μίας χρήσης (OTP) στο κινητό του ή σε εφαρμογή ταυτοποίησης
5. Ο χρήστης εισάγει τον κωδικό επαλήθευσης
6. Η πρόσβαση επιτρέπεται μόνο εφόσον και οι δύο παράγοντες ταυτοποίησης είναι σωστοί



Χωρίς πολυπαραγοντική ταυτοποίηση:

- οι κλεμμένοι ή αδύναμοι κωδικοί μπορούν να οδηγήσουν σε πλήρη πρόσβαση στο σύστημα
- οι επιθέσεις phishing μπορούν εύκολα να παραβιάσουν λογαριασμούς χρηστών
- οι επιτιθέμενοι ενδέχεται να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα και συστήματα του οργανισμού



Ασφάλεια συσκευών με υπευθυνότητα

Η ασφάλεια συσκευών περιλαμβάνει τις πρακτικές προστασίας τελικών συσκευών, όπως φορητοί υπολογιστές, smartphones και σταθεροί υπολογιστές, από μη εξουσιοδοτημένη πρόσβαση, κλοπή ή κακόβουλο λογισμικό.

Καθώς οι συσκευές αποτελούν τα βασικά σημεία εισόδου σε δεδομένα και συστήματα, η διασφάλιση της προστασίας τους είναι υψίστης σημασίας. Αυτό περιλαμβάνει τη χρήση firewalls, κρυπτογράφησης, λογισμικού προστασίας από ιούς και ασφαλών ρυθμίσεων.

Η ασφαλής χρήση συσκευών περιλαμβάνει:

- κλείδωμα της οθόνης όταν απομακρύνεστε από αυτήν
- χρήση εγκεκριμένου λογισμικού
- αποφυγή άγνωστων λήψεων και συσκευών USB
- προστασία των συσκευών κατά τη μεταφορά
- διατήρηση ενημερωμένων συστημάτων και εφαρμογών



Παράδειγμα: Κλείδωμα του υπολογιστή όταν απομακρύνεστε από το γραφείο, διασφάλιση ότι τα ευαίσθητα δεδομένα είναι κρυπτογραφημένα και τακτική ενημέρωση του λογισμικού ασφάλειας.

Γιατί οι ενημερώσεις είναι σημαντικές;

Οι ενημερώσεις συχνά:

- διορθώνουν γνωστά κενά ασφαλείας
- βελτιώνουν την αξιοπιστία του συστήματος
- μειώνουν προβλήματα συμβατότητας
- ενισχύουν την προστασία απέναντι σε γνωστές απειλές

Η διατήρηση του λογισμικού ενημερωμένου διασφαλίζει προστασία από γνωστούς κινδύνους και κρατά τα συστήματα ασφαλή από εξωτερικές απειλές.

Παράδειγμα: Τακτική ενημέρωση λειτουργικών συστημάτων, προγραμμάτων *antivirus* και *browsers* για την κάλυψη κενών ασφαλείας.

Η μη εγκατάσταση ενημερώσεων μπορεί να αφήσει τα συστήματα εκτεθειμένα σε επιθέσεις από κακόβουλο λογισμικό ή hackers.

Πρακτικός κανόνας:

Ενεργοποιήστε τις αυτόματες ενημερώσεις για κρίσιμο λογισμικό και δώστε προτεραιότητα στις ενημερώσεις λειτουργικών συστημάτων και λογισμικού ασφάλειας.

Βασικοί τύποι ενημερώσεων

Είδος	Σκοπός	Παράδειγμα
Patch	Διορθώνει συγκεκριμένα προβλήματα που επηρεάζουν την απόδοση ή την ασφάλεια του συστήματος	Διόρθωση σφάλματος υπολογισμού σε λογισμικό λογιστικής
Hotfix	Άμεση διόρθωση για κρίσιμα προβλήματα εκτός του κανονικού κύκλου ενημερώσεων	Άμεση επίλυση σφάλματος που προκαλεί κατάρρευση συστήματος κατά την καθημερινή λειτουργία
Security Update (Ενημέρωση ασφάλειας)	Αντιμετωπίζει απειλές που μπορούν να εκμεταλλευτούν επιτιθέμενοι	Διόρθωση αδυναμίας που επιτρέπει μη εξουσιοδοτημένη πρόσβαση σε εταιρικά δεδομένα
Critical Update (Κρίσιμη ενημέρωση)	Επιλύει σοβαρά σφάλματα συστήματος που επηρεάζουν τη λειτουργικότητα	Διόρθωση προβλημάτων που εμποδίζουν την πρόσβαση σε βασικά επιχειρησιακά συστήματα
Cumulative Update (Σωρευτική ενημέρωση)	Συνδυάζει πολλαπλές προηγούμενες διορθώσεις και βελτιώσεις σε μία ενημέρωση	Εγκατάσταση μίας ενημέρωσης αντί για πολλές μικρότερες
Service Pack (Πακέτο ενημερώσεων)	Συγκεντρώνει διορθώσεις, ενημερώσεις και βελτιώσεις για ευκολότερη εγκατάσταση	Μαζική ενημέρωση συστημάτων σε όλη την εταιρεία
Ενημέρωση λειτουργιών / Πακέτο νέων δυνατοτήτων	Εισάγει νέες λειτουργίες και βελτιώνει τη λειτουργικότητα του συστήματος	Νέα εργαλεία για συνεργασία ή βελτίωση ροής εργασίας
Upgrade (Αναβάθμιση)	Μεγάλη αλλαγή έκδοσης λογισμικού ή λειτουργικού συστήματος	Μετάβαση από Windows 10 σε Windows 11

Υποενότητα 3 – Προστασία Δεδομένων & Κατανόηση GDPR



Co-funded by
the European Union

Τι θεωρείται δεδομένο στον χώρο εργασίας;

Τα δεδομένα στον χώρο εργασίας περιλαμβάνουν:

- ονόματα και στοιχεία επικοινωνίας
- αρχεία πελατών
- στοιχεία εργαζομένων
- προγράμματα εργασίας
- εσωτερικές αναφορές
- Συμβάσεις
- οικονομικά έγγραφα
- αρχεία επικοινωνίας

Δεν έχουν όλα τα δεδομένα το ίδιο επίπεδο ευαισθησίας, αλλά όλα απαιτούν κατάλληλη διαχείριση.



Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα αναφέρονται σε κάθε πληροφορία που μπορεί να ταυτοποιήσει ένα άτομο, άμεσα ή έμμεσα. Αυτό περιλαμβάνει κοινά αναγνωριστικά στοιχεία, όπως ονόματα, στοιχεία επικοινωνίας, αριθμούς ταυτοποίησης και ακόμη και διαδικτυακά αναγνωριστικά.

Παραδείγματα:

- όνομα
- διεύθυνση email
- αριθμός τηλεφώνου
- στοιχεία ταυτοποίησης



Κατανόηση του GDPR για εργαζομένους

Ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων) είναι ο κανονισμός της Ευρωπαϊκής Ένωσης που προστατεύει τα προσωπικά δεδομένα και θέτει κατευθυντήριες γραμμές για την επεξεργασία τους.

Σε επίπεδο εργαζομένου, η κατανόηση του GDPR δεν απαιτεί νομική εξειδίκευση. Απαιτεί πειθαρχημένη και επαγγελματική συμπεριφορά, όπως:

- πρόσβαση μόνο στα απολύτως απαραίτητα δεδομένα
- χρήση δεδομένων μόνο για νόμιμους επαγγελματικούς σκοπούς
- διαμοιρασμός μέσω εγκεκριμένων καναλιών
- αποφυγή απρόσεκτης έκθεσης δεδομένων
- άμεση αναφορά λαθών



Οι οδηγίες της Ευρωπαϊκής Επιτροπής για την προστασία δεδομένων αποτελούν την πιο αξιόπιστη πηγή γενικής πληροφόρησης σε δημόσιο επίπεδο.

[The European Commission's Data Protection Guidance](#)

Οι 7 βασικές αρχές του GDPR

1. Νομιμότητα, Δικαιοσύνη και Διαφάνεια

Τα δεδομένα πρέπει να συλλέγονται και να χρησιμοποιούνται με νόμιμο και διαφανή τρόπο (π.χ. ενημέρωση πελατών για το γιατί συλλέγονται τα δεδομένα τους και πώς θα χρησιμοποιηθούν).

2. Περιορισμός Σκοπού

Τα δεδομένα πρέπει να χρησιμοποιούνται μόνο για τον συγκεκριμένο σκοπό για τον οποίο συλλέχθηκαν (π.χ. δεδομένα πελατών που συλλέγονται για τιμολόγηση δεν μπορούν να χρησιμοποιηθούν για marketing χωρίς συγκατάθεση).

3. Ελαχιστοποίηση Δεδομένων

Πρέπει να συλλέγονται μόνο τα απαραίτητα δεδομένα (π.χ. αποφυγή ζήτησης περιττών προσωπικών στοιχείων σε φόρμες).

4. Ακρίβεια

Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και ενημερωμένα (π.χ. τακτική ενημέρωση στοιχείων επικοινωνίας πελατών).

5. Περιορισμός Αποθήκευσης

Τα δεδομένα δεν πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από όσο είναι απαραίτητο (π.χ. διαγραφή παλαιών αρχείων εργαζομένων ή πελατών).

6. Ακεραιότητα και Εμπιστευτικότητα (Ασφάλεια)

Τα δεδομένα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή απώλεια (π.χ. χρήση ασφαλών συστημάτων, κωδικών και περιορισμένης πρόσβασης).

7. Λογοδοσία

Οι οργανισμοί πρέπει να μπορούν να αποδεικνύουν τη συμμόρφωση με τον GDPR (π.χ. τήρηση αρχείων σχετικά με τον τρόπο διαχείρισης και προστασίας των δεδομένων).

Γιατί είναι σημαντική η υπεύθυνη διαχείριση δεδομένων

Η υπεύθυνη διαχείριση δεδομένων είναι σημαντική γιατί η κακή διαχείριση μπορεί να επηρεάσει:

- τα δικαιώματα και τα συμφέροντα των ατόμων
- την αξιοπιστία του οργανισμού
- την εμπιστοσύνη των πελατών
- την ποιότητα των εσωτερικών λειτουργιών
- τις νομικές και κανονιστικές υποχρεώσεις

Η προστασία δεδομένων είναι επομένως ταυτόχρονα ηθικό, λειτουργικό και κανονιστικό ζήτημα.

Η μη συμμόρφωση με τον GDPR μπορεί να οδηγήσει σε σημαντικά πρόστιμα και ζημιά στη φήμη του οργανισμού.

Συνηθισμένα λάθη διαχείρισης δεδομένων στον χώρο εργασίας

Τα λάθη στη διαχείριση δεδομένων αναφέρονται σε σφάλματα που γίνονται κατά τη διαχείριση, αποθήκευση ή κοινοποίηση δεδομένων.

Παραδείγματα περιλαμβάνουν:

- αποστολή αρχείων σε λάθος παραλήπτη
- υπερβολική παραχώρηση πρόσβασης σε φακέλους
- αποθήκευση εγγράφων σε μη εγκεκριμένες τοποθεσίες
- προσθήκη περιττών παραληπτών σε emails
- έκθεση εκτυπωμένων ή ορατών δεδομένων
- κοινοποίηση περισσότερων δεδομένων από όσα απαιτεί η εργασία

Αυτά τα λάθη μπορούν να οδηγήσουν σε παραβιάσεις ιδιωτικότητας, διαρροές δεδομένων και ζημιά στη φήμη του οργανισμού.

Τι να κάνετε μετά από ένα λάθος στη διαχείριση δεδομένων

Ακόμη και με τις καλύτερες προφυλάξεις, μπορεί να συμβούν λάθη στη διαχείριση δεδομένων. Το κρίσιμο σημείο είναι να αντιμετωπίζονται άμεσα και υπεύθυνα, ώστε να περιορίζεται η πιθανή ζημιά.

Μια υπεύθυνη αντίδραση συνήθως περιλαμβάνει:

1. αξιολόγηση της κατάστασης
2. να μην αποκρύπτεται το περιστατικό
3. ενημέρωση του αρμόδιου ατόμου ή τμήματος
4. τήρηση των εσωτερικών διαδικασιών
5. περιορισμό της περαιτέρω έκθεσης όπου είναι δυνατό
6. μάθηση από το περιστατικό

Υποενότητα 4 – Ασφαλής Διαχείριση Αρχείων & Εγγράφων



Co-funded by
the European Union

Γιατί είναι σημαντική η οργάνωση αρχείων

Η οργάνωση αρχείων αναφέρεται στη συστηματική μέθοδο αποθήκευσης, ονομασίας και πρόσβασης σε ψηφιακά αρχεία, ώστε να μπορούν να εντοπίζονται εύκολα, να προστατεύονται και να διαχειρίζονται με ασφάλεια.

Η σωστή οργάνωση αρχείων μειώνει κινδύνους όπως η τυχαία έκθεση δεδομένων, η κακή επικοινωνία και η αναποτελεσματική αναζήτηση αρχείων. Διασφαλίζει ότι οι ευαίσθητες πληροφορίες είναι προσβάσιμες μόνο από εξουσιοδοτημένα άτομα και συμβάλλει στη διατήρηση της λειτουργικής αποδοτικότητας.

Παράδειγμα: Χρήση ξεκάθαρης δομής φακέλων και ονοματοδοσίας για την οργάνωση εγγράφων ανά έργο ή τμήμα, αντί για αποθήκευση σε γενικούς ή τυχαίους φακέλους.

Η σαφής ονοματοδοσία, οι δομημένοι φάκελοι, ο έλεγχος εκδόσεων και η χρήση εγκεκριμένων χώρων αποθήκευσης μειώνουν:

- τη σύγχυση
- την ύπαρξη διπλότυπων
- την τυχαία κοινοποίηση
- τη χρήση παρωχημένων εγγράφων
- την περιττή έκθεση δεδομένων

Η οργάνωση αρχείων αποτελεί επομένως τόσο ζήτημα παραγωγικότητας όσο και ασφάλειας.



Βασικές αρχές για την οργάνωση ψηφιακών αρχείων

1. Δημιουργήστε μια λογική δομή

- Δημιουργήστε μια ιεραρχία βασισμένη στη ροή εργασίας σας (π.χ. ανά πελάτη, έργο ή ημερομηνία).
- Διατηρήστε τους υποφακέλους σε περιορισμένο βάθος (3–4 επίπεδα) για να αποφεύγονται τα πολλά κλικ.

2. Συνεπής ονοματοδοσία

- Αναπτύξτε ένα πρότυπο σύστημα ονομασίας (π.χ. YYYY-MM-DD_ΌνομαΕγγράφου_Έκδοση).
- Χρησιμοποιήστε κάτω παύλες () αντί για κενά.
- Αποφύγετε τη χρήση ειδικών χαρακτήρων.

3. Έλεγχος εκδόσεων

- Αποφύγετε ονομασίες όπως final_v2_updated.doc. Χρησιμοποιήστε _v01, _v02 για διαδοχικές εκδόσεις.
- Εξετάστε τη χρήση εργαλείων που καταγράφουν αλλαγές αυτόματα.

4. Τακτική αρχειοθέτηση / καθαρισμός

- Μεταφέρετε ολοκληρωμένα έργα σε φάκελο αρχειοθέτησης για να μειώσετε την ακαταστασία.

Ανακεφαλαίωση βέλτιστων πρακτικών

- Περιορίστε τους υποφακέλους σε 3–4 επίπεδα.
- Χρησιμοποιήστε περιγραφικά ονόματα—σκεφτείτε τι θα αναζητήσετε στο μέλλον.
- Αποθηκεύετε τα αρχεία απευθείας στην τελική τους τοποθεσία, όχι στην επιφάνεια εργασίας.
- Μεταφέρετε τακτικά παλιά αρχεία σε φάκελο αρχειοθέτησης ή σε αποθήκευση cloud.

Αρχές ασφαλέστερης κοινής χρήσης αρχείων

Η κοινοποίηση αρχείων αναφέρεται στη διαδικασία μεταφοράς αρχείων από μία τοποθεσία σε άλλη, είτε εντός ενός οργανισμού είτε προς εξωτερικούς συνεργάτες, διασφαλίζοντας ότι τα αρχεία διαμοιράζονται με ασφάλεια και με τον κατάλληλο τρόπο.

Η κοινοποίηση αρχείων γίνεται επικίνδυνη όταν χρησιμοποιούνται λανθασμένες ρυθμίσεις ή όταν τα αρχεία κοινοποιούνται σε μη εξουσιοδοτημένα άτομα. Για την προστασία τόσο της ακεραιότητας όσο και της εμπιστευτικότητας των δεδομένων, είναι σημαντικό να ακολουθείται μια δομημένη διαδικασία που περιλαμβάνει έλεγχο πρόσβασης, κρυπτογράφηση και χρήση εγκεκριμένων πλατφορμών.

Παράδειγμα: Αποστολή αρχείου σε εξωτερικό συνεργάτη μέσω κρυπτογραφημένου email, αντί για χρήση μη ασφαλούς δημόσιου συνδέσμου.

Πριν κοινοποιήσετε ένα αρχείο, εξετάστε:

- ποιος πραγματικά χρειάζεται πρόσβαση
- ποιο επίπεδο δικαιωμάτων είναι απαραίτητο
- αν το αρχείο είναι η σωστή έκδοση
- αν η πλατφόρμα που χρησιμοποιείται είναι εγκεκριμένη
- αν η πρόσβαση πρέπει να είναι χρονικά περιορισμένη



Διατήρηση ελέγχου εγγράφων σε ψηφιακά περιβάλλοντα

Σε αντίθεση με την παραδοσιακή κοινοποίηση αρχείων (π.χ. συνημμένα σε email), τα συστήματα ελεγχόμενης πρόσβασης διασφαλίζουν ότι το αρχείο παραμένει σε ένα ελεγχόμενο περιβάλλον, αντί να αντιγράφεται σε πολλαπλές συσκευές.

Σύγχρονες πλατφόρμες όπως το OneDrive, το Google Drive και το SharePoint παρέχουν μηχανισμούς για τον έλεγχο:

- της πρόσβασης (ποιος μπορεί να ανοίξει το αρχείο)
- της ορατότητας (ποιος μπορεί να δει ότι υπάρχει)
- της χρήσης (προβολή, σχολιασμός, επεξεργασία, λήψη)

Αυτό μετατρέπει την κοινοποίηση αρχείων από απλή διανομή σε ελεγχόμενη πρόσβαση.

Παράδειγμα: Αντί να αποστέλλει μια οικονομική αναφορά μέσω email, ένας εργαζόμενος κοινοποιεί έναν σύνδεσμο με περιορισμένη πρόσβαση σε έναν πελάτη.

- Η πρόσβαση περιορίζεται σε συγκεκριμένους χρήστες
- Η δυνατότητα λήψης είναι απενεργοποιημένη
- Η πρόσβαση μπορεί να ανακληθεί οποιαδήποτε στιγμή

Η ασφαλής κοινοποίηση αρχείων δεν αφορά απλώς την αποστολή αρχείων, αλλά τη διατήρηση ελέγχου των δεδομένων σε όλο τον κύκλο ζωής τους.

Ρίσκα

- απώλεια ελέγχου μετά την αποστολή αρχείων
- ανεξέλεγκτη προώθηση ή αντιγραφή
- αποθήκευση ευαίσθητων δεδομένων σε μη ασφαλείς τοποθεσίες
- αδυναμία παρακολούθησης πρόσβασης ή χρήσης

Σωστές Πρακτικές

- Κοινοποιείτε συνδέσμους αντί για συνημμένα αρχεία
- Χρησιμοποιείτε μόνο εγκεκριμένες πλατφόρμες του οργανισμού
- Περιορίζετε την πρόσβαση σε συγκεκριμένους χρήστες
- Ελέγχετε τακτικά και αφαιρείτε την πρόσβαση όταν δεν είναι πλέον απαραίτητη

Προστασία ευαίσθητων εγγράφων

Η προστασία ευαίσθητων εγγράφων περιλαμβάνει την ασφάλεια τόσο του ορατού περιεχομένου όσο και των κρυφών δεδομένων γνωστών ως μεταδεδομένα (metadata) μέσα σε ένα αρχείο, ώστε να αποφεύγεται η μη σκόπιμη αποκάλυψη πληροφοριών.

Τα έγγραφα συχνά περιέχουν κρυφές πληροφορίες που δεν είναι ορατές κατά την κανονική προβολή, όπως στοιχεία συγγραφέα, ιστορικό επεξεργασίας, καταγεγραμμένες αλλαγές, εσωτερικά σχόλια, διαδρομές αρχείων ή αναφορές συστήματος.

Αυτά τα μεταδεδομένα μπορούν να αποκαλύψουν εμπιστευτικές πληροφορίες του οργανισμού εάν δεν αφαιρεθούν.

Παράδειγμα: Ένας εργαζόμενος κοινοποιεί ένα έγγραφο Word εξωτερικά χωρίς να το «καθαρίσει». Ο παραλήπτης μπορεί να δει εσωτερικές συζητήσεις, προηγούμενες επεξεργασίες και ονόματα εργαζομένων ή πελατών.

Η ασφάλεια δεν αφορά μόνο την προστασία του ορατού περιεχομένου, αλλά και τον έλεγχο των κρυφών και παρασκηνιακών πληροφοριών.

Ρίσκα

- έκθεση εσωτερικής στρατηγικής ή επικοινωνίας
- αποκάλυψη εμπιστευτικών πληροφοριών πελατών
- ζημιά στη φήμη και κίνδυνοι μη συμμόρφωσης με τον GDPR

Σωστή Πρακτική

- Χρησιμοποιείτε κρυπτογράφηση εγγράφων για ευαίσθητα αρχεία
- Εφαρμόζετε προστασία με κωδικό όπου είναι απαραίτητο
- Αφαιρείτε μεταδεδομένα χρησιμοποιώντας εργαλεία όπως το "Inspect Document"
- Κοινοποιείτε τους κωδικούς μέσω ξεχωριστού καναλιού επικοινωνίας

Υποενότητα 5 – Υπεύθυνη χρήση εργαλείων Τεχνητής Νοημοσύνης



Τεχνητή Νοημοσύνη: Εργαλείο παραγωγικότητας ή παράγοντας κινδύνου;

Τα εργαλεία Τεχνητής Νοημοσύνης (TN) είναι λογισμικά που χρησιμοποιούν μηχανική μάθηση και τεχνητή νοημοσύνη για την επεξεργασία δεδομένων, την αυτοματοποίηση εργασιών και την παραγωγή πληροφοριών.

Η TN μπορεί να ενισχύσει την παραγωγικότητα, αλλά μπορεί επίσης να δημιουργήσει κινδύνους, ιδιαίτερα όταν εμπλέκονται προσωπικά ή ευαίσθητα δεδομένα. Η υπεύθυνη χρήση της TN σημαίνει διασφάλιση της ιδιωτικότητας, της ασφάλειας και της συμμόρφωσης με τη νομοθεσία.

Τα εργαλεία TN μπορούν να βοηθήσουν σε:

- σύνοψη πληροφοριών
- δομή και οργάνωση κειμένου
- δημιουργία πρώτων προσχεδίων
- υποστήριξη οργάνωσης ιδεών

Ρίσκο

Κάθε εντολή (prompt) που εισάγεται σε ένα δημόσιο σύστημα TN αποτελεί πιθανή μεταφορά δεδομένων σε εξωτερικό σύστημα

Παράδειγμα:

Εάν χρησιμοποιείτε TN για τη σύνοψη σχολίων πελατών, πρέπει να διασφαλίσετε ότι δεν περιλαμβάνονται προσωπικά αναγνωρίσιμες πληροφορίες (PII) στο σύνολο δεδομένων.

Η TN δεν είναι απλώς ένα εργαλείο, αλλά ένα περιβάλλον επεξεργασίας δεδομένων.

Κίνδυνοι από τη χρήση εργαλείων Τεχνητής Νοημοσύνης

Ρίσκο 1: Μη εξουσιοδοτημένη χρήση προσωπικών δεδομένων

Κοινοποίηση ή χρήση προσωπικών πληροφοριών χωρίς κατάλληλη συγκατάθεση ή μέτρα ασφάλειας.

Ρίσκο 2: Κακή χρήση αποτελεσμάτων ΤΝ

Η ΤΝ μπορεί να παράγει πληροφορίες, αλλά αν χρησιμοποιηθούν λανθασμένα, μπορεί να οδηγήσουν σε μεροληπτικές ή άδικες αποφάσεις

Ρίσκο 3: Μη συμμόρφωση με τη νομοθεσία προστασίας δεδομένων

Παραβίαση νόμων όπως ο GDPR λόγω λανθασμένης διαχείρισης προσωπικών ή ευαίσθητων δεδομένων.

Παράδειγμα: Χρήση ΤΝ για ανάλυση σχολίων πελατών, συμπεριλαμβάνοντας ευαίσθητα δεδομένα όπως αριθμούς τηλεφώνου ή διευθύνσεις email.

Η ΤΝ πρέπει να χρησιμοποιείται για:

- υποστήριξη της λήψης αποφάσεων
- βελτίωση της παραγωγικότητας

ΟΧΙ για:

- αντικατάσταση της επαγγελματικής κρίσης
- επεξεργασία ευαίσθητων δεδομένων χωρίς έλεγχο

Βέλτιστες πρακτικές για την υπεύθυνη χρήση της Τεχνητής Νοημοσύνης

Πρακτική 1: Ανώνυμοποιείτε τα δεδομένα

Ανώνυμοποιείτε πάντα τα δεδομένα πριν τα εισάγετε σε εργαλεία ΤΝ.

Πρακτική 2: Αποφύγετε την κοινοποίηση ευαίσθητων δεδομένων

Κοινοποιείτε προσωπικά δεδομένα μόνο όταν είναι απολύτως απαραίτητο και με ρητή έγκριση.

Πρακτική 3: Επιλογή συμμορφούμενων εργαλείων Τεχνητής Νοημοσύνης

Επιλέγετε εργαλεία ΤΝ που συμμορφώνονται με τη νομοθεσία προστασίας δεδομένων (π.χ. GDPR).

Παράδειγμα:

Για ανάλυση συναισθήματος πελατών, αφαιρέστε ή ανωνυμοποιήστε προσωπικά αναγνωρίσιμα δεδομένα (π.χ. ονόματα, email) πριν τα εισάγετε στο σύστημα.

Ψευδαισθήσεις Τεχνητής Νοημοσύνης και ανεξέλεγκτη χρήση εργαλείων ΤΝ

Η ψευδαίσθηση ΤΝ (AI hallucination) είναι όταν η Τεχνητή Νοημοσύνη παράγει λανθασμένες ή παραπλανητικές πληροφορίες και τις παρουσιάζει ως ακριβείς.

Το Shadow AI αναφέρεται στη χρήση μη εγκεκριμένων εργαλείων ΤΝ εκτός του ελέγχου του οργανισμού.

Τα εργαλεία ΤΝ μπορούν να εισάγουν δύο βασικούς κινδύνους:

1. Μη επαληθευμένα αποτελέσματα (ψευδαισθήσεις)
Η ΤΝ μπορεί να φαίνεται αξιόπιστη, αλλά να παρέχει ελλιπείς ή λανθασμένες πληροφορίες ή να δημιουργεί περιεχόμενο χωρίς έγκυρες πηγές.
2. Ανεξέλεγκτη χρήση (Shadow AI)
Οι εργαζόμενοι μπορεί να χρησιμοποιούν προσωπικά εργαλεία ΤΝ για εξοικονόμηση χρόνου, αυτοματοποίηση εργασιών ή επεξεργασία δεδομένων που σχετίζονται με την εργασία.

Και οι δύο αυτοί κίνδυνοι επηρεάζουν τη λήψη αποφάσεων και την προστασία δεδομένων.

Ρίσκα

- λανθασμένες επιχειρησιακές ή τεχνικές αποφάσεις
- επαγγελματικά λάθη και ευθύνη
- απώλεια ελέγχου δεδομένων
- έλλειψη καταγραφής ενεργειών (audit trail) έκθεση οργανωσιακών ή προσωπικών δεδομένων
- χρήση δεδομένων σε εξωτερικά μοντέλα εκπαίδευσης ΤΝ

Σωστές Πρακτικές

- επαληθεύετε πάντα το περιεχόμενο που παράγεται από ΤΝ
- διασταυρώνετε πληροφορίες με αξιόπιστες και επίσημες πηγές
- μην βασίζεστε τυφλά στα αποτελέσματα της ΤΝ
- χρησιμοποιείτε μόνο εγκεκριμένα (εταιρικά) εργαλεία ΤΝ
- αποφεύγετε τη χρήση προσωπικών λογαριασμών ΤΝ για εργασιακές δραστηριότητες

Όταν η ευκολία οδηγεί σε έκθεση δεδομένων

Ένας εργαζόμενος χρησιμοποιεί ένα δημόσιο εργαλείο TN για να αναλύσει σχόλια πελατών και περιλαμβάνει πραγματικά δεδομένα, όπως ονόματα, emails και στοιχεία συναλλαγών. Η ενέργεια φαίνεται αποδοτική, αλλά εισάγει κρυφούς κινδύνους.

Τι συμβαίνει → Τα δεδομένα επεξεργάζονται εκτός του οργανισμού, με αποτέλεσμα την απώλεια ελέγχου και την έκθεση ευαίσθητων προσωπικών πληροφοριών.

Γιατί είναι πρόβλημα;

- κοινοποίηση προσωπικών δεδομένων χωρίς κατάλληλη νομική βάση
- παραβίαση της εμπιστευτικότητας και της αρχής ελαχιστοποίησης δεδομένων
- δημιουργία άμεσου κινδύνου μη συμμόρφωσης με τον GDPR

Επιπτώσεις

- παραβίαση δεδομένων
- νομικές και οικονομικές συνέπειες
- απώλεια εμπιστοσύνης πελατών

Η χρήση TN με πραγματικά δεδομένα χωρίς έλεγχο ισοδυναμεί με κοινοποίησή τους σε τρίτο μέρος.

Σωστή πρακτική

- μην εισάγετε ποτέ προσωπικά δεδομένα σε δημόσια εργαλεία TN
- ανωνυμοποιείτε τα δεδομένα πριν από τη χρήση
- χρησιμοποιείτε μόνο εγκεκριμένες λύσεις TN

Υποενότητα 6 – Εξ αποστάσεως εργασία & Ψηφιακή ευημερία



Ο χώρος εργασίας είναι παντού

Η εξ αποστάσεως εργασία επεκτείνει το εργασιακό περιβάλλον πέρα από το γραφείο, σε σπίτια, δημόσιους χώρους και κινητά περιβάλλοντα.

Όταν εργάζεστε απομακρυσμένα, ο οργανισμός χάνει τον άμεσο έλεγχο σε:

- τα δίκτυα
- τις συσκευές
- το φυσικό περιβάλλον

Αυτό αυξάνει την έκθεση σε κινδύνους ασφάλειας.

Η ψηφιακή ασφάλεια δεν εξαρτάται μόνο από τα συστήματα, αλλά και από το πού και πώς εκτελείται η εργασία.

Κίνδυνοι εξ αποστάσεως εργασίας Κατανόηση της έκθεσης σε κινδύνους

Οι κίνδυνοι της εξ αποστάσεως εργασίας αναφέρονται στις προκλήσεις ασφάλειας και τις πιθανές ευπάθειες που προκύπτουν όταν εργάζεστε εκτός παραδοσιακού γραφειακού περιβάλλοντος, συχνά χρησιμοποιώντας προσωπικές συσκευές ή μη ασφαλή δίκτυα.

Η εξ αποστάσεως εργασία μπορεί να εκθέσει τους χρήστες σε:

- δημόσια ή μη ασφαλή δίκτυα Wi-Fi
- ορατές οθόνες σε δημόσιους χώρους
- κοινόχρηστες ή προσωπικές συσκευές
- συνομιλίες που μπορούν να ακουστούν από τρίτους
- εξοπλισμό που παραμένει χωρίς επίβλεψη
- περιβάλλοντα με περισπασμούς

Η εργασία από απόσταση απαιτεί επομένως συνειδητή και προσεκτική συμπεριφορά προστασίας.

Παράδειγμα: Εργασία από καφετέρια και πρόσβαση σε εταιρικά αρχεία μέσω ανοιχτού Wi-Fi.

Ρίσκα

- υποκλοπή δεδομένων
- μη εξουσιοδοτημένη πρόσβαση
- τυχαία έκθεση ευαίσθητων πληροφοριών

Ασφαλέστερη συμπεριφορά στην εξ αποστάσεως εργασία

Ασφαλέστερες πρακτικές περιλαμβάνουν:

- χρήση πιο ασφαλών δικτύων όπου είναι δυνατό
- προστασία της ορατότητας της οθόνης
- κλείδωμα συσκευών όταν απομακρύνεστε
- διαχωρισμός εργασιακής και προσωπικής χρήσης
- προσεκτική διαχείριση αρχείων εκτός του κύριου χώρου εργασίας
- αποφυγή εκτέλεσης ευαίσθητων εργασιών σε εκτεθειμένα περιβάλλοντα όπου είναι δυνατό

Η εξ αποστάσεως εργασία απαιτεί συνειδητή και προσεκτική συμπεριφορά, όχι αυτόματες συνήθειες.

Από το οικιακό δίκτυο έως την προστασία συσκευών

- αλλάξτε τους προεπιλεγμένους κωδικούς του router
- ενεργοποιήστε ισχυρή κρυπτογράφηση Wi-Fi (WPA2/WPA3)
- χρησιμοποιήστε ξεχωριστά δίκτυα για επαγγελματικές συσκευές
- ενεργοποιήστε VPN όταν εργάζεστε απομακρυσμένα

Ψηφιακή ευημερία ως μέρος της ψηφιακής ασφάλειας

Η ψηφιακή ευημερία αναφέρεται στη βιώσιμη και υγιή χρήση των ψηφιακών τεχνολογιών, διασφαλίζοντας ότι τα άτομα δεν επιβαρύνονται από ψηφιακή υπερφόρτωση, άγχος ή εξουθένωση λόγω υπερβολικής χρήσης ψηφιακών εργαλείων.

Η υπερβολική χρήση ψηφιακών τεχνολογιών, ιδιαίτερα για εργασία, μπορεί να οδηγήσει σε ψηφιακή κόπωση, η οποία μειώνει την παραγωγικότητα, αυξάνει τα λάθη και οδηγεί σε κακή λήψη αποφάσεων.

Παράδειγμα:

Συνεχής έλεγχος emails ή ειδοποιήσεων κατά τη διάρκεια της ημέρας, που οδηγεί σε διάσπαση προσοχής και πνευματική κόπωση.

Πώς η ψηφιακή υπερφόρτωση επηρεάζει την ασφάλεια

Η ψηφιακή υπερφόρτωση μπορεί να οδηγήσει σε:

- βιαστικές αποφάσεις
- ελλιπή έλεγχο πριν από την αποστολή
- απρόσεκτα κλικ
- μειωμένη συγκέντρωση
- συνεχή εναλλαγή εργασιών
- πιο συχνά αποτρέψιμα λάθη

Η ψηφιακή ευημερία δεν αποτελεί μόνο ζήτημα προσωπικής άνεσης, είναι και ζήτημα ασφάλειας.

Πρακτικές συνήθειες ψηφιακής ευημερίας

1. Κάνετε τακτικά σύντομα διαλείμματα

→ μειώνει την κόπωση και βελτιώνει τη συγκέντρωση

2. Διαχειριστείτε τις ειδοποιήσεις

→ περιορίστε τις διακοπές για να αποφύγετε τη συνεχή εναλλαγή εργασιών

3. Χρησιμοποιήστε περιόδους συγκεντρωμένης εργασίας

→ αφιερώστε αδιάκοπο χρόνο σε σύνθετες ή ευαίσθητες εργασίες

4. Επιβραδύνετε πριν στείλετε ή κάνετε κλικ

→ ελέγξτε παραλήπτες, συνδέσμους και συνημμένα πριν ενεργήσετε

5. Δώστε ιδιαίτερη προσοχή σε ευαίσθητα δεδομένα

→ ελέγξτε διπλά το περιεχόμενο, την πρόσβαση και το πλαίσιο πριν την κοινοποίηση

Ένας συγκεντρωμένος χρήστης είναι πιο ασφαλής χρήστης.

Η ψηφιακή ασφάλεια δεν εξαρτάται μόνο από τα εργαλεία, αλλά και από την προσοχή, την πειθαρχία και τη σωστή διαχείριση του εαυτού.

Αναφορές & Περαιτέρω Μελέτη

- European Commission (2024) *EU Data Protection Rules (GDPR)*. Διαθέσιμο στο: https://commission.europa.eu/law/law-topic/data-protection_en
- OECD (2023) *OECD AI Principles Overview*. Διαθέσιμο στο: <https://oecd.ai/en/ai-principles>
- European Commission (2024) *Ethics Guidelines for Trustworthy AI*. Διαθέσιμο στο: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- OECD (2022) *Productivity and Digitalisation in the Workplace*. Διαθέσιμο στο: <https://www.oecd.org/digital>
- ENISA (European Union Agency for Cybersecurity) (2023) *Cyber Hygiene: Guidelines for SMEs and Organisations*. Διαθέσιμο στο: <https://www.enisa.europa.eu/topics/cyber-hygiene>
- National Cyber Security Centre (NCSC) (2023) *Multi-factor authentication (MFA): how to set up and use it*. Διαθέσιμο στο: <https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services>

Πληροφοριακός & Δεδομενικός Γραμματισμός σε Επαγγελματικά Περιβάλλοντα

ΕΝΟΤΗΤΑ 2



Δομή Ενότητας



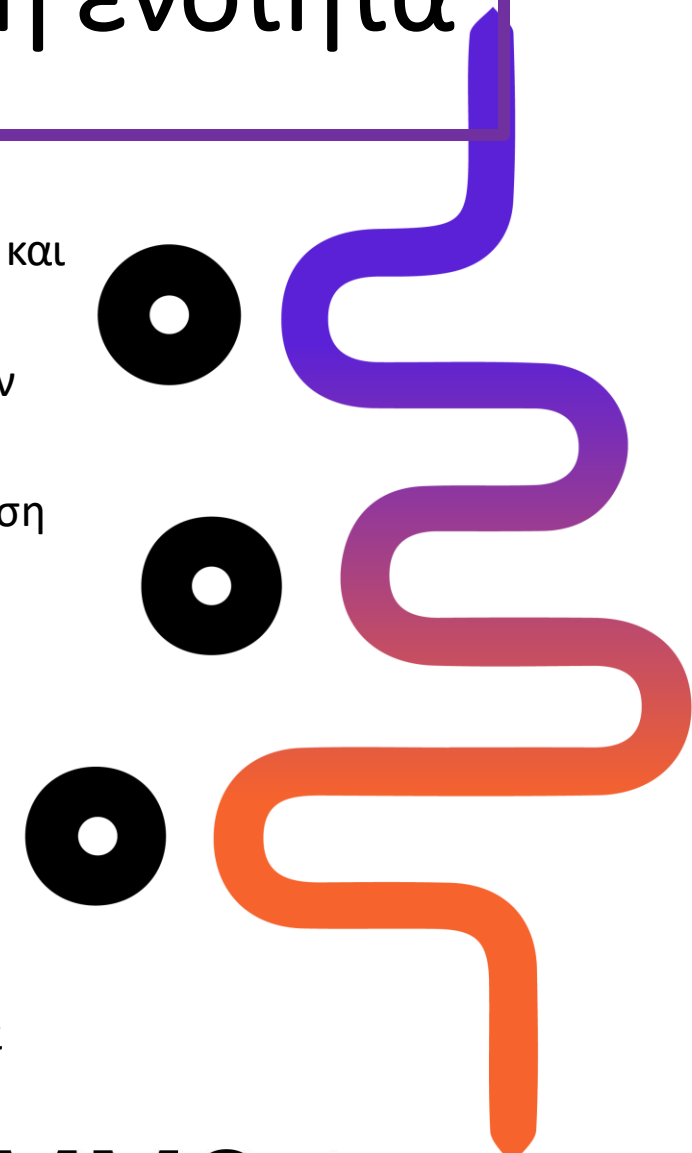
Γιατί είναι σημαντική αυτή η ενότητα

Στους σύγχρονους χώρους εργασίας, η πληροφορία δεν είναι απλώς «κάτι στο οποίο έχουμε πρόσβαση». Αποτελεί έναν βασικό πόρο που επηρεάζει τη δράση, την ποιότητα και την εμπιστοσύνη.

Οι κακές πρακτικές στη διαχείριση πληροφοριών και δεδομένων μπορούν να οδηγήσουν σε:

- Λειτουργικά προβλήματα, όπως καθυστερήσεις, διπλότυπες εγγραφές, σύγχυση, χρήση λανθασμένων εκδόσεων και ασυνεπή αναφορά δεδομένων.
- Οικονομικές συνέπειες, όπως λανθασμένες επιλογές προμηθευτών, ανακριβείς υπολογισμούς και μη αποδοτική χρήση χρόνου και πόρων.
- Κινδύνους συμμόρφωσης και ηθικής, όπως κακή χρήση ευαίσθητων πληροφοριών, ανεπαρκή έλεγχο σε κοινόχρηστα αρχεία και περιορισμένη ιχνηλασιμότητα.
- Ζημιά στη φήμη, όπως μείωση της εμπιστοσύνης από προϊσταμένους, συναδέλφους, πελάτες ή εξωτερικούς συνεργάτες.

Στις μικροεπιχειρήσεις, αυτοί οι κίνδυνοι ενισχύονται, καθώς ένα μόνο λάθος μπορεί να επηρεάσει πολλαπλές διαδικασίες ταυτόχρονα.

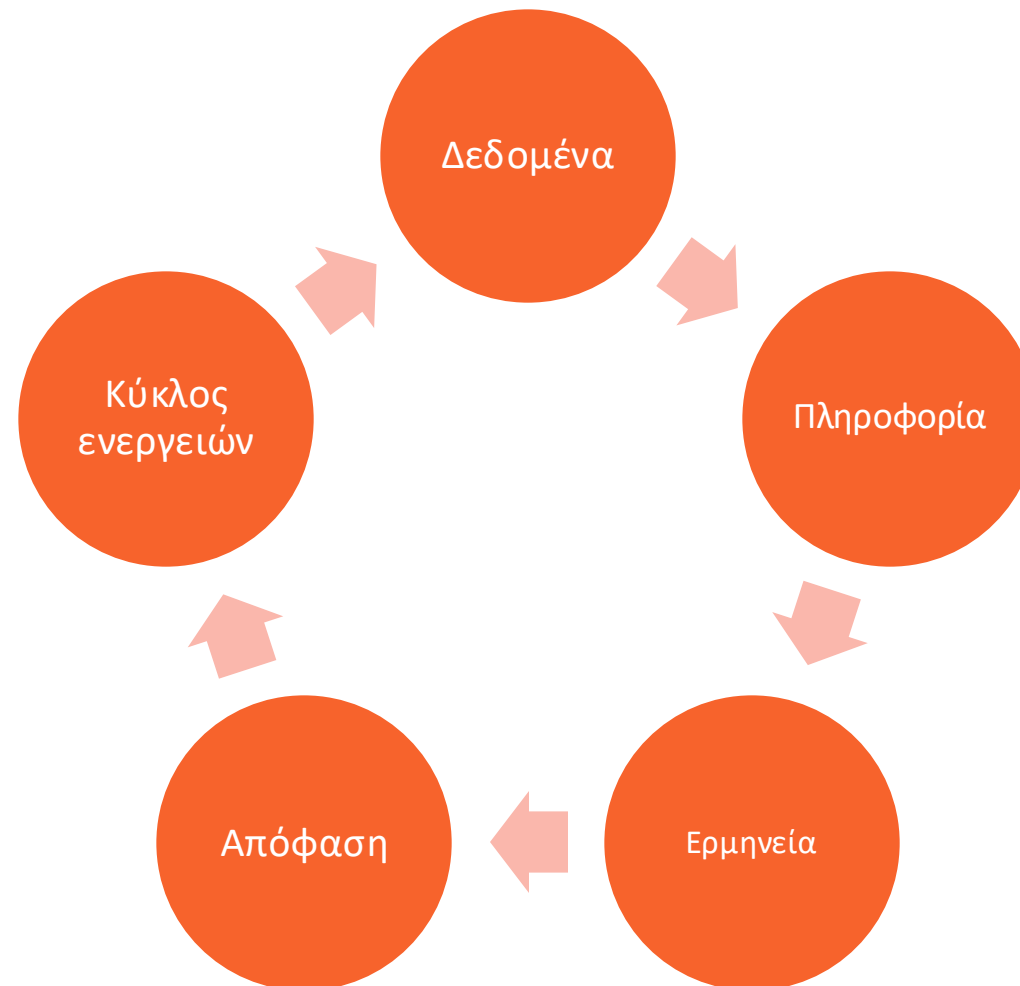


Υποενότητα 1 – Κατανόηση Δεδομένων και Πληροφοριών



Co-funded by
the European Union

Από την πληροφορία στη λήψη αποφάσεων (κύκλος ζωής)



Πληροφοριακός γραμματισμός ως επαγγελματικό πλεονέκτημα

Ο πληροφοριακός γραμματισμός είναι η ικανότητα εντοπισμού, αξιολόγησης, οργάνωσης και χρήσης πληροφοριών με αποτελεσματικό και ηθικό τρόπο. Αποτελεί δεξιότητα που εφαρμόζεται σε κάθε επαγγελματικό πεδίο και είναι κρίσιμη για τη λήψη τεκμηριωμένων αποφάσεων, την επίλυση προβλημάτων και την εξέλιξη της γνώσης στον χώρο εργασίας.

Βασικά στοιχεία του πληροφοριακού γραμματισμού:

- **Εντοπισμός πληροφοριών:** Γνώση του πού να αναζητήσετε, ποιες βάσεις δεδομένων ή πλατφόρμες να χρησιμοποιήσετε και πώς να φιλτράρετε μη σχετικές πληροφορίες.
- **Αξιολόγηση πληροφοριών:** Εκτίμηση της αξιοπιστίας, της ακρίβειας και της συνάφειας των πληροφοριών.
- **Οργάνωση πληροφοριών:** Δημιουργία συστημάτων διαχείρισης που διασφαλίζουν την προσβασιμότητα και την ιχνηλασιμότητα των πληροφοριών.
- **Χρήση πληροφοριών:** Εφαρμογή των πληροφοριών για την επίλυση προβλημάτων, την υποστήριξη αποφάσεων ή τη δημιουργία νέας γνώσης.

Ο πληροφοριακός γραμματισμός δεν περιορίζεται στην απλή πρόσβαση σε δεδομένα.

Αφορά την ανάπτυξη της ικανότητας κριτικής επεξεργασίας των πληροφοριών, ώστε να χρησιμοποιούνται αποτελεσματικά στον χώρο εργασίας.

Στα σύγχρονα επαγγελματικά περιβάλλοντα, η πληροφορία δεν είναι ουδέτερη ή παθητική.

Αποτελεί βασικό πόρο που επηρεάζει άμεσα τις αποφάσεις (ποιες ενέργειες λαμβάνονται και γιατί), τις λειτουργίες (πώς οργανώνεται και εκτελείται η εργασία) και τα αποτελέσματα (ποιότητα, αποδοτικότητα και επίδοση).

Δεδομένα vs Πληροφορία vs Γνώση

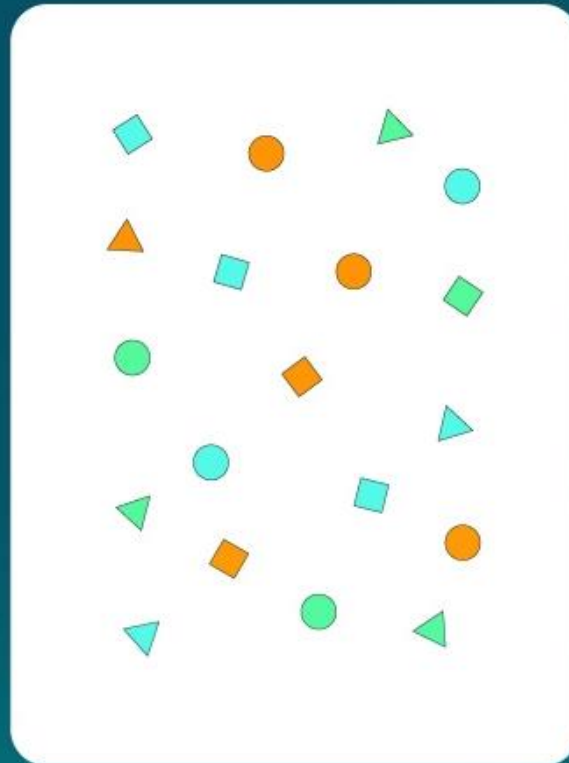
- **Δεδομένα:** Ακατέργαστα γεγονότα και αριθμοί που έχουν ελάχιστο νόημα από μόνα τους.
Παράδειγμα: οι «25, 10, 35» είναι απλώς αριθμοί χωρίς πλαίσιο.
- **Πληροφορία:** Δεδομένα που έχουν οργανωθεί ή επεξεργαστεί ώστε να αποκτήσουν νόημα.
Παράδειγμα: Μια αναφορά που παρουσιάζει τα στοιχεία πωλήσεων του τελευταίου τριμήνου δίνει πλαίσιο στους αριθμούς, όπως τάσεις ή συμπεράσματα.
- **Γνώση:** Πληροφορία που έχει ερμηνευτεί, κατανοηθεί και εφαρμοστεί στη λήψη αποφάσεων ή στη δράση. Παράδειγμα: Ένας μάνατζερ που χρησιμοποιεί την αναφορά πωλήσεων για να προβλέψει τις πωλήσεις του επόμενου τριμήνου και να προσαρμόσει τη στρατηγική marketing.

Η κατανόηση της διαφοράς μεταξύ αυτών των εννοιών είναι κρίσιμη για τη λήψη τεκμηριωμένων αποφάσεων.

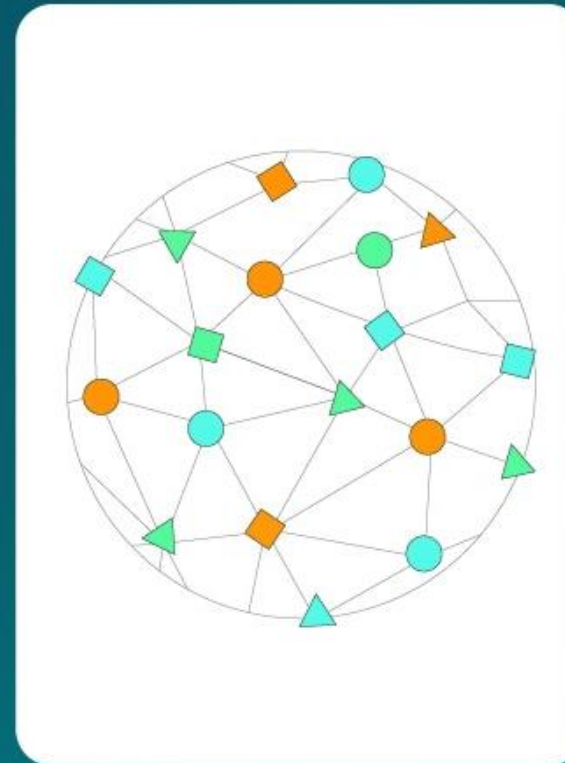
Το κλειδί για την αποτελεσματική χρήση της πληροφορίας είναι η κατανόηση του πλαισίου της και η μετατροπή της σε αξιοποιήσιμη γνώση. Τα δεδομένα από μόνα τους είναι συχνά άχρηστα χωρίς την κατάλληλη ερμηνεία.

Δεδομένα vs Πληροφορία vs Γνώση

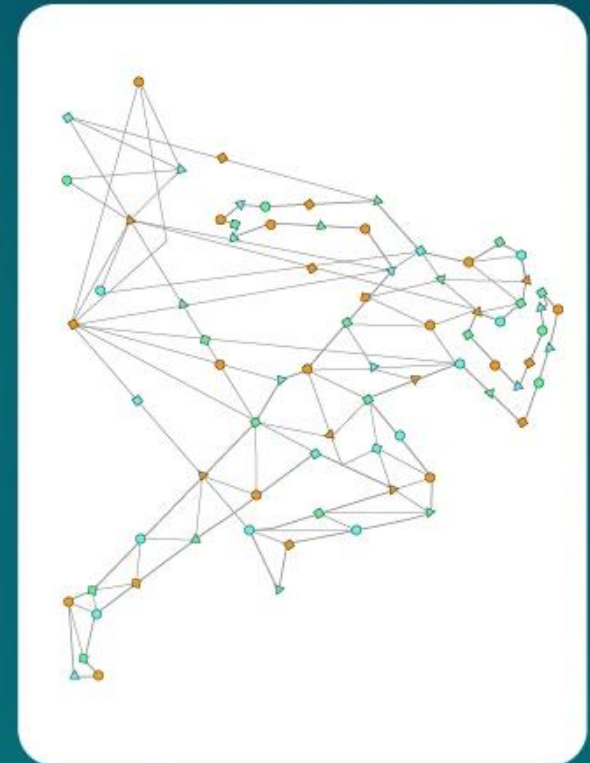
Data



Information



Knowledge



Δομημένα vs Μη δομημένα δεδομένα

- **Δομημένα δεδομένα:** Δεδομένα που είναι οργανωμένα σε γραμμές και στήλες, συνήθως σε βάσεις δεδομένων ή υπολογιστικά φύλλα. Είναι εύκολα στην καταχώρηση, αναζήτηση, φιλτράρισμα, αποθήκευση, ερώτηση και ανάλυση. Παράδειγμα: Μια βάση δεδομένων πελατών με πεδία όπως όνομα πελάτη, αριθμός τηλεφώνου και email.
- **Μη δομημένα δεδομένα:** Δεδομένα που δεν ακολουθούν προκαθορισμένη μορφή. Είναι πιο δύσκολο να οργανωθούν και να αναλυθούν. Παράδειγμα: Emails, αναρτήσεις σε μέσα κοινωνικής δικτύωσης, αρχεία κειμένου, PDFs και αρχεία πολυμέσων.

Τα μη δομημένα δεδομένα συχνά περιέχουν πολύτιμες πληροφορίες, αλλά απαιτούν κατάλληλη επεξεργασία για να αξιοποιηθούν πλήρως.

Τα δομημένα δεδομένα είναι πιο εύκολα στην επεξεργασία και ανάλυση, ενώ τα μη δομημένα δεδομένα συχνά κρύβουν σημαντικά ευρύματα που απαιτούν επιπλέον εργασία για να ερμηνευτούν και να οργανωθούν.

Οι επαγγελματίες χρειάζεται να κατανοούν και να διαχειρίζονται και τους δύο τύπους δεδομένων, καθώς παίζουν καθοριστικό ρόλο στη λήψη αποφάσεων και στην ανάλυση.

Ένας ολοκληρωμένος οδηγός σύγκρισης δομημένων και μη δομημένων δεδομένων (Structured vs Unstructured Data) αναδεικνύει τις βασικές διαφορές στη μορφή, την αποθήκευση και την ανάλυση, καθώς και τον τρόπο με τον οποίο σύγχρονες αρχιτεκτονικές όπως τα Lakehouse διαχειρίζονται όλους τους τύπους δεδομένων για την υποστήριξη της επιχειρηματικής ευφυΐας και της Τεχνητής Νοημοσύνης.

[Structured vs Unstructured Data](#)

Unstructured Data



Vs

Structured Data



Πραγματικότητα στον χώρο εργασίας

Στον σύγχρονο χώρο εργασίας, οι εργοδότες αναμένουν όλο και περισσότερο:

- κριτική σκέψη
- ικανότητα αξιολόγησης πληροφοριών
- ευελιξία στη διαχείριση διαφορετικών πηγών δεδομένων
- μάθηση μέσω πράξης και επίλυση προβλημάτων

Σε ένα τυπικό επαγγελματικό περιβάλλον, ιδιαίτερα στις ΜΜΕ, οι εργαζόμενοι συχνά διαχειρίζονται πολλαπλές εργασίες και καλούνται να λάβουν γρήγορες αποφάσεις.

Αυτό το περιβάλλον συχνά σημαίνει περιορισμένη πρόσβαση σε «τέλεια» δεδομένα και ύπαρξη ελλιπών πληροφοριών.

Παράδειγμα:

Ένας υπεύθυνος πωλήσεων μπορεί να χρειάζεται να αναλύσει τάσεις της αγοράς, σχόλια πελατών και εσωτερικά δεδομένα απόδοσης, αλλά να έχει πρόσβαση μόνο σε αποσπασματικές πληροφορίες.

Οι τεκμηριωμένες αποφάσεις απαιτούν συχνά τη σύνθεση διαφορετικών τύπων δεδομένων και πληροφοριών από πολλαπλές πηγές.

Η κατανόηση της φύσης των πληροφοριών και η συστηματική οργάνωσή τους είναι κρίσιμη για την αποφυγή λαθών και αναποτελεσματικότητας.

Κίνδυνοι κακής διαχείρισης πληροφοριών

Συνέπειες κακής διαχείρισης πληροφοριών:

- **Λανθασμένες αποφάσεις:** Η χρήση λανθασμένων ή μη αξιόπιστων πληροφοριών μπορεί να οδηγήσει σε κακές επιχειρηματικές αποφάσεις.
- **Λειτουργικές καθυστερήσεις:** Η κακή διαχείριση δεδομένων μπορεί να προκαλέσει καθυστερήσεις σε διαδικασίες ή χαμένες προθεσμίες.
- **Κίνδυνοι συμμόρφωσης:** Η χρήση παρωχημένων ή ανακριβών πληροφοριών μπορεί να οδηγήσει σε αποτυχία συμμόρφωσης με κανονιστικές απαιτήσεις.
- **Οικονομικές απώλειες:** Λανθασμένα οικονομικά δεδομένα μπορεί να οδηγήσουν σε κακές επενδύσεις ή χαμένες ευκαιρίες.

Παράδειγμα: Ένας εργαζόμενος μπορεί να κάνει λανθασμένες οικονομικές προβλέψεις βασισμένες σε παρωχημένα δεδομένα πωλήσεων, οδηγώντας σε κακές αποφάσεις προϋπολογισμού και οικονομικές απώλειες.

Η αναποτελεσματική διαχείριση πληροφοριών δημιουργεί ένα φαινόμενο «ντόμινο», που μπορεί να οδηγήσει σε λειτουργική αναποτελεσματικότητα και σημαντικούς επιχειρηματικούς κινδύνους.

Μάθετε περισσότερα για τους κινδύνους της κακής διαχείρισης δεδομένων στον οδηγό της IBM για τη Διαχείριση Δεδομένων [IBM Guide to Data Management](#)

Τι σημαίνει αυτό για εσάς

Για να αξιοποιείτε σωστά την πληροφορία, πρέπει:

- να κατανοείτε τι είναι πληροφορία και τι δεν είναι
- να αναγνωρίζετε πότε η πληροφορία είναι ελλιπής ή μη αξιόπιστη
- να οργανώνετε τα δεδομένα με τρόπο που υποστηρίζει τη δράση και την ιχνηλασιμότητα
- να εφαρμόζετε την πληροφορία με κρίση και υπευθυνότητα

Οι εργοδότες δίνουν ολοένα και μεγαλύτερη έμφαση σε δεξιότητες, όπως η προσαρμοστικότητα, η πρωτοβουλία και η κριτική σκέψη, αντί για στενά ορισμένες τεχνικές δεξιότητες.

Η διαχείριση πληροφοριών δεν αφορά πλέον μόνο τη συλλογή δεδομένων, αλλά κυρίως την αποτελεσματική αξιοποίησή τους.

Η ανάπτυξη μιας ολιστικής προσέγγισης στην πληροφορία, που συνδυάζει δεξιότητες διαχείρισης δεδομένων με κριτική σκέψη και προσαρμοστικότητα, είναι απαραίτητη για την κάλυψη των σύγχρονων απαιτήσεων του χώρου εργασίας.

Υποενότητα 2 – Αναζήτηση και Αξιολόγηση Πληροφοριών



Co-funded by
the European Union

Quiz3

Παρακαλούμε επιλέξτε τη σωστή απάντηση.

Ποια πηγή πρέπει να τίθεται σε προτεραιότητα για επαγγελματικές αποφάσεις;

- ☐ 3. Επίσημη θεσμική πηγή
- ☐ 1. Άρθρο σε ιστολόγιο (blog)
- ☐ 2. Ανάρτηση στα μέσα κοινωνικής δικτύωσης
- ☐ 4. Περίληψη παραχθείσα από AI

Τύποι αναγκών πληροφόρησης στον χώρο εργασίας

Σε κάθε επαγγελματικό περιβάλλον, οι εργαζόμενοι χρειάζεται να αναζητούν και να επεξεργάζονται πληροφορίες για να ολοκληρώνουν εργασίες, να επιλύουν προβλήματα ή να λαμβάνουν αποφάσεις. Οι ανάγκες αυτές διαφέρουν ανάλογα με τον κλάδο και τον ρόλο.

Βασικοί τύποι αναγκών πληροφόρησης περιλαμβάνουν:

- **Λειτουργικές πληροφορίες (Operational Information):** Πληροφορίες που απαιτούνται για την ομαλή καθημερινή λειτουργία (π.χ. στοιχεία προμηθευτών, τιμές, επίπεδα αποθεμάτων).
- **Κανονιστικές πληροφορίες (Regulatory Information):** Πληροφορίες που σχετίζονται με νόμους, κανονισμούς και απαιτήσεις συμμόρφωσης (π.χ. οδηγίες υγείας και ασφάλειας, πολιτικές GDPR).
- **Τεχνικές πληροφορίες (Technical Information):** Πληροφορίες που σχετίζονται με εργαλεία, εξοπλισμό ή λογισμικό (π.χ. εγχειρίδια χρήσης, οδηγοί αντιμετώπισης προβλημάτων).
- **Πληροφορίες που σχετίζονται με πελάτες (Customer-Related Information):** Πληροφορίες για ανάγκες, σχόλια, προτιμήσεις και ιστορικό πελατών (π.χ. συστήματα CRM, αιτήματα εξυπηρέτησης).

Ο τύπος της πληροφορίας που απαιτείται μπορεί να διαφέρει σημαντικά ανάλογα με την εργασία. Η κατανόηση του είδους της πληροφορίας που χρειάζεστε βοηθά να στοχεύετε πιο αποτελεσματικά την αναζήτησή σας.

Επαγγελματικές πηγές

Τι καθιστά μια πηγή επαγγελματική;

- Αξιοπιστία (Credibility): Αξιόπιστες πηγές προέρχονται από ειδικούς ή αναγνωρισμένους οργανισμούς στον τομέα. Για παράδειγμα, άρθρα από ακαδημαϊκά περιοδικά, κυβερνητικές δημοσιεύσεις ή αξιόπιστα ιδρύματα.
- Αυθεντία (Authority): Πηγές που προέρχονται από αναγνωρισμένους συγγραφείς ή εκδότες, όπως ειδικοί του κλάδου, καθηγητές ή επαγγελματικές ενώσεις.
- Ακρίβεια (Accuracy): Πληροφορίες που μπορούν να επαληθευτούν μέσω πολλαπλών πηγών, διασφαλίζοντας ότι είναι έγκυρες και αξιόπιστες.
- Συνάφεια (Relevance): Η πληροφορία πρέπει να είναι ενημερωμένη και σχετική με τη συγκεκριμένη εργασία ή ερώτημα.

Παραδείγματα επαγγελματικών πηγών:

- ακαδημαϊκά περιοδικά (π.χ. ResearchGate, Academia.edu)
- εκθέσεις κλάδου (π.χ. από εταιρείες όπως Deloitte)
- κυβερνητικές δημοσιεύσεις (π.χ. κανονισμοί ΕΕ, επίσημες οδηγίες)

Η χρήση επαγγελματικών πηγών διασφαλίζει ότι οι πληροφορίες είναι ακριβείς, αξιόπιστες και έγκυρες, κάτι που είναι κρίσιμο για τη λήψη τεκμηριωμένων αποφάσεων στον χώρο εργασίας.

Κατανόηση διαφορετικών τύπων πηγών πληροφόρησης

Στα επαγγελματικά περιβάλλοντα, η πληροφορία παράγεται και προσπελαύνεται μέσω διαφορετικών τύπων πηγών, καθεμία με διαφορετικά επίπεδα αξιοπιστίας, εγκυρότητας και σκοπού:

- Επίσημες / Θεσμικές πηγές (π.χ. Ευρωπαϊκή Επιτροπή, νομοθεσία, ρυθμιστικοί φορείς, εσωτερικές πολιτικές) → Υψηλή αξιοπιστία, επίσημη επικύρωση, νομική σημασία
- Επαγγελματικές / Κλαδικές πηγές (π.χ. τεχνική τεκμηρίωση, δεδομένα προμηθευτών, εκθέσεις κλάδου) → Πρακτικές και εξειδικευμένες, αλλά μπορεί να περιλαμβάνουν εμπορική προκατάληψη
- Εσωτερικές οργανωσιακές πηγές (π.χ. αρχεία εταιρείας, αναφορές, βάσεις δεδομένων, προηγούμενη εργασία) → Σχετικές με το πλαίσιο του οργανισμού και λειτουργικά χρήσιμες, αλλά μπορεί να είναι παρωχημένες ή ασυνεπείς
- Ανοιχτές διαδικτυακές πηγές (π.χ. ιστοσελίδες, blogs, forums, άρθρα) → Εύκολη πρόσβαση, μεταβλητή ποιότητα, συχνά χωρίς επαλήθευση
- Περιεχόμενο που παράγεται από ΤΝ (π.χ. ChatGPT, Gemini, copilots) → Γρήγορο και δομημένο, αλλά απαιτεί επαλήθευση και κριτική σκέψη

Η αξία της πληροφορίας εξαρτάται σε μεγάλο βαθμό από την προέλευσή της.

Στρατηγικές αναζήτησης

Η αποτελεσματική αναζήτηση είναι απαραίτητη για την εύρεση σχετικών και αξιόπιστων πληροφοριών.

Βασικές στρατηγικές περιλαμβάνουν:

- Χρήση ακριβών λέξεων-κλειδιών: Κατά την αναζήτηση στο διαδίκτυο ή σε βάσεις δεδομένων, η χρήση συγκεκριμένων και στοχευμένων λέξεων-κλειδιών οδηγεί σε πιο σχετικά αποτελέσματα.
- Εφαρμογή φίλτρων: Οι περισσότερες μηχανές αναζήτησης και βάσεις δεδομένων επιτρέπουν φιλτράρισμα αποτελεσμάτων βάσει κριτηρίων όπως ημερομηνία, συγγραφέας ή τύπος πηγής (π.χ. ακαδημαϊκά άρθρα, εκθέσεις).
- Χρήση πολλαπλών πηγών: Μην βασίζεστε σε μία μόνο πηγή. Η διασταύρωση πληροφοριών από διαφορετικές πηγές αυξάνει την ακρίβεια και την αξιοπιστία.

Μια αποτελεσματική στρατηγική αναζήτησης απαιτεί περισσότερα από την απλή πληκτρολόγηση λέξεων σε μια μηχανή αναζήτησης.

Ορίστε ξεκάθαρα το ερώτημα πριν ξεκινήσετε την αναζήτηση.

Η καλή αναζήτηση ξεκινά από σαφή ορισμό του προβλήματος, όχι από το εργαλείο.

Κίνδυνοι στην αναζήτηση

Πιθανά προβλήματα κατά την αναζήτηση πληροφοριών:

- Παρωχημένη πληροφορία: Η χρήση παλιών δεδομένων ή ερευνών μπορεί να οδηγήσει σε αποφάσεις βασισμένες σε ξεπερασμένα στοιχεία.
- Μεροληψία στις πηγές: Ορισμένες πηγές μπορεί να παρουσιάζουν πληροφορίες με συγκεκριμένη προκατάληψη (π.χ. εμπορικές ιστοσελίδες που προωθούν τα δικά τους προϊόντα).
- Ελλιπής πληροφορία: Μια πηγή μπορεί να παραλείπει σημαντικό πλαίσιο ή βασικά στοιχεία, οδηγώντας σε παρερμηνείες ή λάθη.

Συνηθισμένοι κίνδυνοι:

- χρήση μη επαληθευμένων διαδικτυακών πηγών, όπως blogs ή προσωπικές ιστοσελίδες
- εξάρτηση από μέσα κοινωνικής δικτύωσης ή περιεχόμενο χρηστών που μπορεί να μην είναι αξιόπιστο

Για τη λήψη τεκμηριωμένων αποφάσεων, είναι κρίσιμο να γνωρίζετε τους κινδύνους που σχετίζονται με την αναζήτηση και χρήση πληροφοριών.

Η αξιολόγηση της αξιοπιστίας των πηγών αποτελεί βασικό μέρος της διαδικασίας συλλογής πληροφοριών.

Εργαλεία αναζήτησης πληροφοριών: Παραδοσιακές μηχανές αναζήτησης

Παραδοσιακές μηχανές αναζήτησης:

Η Google είναι η πιο διαδεδομένη μηχανή αναζήτησης παγκοσμίως. Χρησιμοποιεί έναν συνδυασμό αλγορίθμων για να κατατάσσει ιστοσελίδες με βάση τη συνάφεια και την ποιότητά τους.

Πώς λειτουργεί η Google:

- **Ανίχνευση (Crawling):** Η Google χρησιμοποιεί bots για να εξερευνά το διαδίκτυο και να εντοπίζει ιστοσελίδες.
- **Ευρετηρίαση (Indexing):** Οι σελίδες κατηγοριοποιούνται με βάση λέξεις-κλειδιά, συνδέσμους και περιεχόμενο.
- **Κατάταξη (Ranking):** Με βάση αλγορίθμους, η Google κατατάσσει τις σελίδες ανάλογα με τη συνάφεια και την αυθεντία τους, λαμβάνοντας υπόψη παράγοντες όπως λέξεις-κλειδιά, backlinks, ασφάλεια ιστοσελίδας και αλληλεπίδραση χρηστών.

Συμβουλές αναζήτησης:

- χρησιμοποιείτε συγκεκριμένες λέξεις-κλειδιά για πιο στοχευμένα αποτελέσματα
- εφαρμόζετε φίλτρα (π.χ. χρονικό εύρος) για περιορισμό αποτελεσμάτων
- χρησιμοποιείτε το Google Scholar για ακαδημαϊκές πηγές
- χρησιμοποιείτε το Google News για ενημερωμένες πληροφορίες

Τα πρώτα αποτελέσματα δεν είναι πάντα:

- τα πιο ακριβή
- τα πιο αξιόπιστα

Για αυτό πρέπει να:

- ελέγχετε πολλαπλά αποτελέσματα
- κοιτάτε πέρα από την πρώτη σελίδα
- αξιολογείτε την αξιοπιστία της πηγής

Κίνδυνος

- Υπόθεση ότι: «το πρώτο αποτέλεσμα = το καλύτερο αποτέλεσμα»
- Οι μηχανές αναζήτησης βελτιστοποιούν τα αποτελέσματα για συνάφεια και αλληλεπίδραση, όχι πάντα για αλήθεια ή αξιοπιστία.

Η νέα τάση: Αναζήτηση πληροφοριών με Τεχνητή Νοημοσύνη

Τα εργαλεία Τεχνητής Νοημοσύνης, όπως το ChatGPT και το Google Gemini, αλλάζουν τον τρόπο με τον οποίο αλληλεπιδρούμε με τις μηχανές αναζήτησης.

Αντί να επιστρέφουν απλώς μια λίστα από συνδέσμους, χρησιμοποιούν προηγμένη επεξεργασία φυσικής γλώσσας (NLP) για να παρέχουν άμεσες απαντήσεις, να συνοψίζουν σύνθετα θέματα γρήγορα, να κατανοούν ερωτήματα σε φυσική γλώσσα και να υποστηρίζουν διαλογική αναζήτηση.

Πώς λειτουργούν τα εργαλεία TN:

- Κατανόηση εισόδου (Input Understanding): Ο χρήστης εισάγει μια ερώτηση και το σύστημα αναλύει το πλαίσιο και την πρόθεση.
- Ανάκτηση δεδομένων (Data Retrieval): Η TN αξιοποιεί μεγάλους όγκους προεκπαιδευμένης γνώσης και δεδομένων (βιβλία, ιστοσελίδες, αναφορές κ.λπ.).
- Παραγωγή απάντησης (Response Generation): Δημιουργεί μια απάντηση βασισμένη σε μοτίβα, γνώσεις και εκπαίδευση, παρέχοντας σαφή και άμεση πληροφόρηση αντί για απλούς συνδέσμους.
- Παράδειγμα: Αν ρωτήσετε «Ποιες είναι οι βασικές διαφορές μεταξύ δομημένων και μη δομημένων δεδομένων;», η TN παρέχει άμεσα μια δομημένη απάντηση αντί για λίστα άρθρων.

Γιατί η αναζήτηση με TN αποτελεί σημαντική εξέλιξη:

- Αποδοτικότητα: Παρέχει άμεσες απαντήσεις, εξοικονομώντας χρόνο.
- Κατανόηση συμφραζομένων: Μπορεί να ερμηνεύσει σύνθετα ή πολυεπίπεδα ερωτήματα και να δώσει πιο ολοκληρωμένες απαντήσεις.
- Εξατομικευμένη αλληλεπίδραση: Μπορεί να λαμβάνει υπόψη προηγούμενες αλληλεπιδράσεις και να βελτιώνει σταδιακά τις απαντήσεις.

Αξιολόγηση πληροφοριών: Βασικά κριτήρια

Πριν χρησιμοποιήσετε πληροφορίες, αξιολογήστε:

- **Ακρίβεια (Accuracy):** Είναι η πληροφορία σωστή και χωρίς λάθη; Μπορεί να επαληθευτεί μέσω άλλων αξιόπιστων πηγών;
- **Συνάφεια (Relevance):** Απαντά άμεσα στο ερώτημα ή στο πρόβλημα; Είναι επίκαιρη και χρήσιμη για τη λήψη αποφάσεων;
- **Αυθεντία (Authority):** Ποιος είναι ο συγγραφέας ή η πηγή; Διαθέτει την απαραίτητη γνώση ή τα κατάλληλα προσόντα;
- **Επικαιρότητα (Timeliness):** Είναι η πληροφορία πρόσφατη; Σε ταχέως μεταβαλλόμενους τομείς, τα παρωχημένα δεδομένα μπορεί να οδηγήσουν σε λάθος αποφάσεις.
- **Σκοπός (Purpose):** Ποια είναι η πρόθεση της πληροφορίας; Είναι αντικειμενική ή προσπαθεί να πείσει ή να προωθήσει κάτι;

Η παράλειψη αξιολόγησης οδηγεί σε:

- κακή χρήση πληροφοριών
- λανθασμένες αποφάσεις

Να εφαρμόζετε πάντα τουλάχιστον 2–3 από αυτά τα κριτήρια πριν χρησιμοποιήσετε μια πληροφορία.

Η αξιολόγηση αποτελεί φίλτρο απόφασης, όχι προαιρετικό βήμα.

Ο οδηγός αξιολόγησης πληροφοριών του UNC Chapel Hill παρέχει ένα δομημένο και ευρέως χρησιμοποιούμενο πλαίσιο για την εκτίμηση της ποιότητας, της αξιοπιστίας και της χρησιμότητας των πηγών, τόσο σε ακαδημαϊκά όσο και σε επαγγελματικά περιβάλλοντα.

[UNC Chapel Hill – Evaluating Information Guide](#)

Quiz4

Παρακαλούμε επιλέξτε τη σωστή απάντηση.

Ποια είναι η σωστή ενέργεια όταν οι πηγές πληροφοριών συγκρούονται μεταξύ τους;

- ☐ 2. Επιλογή της ταχύτερης απάντησης
- ☐ 4. Παράβλεψη του ζητήματος
- ☐ 3. Σύγκριση και επαλήθευση πολλαπλών πηγών
- ☐ 1. Επιλογή της ευκολότερης πηγής

Εντοπισμός μη αξιόπιστων πληροφοριών

Ενδείξεις μη αξιόπιστης πληροφορίας:

- Έλλειψη πηγής ή αναφοράς: Η απουσία σαφούς πηγής σημαίνει ότι η πληροφορία δεν μπορεί να επαληθευτεί και θεωρείται ύποπτη.
- Μεροληψία ή συναισθηματική γλώσσα: Πληροφορίες που χρησιμοποιούν έντονα συναισθηματική ή προκατειλημμένη γλώσσα για να προωθήσουν μια άποψη πρέπει να αντιμετωπίζονται με προσοχή.
- Ασαφής ή παραπλανητικός συγγραφέας: Εάν τα προσόντα του συγγραφέα δεν είναι σαφή ή δεν σχετίζονται με το θέμα, απαιτείται επιφυλακτικότητα.
- Υπερβολικοί ισχυρισμοί: Δηλώσεις που υπόσχονται ακραία ή «πολύ καλά για να είναι αληθινά» αποτελέσματα χωρίς αποδείξεις.
- Ασυνεπής ή αντιφατική πληροφορία: Εάν η πληροφορία έρχεται σε αντίθεση με καθιερωμένα δεδομένα ή επιστημονική συναίνεση, πρέπει να εξετάζεται προσεκτικά.

Η ικανότητα αναγνώρισης αυτών των «red flags» βοηθά στην αποφυγή παραπληροφόρησης και στην εστίαση σε αξιόπιστες πηγές.

Αξιολόγηση πληροφοριών που παράγονται από Τεχνητή Νοημοσύνη

Τα εργαλεία Τεχνητής Νοημοσύνης, όπως το ChatGPT ή το Google Gemini, έχουν σχεδιαστεί για να απαντούν σε ερωτήσεις και να παρέχουν πληροφορίες γρήγορα, αλλά δεν επαληθεύουν τα δεδομένα σε πραγματικό χρόνο.

Η ΤΝ μπορεί να παράγει περιεχόμενο που φαίνεται ακριβές, αλλά ενδέχεται να βασίζεται σε παρωχημένα, ελλιπή ή μεροληπτικά δεδομένα.

Περιορισμοί της ΤΝ στην αξιολόγηση πληροφοριών:

- Δεν υπάρχει επαλήθευση σε πραγματικό χρόνο: Η ΤΝ δεν έχει πρόσβαση σε ζωντανά δεδομένα για να διασφαλίσει την επικαιρότητα της πληροφορίας.
- Μεροληψία στα δεδομένα εκπαίδευσης: Η ΤΝ εκπαιδεύεται σε μεγάλα σύνολα δεδομένων, τα οποία μπορεί να περιλαμβάνουν προκαταλήψεις ή ανακρίβειες.
- Έλλειψη πλήρους κατανόησης πλαισίου: Η ΤΝ μπορεί να μην κατανοεί πλήρως σύνθετες ή λεπτές καταστάσεις που απαιτούν ανθρώπινη κρίση.

Βέλτιστες πρακτικές για τη χρήση πληροφοριών από ΤΝ:

- να διασταυρώνετε πάντα τις πληροφορίες με άλλες αξιόπιστες πηγές
- να κατανοείτε ότι η ΤΝ υποστηρίζει αλλά δεν αντικαθιστά την κριτική σκέψη
- να χρησιμοποιείτε την ΤΝ ως εργαλείο υποστήριξης και όχι ως μοναδική πηγή αλήθειας

Η ευθύνη για την ακρίβεια της πληροφορίας ανήκει στον άνθρωπο χρήστη, όχι στο εργαλείο.

Τι κάνετε όταν οι πηγές συγκρούονται;

Μπορεί να βρείτε ότι:

- Η Πηγή Α αναφέρει κάτι
- Η Πηγή Β αναφέρει κάτι διαφορετικό

Σε αυτή την περίπτωση, θα πρέπει να:

- ελέγξετε την αυθεντία της πηγής
- συγκρίνετε πολλαπλές αναφορές
- δώσετε προτεραιότητα σε επίσημα ή επικυρωμένα δεδομένα
- καθυστερήσετε την απόφαση, εάν είναι απαραίτητο

Η επιλογή της πιο εύκολης ή γρήγορης απάντησης δεν αποτελεί σωστή πρακτική.

Η επαγγελματική κρίση δοκιμάζεται όταν η πληροφορία είναι αβέβαιη ή αντικρουόμενη.



Επιπτώσεις κινδύνου από κακή αξιολόγηση πληροφοριών

Επιπτώσεις κινδύνου από κακή αξιολόγηση πληροφοριών:

- Νομικοί κίνδυνοι: Η χρήση παρωχημένων πληροφοριών συμμόρφωσης μπορεί να οδηγήσει σε πρόστιμα ή νομικές κυρώσεις.
- Λειτουργικοί κίνδυνοι: Η λανθασμένη κατανόηση τεχνικής τεκμηρίωσης μπορεί να προκαλέσει βλάβες εξοπλισμού ή καθυστερήσεις στην παραγωγή.
- Οικονομικοί κίνδυνοι: Η κακή ανάλυση της αγοράς μπορεί να οδηγήσει σε λανθασμένες επενδυτικές αποφάσεις ή χαμένες ευκαιρίες.
- Κίνδυνοι φήμης: Η χρήση μεροληπτικών ή λανθασμένων πληροφοριών μπορεί να βλάψει τη φήμη της επιχείρησης και να μειώσει την εμπιστοσύνη των πελατών.

Η αξιολόγηση της ποιότητας και της αξιοπιστίας της πληροφορίας μειώνει τους κινδύνους και διασφαλίζει ότι οι αποφάσεις λαμβάνονται σύμφωνα με επαγγελματικά πρότυπα και κανονισμούς.

Παράδειγμα: Λανθασμένα δεδομένα προμηθευτή → λάθος σύμβαση → οικονομική απώλεια

Επαγγελματική διαδικασία αξιολόγησης πληροφοριών

Μια δομημένη προσέγγιση:

- **Επαληθεύστε τις πληροφορίες:** Διασταυρώστε γεγονότα και δεδομένα με πολλές αξιόπιστες πηγές.
- **Θέστε βασικά ερωτήματα:** Ποιος είναι ο συγγραφέας; Ποια είναι η αυθεντία του; Πότε δημοσιεύθηκε; Γιατί χρησιμοποιείται αυτή η πηγή;
- **Καταγράψτε τα ευρήματά σας:** Διατηρείτε αρχείο των πηγών που χρησιμοποιήθηκαν, ιδιαίτερα όταν λαμβάνετε αποφάσεις βάσει αυτών των πληροφοριών.
- **Χρησιμοποιήστε εργαλεία:** Αξιοποιήστε υπεύθυνα εργαλεία επαλήθευσης γεγονότων, βάσεις δεδομένων και ΤΝ για να ενισχύσετε τη διαδικασία αξιολόγησης πληροφοριών.

Μια επαγγελματική προσέγγιση στην αξιολόγηση πληροφοριών περιλαμβάνει προσεκτική επαλήθευση, κριτική σκέψη και μια δομημένη διαδικασία οργάνωσης και καταγραφής των ευρημάτων. Αυτό προστατεύει τόσο την προσωπική όσο και την οργανωσιακή αξιοπιστία.

Μην παραλείπετε ποτέ την αξιολόγηση λόγω:

- πίεσης χρόνου
- ρουτίνας
- υποθέσεων

Υποενότητα 3 – Οργάνωση & Διαχείριση Πληροφοριών και Δεδομένων



Γιατί η οργάνωση αποτελεί επαγγελματική δεξιότητα

Στα επαγγελματικά περιβάλλοντα, η οργάνωση της πληροφορίας δεν αποτελεί απλώς μια τεχνική λεπτομέρεια, αλλά μια βασική επαγγελματική δεξιότητα που επηρεάζει άμεσα την απόδοση.

Η οργάνωση των δεδομένων είναι απαραίτητη για την αποδοτικότητα, την παραγωγικότητα και την ασφάλεια των πληροφοριών. Στον χώρο εργασίας διασφαλίζει ότι:

- η πληροφορία είναι εύκολα προσβάσιμη γρήγορα και με σιγουριά όταν χρειάζεται
- τα λάθη μειώνονται, καθώς τα δεδομένα είναι σωστά δομημένα και εύκολα επαληθεύσιμα
- η συνεργασία με συναδέλφους γίνεται πιο αποτελεσματική
- οι κίνδυνοι ασφάλειας περιορίζονται, καθώς η σωστή οργάνωση αποτρέπει την τυχαία έκθεση δεδομένων

Λογική δομής φακέλων

Αποτελεσματική δομή φακέλων: Ένας από τους καλύτερους τρόπους οργάνωσης δεδομένων είναι η δημιουργία μιας σαφούς και συνεπούς δομής φακέλων.

Βασικές κατευθυντήριες γραμμές περιλαμβάνουν:

- Κατηγοριοποίηση: Ομαδοποιήστε τα αρχεία ανά έργο, τμήμα ή ημερομηνία, ώστε να εντοπίζονται εύκολα.
- Συνέπεια: Ακολουθείτε πάντα το ίδιο σύστημα ονοματοδοσίας και αρχειοθέτησης για κάθε έργο, ώστε τα αρχεία να είναι εύκολα προσβάσιμα.
- Υποφάκελοι: Διαχωρίστε μεγάλα έργα σε υποφακέλους για συγκεκριμένες εργασίες, διευκολύνοντας την παρακολούθηση των διαφορετικών σταδίων.

Μια επαγγελματική δομή φακέλων πρέπει να αντικατοπτρίζει τη λογική της εργασίας:

- ανά έργο → όταν η εργασία βασίζεται σε projects
- ανά λειτουργία → όταν οι εργασίες είναι επαναλαμβανόμενες (π.χ. οικονομικά, HR)
- ανά στάδιο διαδικασίας → όταν οι ροές εργασίας ακολουθούν φάσεις

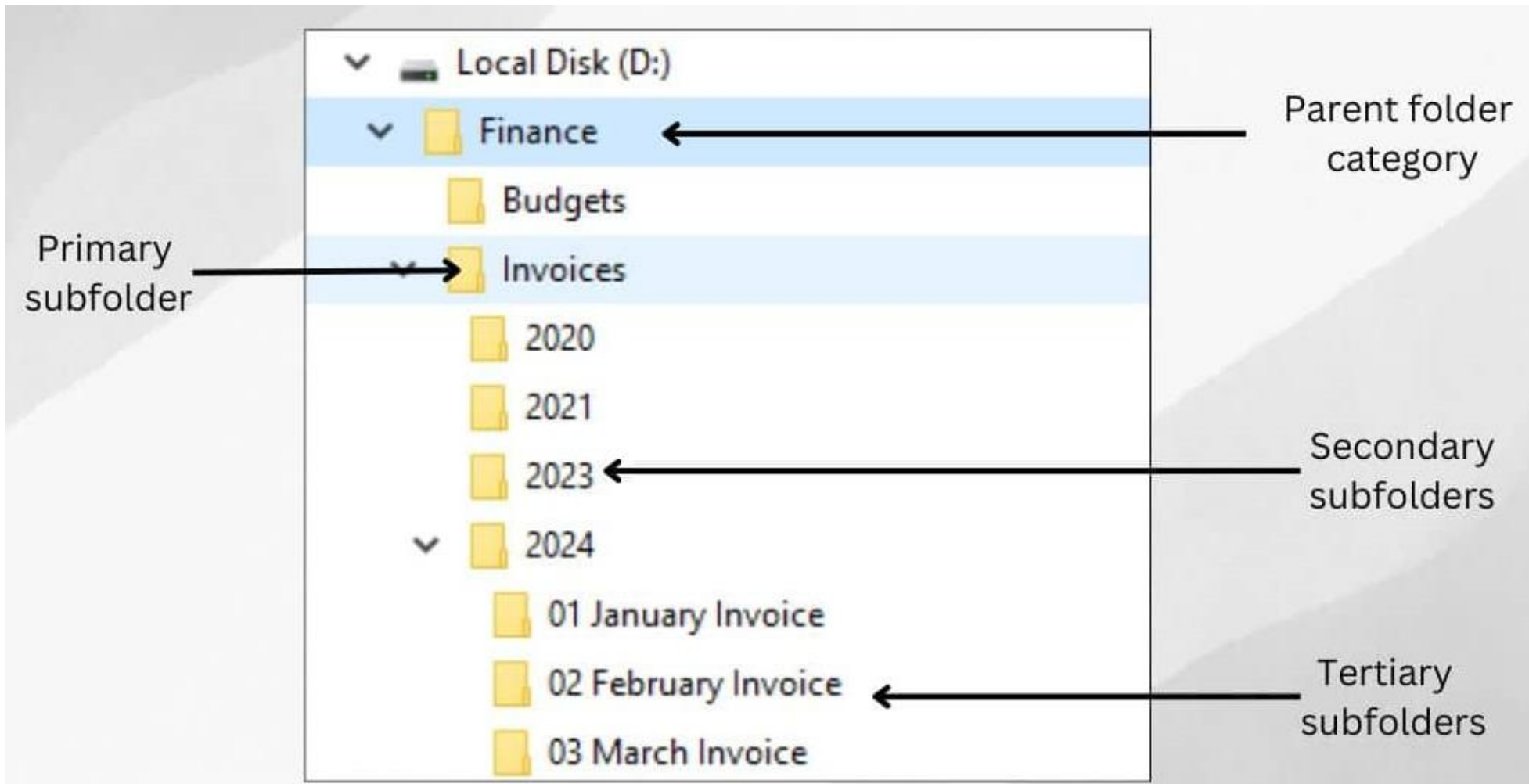
Παράδειγμα δομής: Έργο → Φάση → Τύπος Εγγράφου → Έκδοση

Μια καλά δομημένη οργάνωση φακέλων μειώνει τη σύγχυση, διευκολύνει την ανάκτηση δεδομένων και αποτρέπει την απώλεια σημαντικών αρχείων.

Βέλτιστες πρακτικές:

- Διατηρήστε τη δομή απλή και κατανοητή.
- Χρησιμοποιείτε περιγραφικά ονόματα για φακέλους και αρχεία, ώστε το περιεχόμενό τους να είναι σαφές.
- Αποφεύγετε περιττούς υποφακέλους και πολύπλοκες ιεραρχίες που δυσκολεύουν την πλοήγηση.
- Διασφαλίστε ότι η δομή φακέλων υποστηρίζει τη συνεργασία, με κατάλληλα δικαιώματα και επίπεδα πρόσβασης.

Παράδειγμα ομαδοποίησης φακέλων ανά κατηγορία:



Ονοματοδοσία αρχείων

Οι συνεπείς συμβάσεις ονοματοδοσίας βοηθούν ώστε τα αρχεία να είναι εύκολα στην αναγνώριση και την ανάκτηση.

Βασικές κατευθυντήριες γραμμές περιλαμβάνουν:

- Να είναι περιγραφικά (Be Descriptive): Συμπεριλάβετε βασικές πληροφορίες όπως όνομα έργου, ημερομηνία, έκδοση και τύπο περιεχομένου. Παράδειγμα: ClientXYZ_ProjectReport_2023-10-15_V1
- Να είναι απλά (Keep it Simple): Αποφύγετε πολύ μεγάλα ονόματα και περιττές λεπτομέρειες. Στόχος είναι η άμεση κατανόηση.
- Αποφυγή ειδικών χαρακτήρων (Avoid Special Characters): Χαρακτήρες όπως !, @, # μπορεί να δημιουργήσουν προβλήματα. Χρησιμοποιείτε γράμματα, αριθμούς και παύλες.
- Συνεπής μορφή ημερομηνίας (Use Consistent Date Formats): Χρησιμοποιείτε πάντα την ίδια μορφή, όπως YYYY-MM-DD, ώστε τα αρχεία να ταξινομούνται χρονολογικά.

Γιατί είναι σημαντικές οι συμβάσεις ονοματοδοσίας:

- Σαφήνεια (Clarity): Τα σωστά ονομασμένα αρχεία είναι πιο εύκολα στην κατανόηση και πρόσβαση.
- Συνέπεια (Consistency): Η τυποποίηση αποτρέπει σύγχυση όταν πολλοί χρήστες διαχειρίζονται αρχεία.
- Έλεγχος εκδόσεων (Version Control): Η χρήση αριθμών έκδοσης βοηθά στην παρακολούθηση αλλαγών και στην αποφυγή λαθών.

Τι είναι η διαχείριση εκδόσεων;

Η διαχείριση εκδόσεων αφορά την οργάνωση των αρχείων με τρόπο που επιτρέπει την παρακολούθηση της εξέλιξης ενός εγγράφου με την πάροδο του χρόνου.

Βοηθά να:

- αποφεύγεται η σύγχυση όταν υπάρχουν πολλαπλές εκδόσεις του ίδιου εγγράφου
- διατηρείται αρχείο των αλλαγών που έχουν πραγματοποιηθεί
- εντοπίζεται εύκολα η πιο πρόσφατη έκδοση ενός αρχείου

Βέλτιστες πρακτικές για διαχείριση εκδόσεων:

- Χρήση αριθμών έκδοσης: Να επισημαίνετε πάντα κάθε έκδοση (π.χ. v1, v2, final) ώστε να παρακολουθούνται οι αλλαγές.
- Χρήση cloud συστημάτων: Πλατφόρμες όπως το Google Drive ή το OneDrive προσφέρουν ενσωματωμένο ιστορικό εκδόσεων.
- Περιορισμός εκδόσεων: Αποφεύγετε τη δημιουργία υπερβολικών εκδόσεων χωρίς λόγο. Κάνετε σαφείς και ουσιαστικές ενημερώσεις.
- Παράδειγμα: Μια ομάδα marketing μπορεί να ονομάζει τα αρχεία της ως:
Proposal_ClientXYZ_v1 → Proposal_ClientXYZ_v2 → Proposal_ClientXYZ_final
- Η χρήση διαχείρισης εκδόσεων διασφαλίζει ότι όλοι εργάζονται στην πιο πρόσφατη και σωστή έκδοση, μειώνοντας λάθη και σύγχυση.

Συνηθισμένα λάθη στην οργάνωση δεδομένων

Συνηθισμένα λάθη στην οργάνωση δεδομένων:

- Υπερβολικά πολύπλοκη δομή φακέλων: Η δημιουργία πολλών υποφακέλων ή περιττών κατηγοριών δυσκολεύει την εύρεση αρχείων.
- Ασυνεπής ονοματοδοσία: Η αλλαγή συμβάσεων ονοματοδοσίας ή η χρήση ασαφών ονομάτων δυσκολεύει την κατανόηση του περιεχομένου των αρχείων.
- Αποθήκευση αρχείων σε τυχαίες τοποθεσίες: Η αποθήκευση αρχείων χωρίς συγκεκριμένη δομή οδηγεί σε απώλεια ή δυσκολία εντοπισμού.
- Έλλειψη αντιγράφων ασφαλείας: Η μη δημιουργία backup μπορεί να οδηγήσει σε μόνιμη απώλεια δεδομένων σε περίπτωση τεχνικού προβλήματος.

Πώς να αποφύγετε αυτά τα λάθη:

- διατηρήστε τη δομή φακέλων απλή και κατανοητή
- χρησιμοποιείτε συνεπή σύστημα ονοματοδοσίας σε όλα τα αρχεία
- δημιουργείτε τακτικά αντίγραφα ασφαλείας για αποφυγή απώλειας δεδομένων

Τα συνηθισμένα λάθη στην οργάνωση δεδομένων οδηγούν σε αναποτελεσματικότητα και απογοήτευση.

Τι είναι τα δομημένα δεδομένα (εκτεταμένα);

Τα δομημένα δεδομένα αναφέρονται σε δεδομένα που είναι οργανωμένα σε προκαθορισμένη μορφή, όπως γραμμές, στήλες και πίνακες, γεγονός που επιτρέπει την εύκολη επεξεργασία και ανάλυσή τους.

Χαρακτηριστικά δομημένων δεδομένων:

- Οργανωμένα: Τα δεδομένα είναι διατεταγμένα σε γραμμές και στήλες, διευκολύνοντας την καταχώρηση, την αναζήτηση και την ανάλυση.
- Συνεπή: Κάθε εγγραφή ακολουθεί την ίδια μορφή, όπως ημερομηνίες, αριθμούς ή κείμενο.
- Εύκολα στην επεξεργασία: Λόγω της προβλέψιμης δομής τους, μπορούν να αναλυθούν εύκολα με εργαλεία όπως το Excel ή το Google Sheets.

Παράδειγμα: Μια βάση δεδομένων πελατών με στήλες για όνομα, email, αριθμό τηλεφώνου και ιστορικό αγορών αποτελεί χαρακτηριστικό παράδειγμα δομημένων δεδομένων.

Τα δομημένα δεδομένα είναι ιδανικά για ανάλυση, καθώς η ομοιομορφία τους επιτρέπει την εύκολη ταξινόμηση, αναζήτηση και εξαγωγή συμπερασμάτων.

Τι είναι τα μη δομημένα δεδομένα (εκτεταμένα);

Τα μη δομημένα δεδομένα αναφέρονται σε πληροφορίες που δεν ακολουθούν προκαθορισμένη μορφή και είναι δύσκολο να οργανωθούν και να αναλυθούν συστηματικά.

Παραδείγματα περιλαμβάνουν emails, αρχεία PDF, μηνύματα συνομιλίας και σημειώσεις.

Στην πράξη, το μεγαλύτερο μέρος της πληροφορίας αρχικά υπάρχει ως μη δομημένα δεδομένα.

Ωστόσο, παρουσιάζουν ορισμένες προκλήσεις:

- είναι δύσκολα στην αναζήτηση
- είναι δύσκολη η σύγκριση μεταξύ τους
- μπορούν εύκολα να χαθούν ή να παραλειφθούν

Παράδειγμα: Αιτήματα πελατών σε emails σε σύγκριση με ένα δομημένο σύστημα CRM.

Μετατρέψτε σημαντικά μη δομημένα δεδομένα σε δομημένη μορφή, ώστε να μπορούν να αξιοποιηθούν αποτελεσματικά.

Τα μη δομημένα δεδομένα είναι χρήσιμα για επικοινωνία, αλλά ενέχουν κινδύνους όταν χρησιμοποιούνται για λήψη αποφάσεων χωρίς κατάλληλη οργάνωση και επεξεργασία.

Από τα μη δομημένα στα δομημένα δεδομένα

Στον επαγγελματικό χώρο, η εργασία με πληροφορία απαιτεί τη μετατροπή της σε αξιοποιήσιμη μορφή:

Είσοδος → Επεξεργασία → Χρήση

Παράδειγμα: Emails / σημειώσεις → Υπολογιστικό φύλλο / σύστημα → Απόφαση

Παράδειγμα ροής εργασίας: Παραγγελίες πελατών (emails) → καταχώρηση σε spreadsheet → ανάλυση για εντοπισμό τάσεων

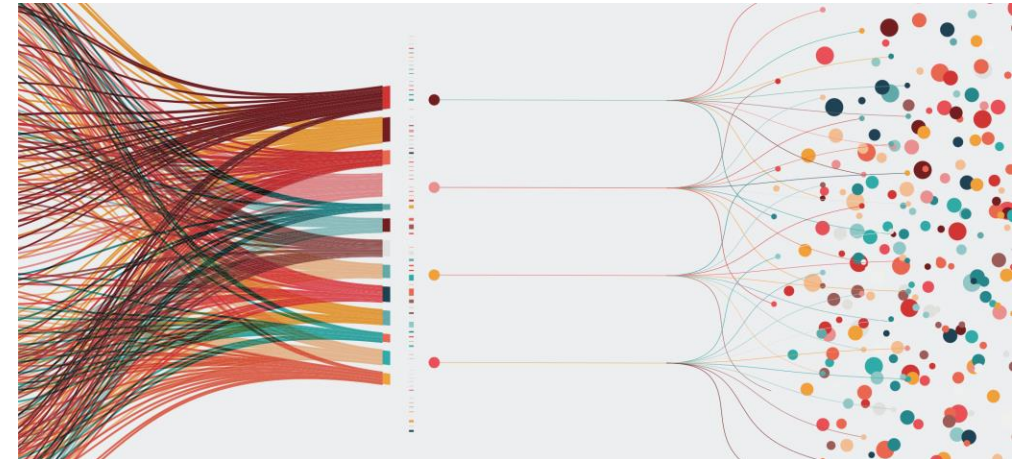
Γιατί είναι σημαντικό αυτό το βήμα:

- μειώνει την ασάφεια
- βελτιώνει την ιχνηλασιμότητα
- υποστηρίζει την αυτοματοποίηση

Η παράλειψη της δομής οδηγεί σε:

- ασυνεπείς αποφάσεις
- απώλεια πληροφοριών

Η μετάβαση από τα μη δομημένα στα δομημένα δεδομένα είναι το σημείο όπου ξεκινά ο επαγγελματικός έλεγχος της πληροφορίας.



Υπολογιστικά φύλλα ως εργαλεία δομημένων δεδομένων

Τα υπολογιστικά φύλλα, όπως το Excel και το Google Sheets, αποτελούν βασικά εργαλεία για τη διαχείριση δομημένων δεδομένων. Χρησιμοποιούνται για την οργάνωση δομημένων δεδομένων, την ανάλυση προτύπων και τάσεων και την υποστήριξη λειτουργικών και οικονομικών αποφάσεων.

Βασικές λειτουργίες περιλαμβάνουν:

- καταχώρηση δεδομένων
- ταξινόμηση και φιλτράρισμα
- τύπους και υπολογισμούς
- οπτικοποίηση δεδομένων

Εφαρμογές στον χώρο εργασίας:

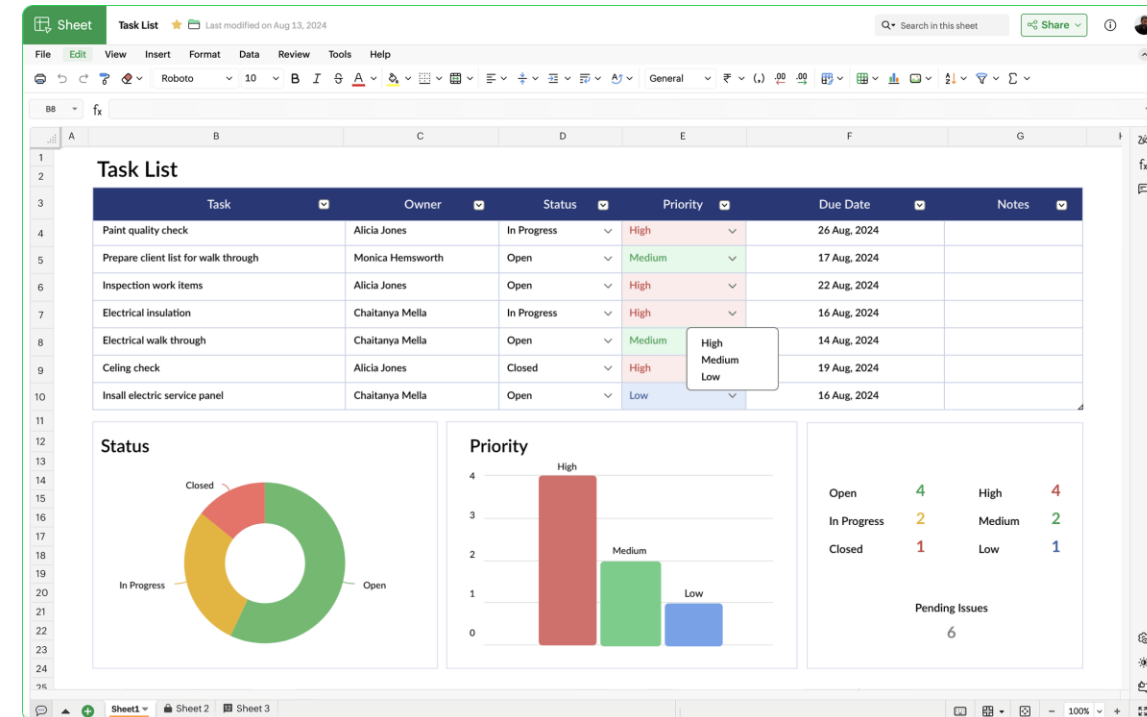
- παρακολούθηση πωλήσεων
- διαχείριση αποθεμάτων
- κατάρτιση προϋπολογισμών
- αναφορές και reporting

Η χρήση υπολογιστικών φύλλων χωρίς σωστή δομή μπορεί να οδηγήσει σε:

- ασυνεπή δεδομένα
- μη αξιόπιστα αποτελέσματα

Τα υπολογιστικά φύλλα δεν είναι απλώς εργαλεία αποθήκευσης, αλλά συστήματα υποστήριξης αποφάσεων.

Στον επίσημο οδηγό εκπαίδευσης Microsoft Excel μπορείτε να βρείτε αξιόπιστα tutorials για τη σωστή δομή, ανάλυση και διαχείριση δεδομένων. [Microsoft Excel Training \(Official Guide\)](#)



Σχεδιασμός υπολογιστικού φύλλου σωστά

Βασικές αρχές σχεδιασμού:

- Μία στήλη = ένας τύπος δεδομένων (π.χ. Ημερομηνία, Ποσό, Όνομα Πελάτη – ποτέ συνδυασμένα)
- Συνεπής μορφή ανά στήλη (π.χ. όλες οι ημερομηνίες στην ίδια μορφή, όλες οι τιμές αριθμητικές)
- Χωρίς κενά ή μικτά πεδία (αποφύγετε κενά, συγχωνευμένα κελιά ή συνδυασμένα δεδομένα)
- Χρήση σαφών επικεφαλίδων (κάθε στήλη πρέπει να περιγράφει ακριβώς το περιεχόμενό της)
- Παράδειγμα:

✗ Λάθος: “12/03 – John – 250€” σε μία στήλη
✓ Σωστό: Ημερομηνία | Όνομα | Ποσό (ξεχωριστές στήλες)

Μια σωστή δομή:

- επιτρέπει ταξινόμηση και φιλτράρισμα
- υποστηρίζει τύπους και αυτοματοποίηση
- μειώνει τα λάθη ερμηνείας

Τα περισσότερα προβλήματα στα υπολογιστικά φύλλα δεν ξεκινούν από τους τύπους, αλλά από τον λάθος σχεδιασμό της δομής.

Σωστή πρακτική

- σχεδιάστε τη δομή πριν από την καταχώρηση δεδομένων
- διατηρήστε τις μορφές απλές και τυποποιημένες
- ελέγξτε τη διάταξη πριν από τη χρήση

Κίνδυνοι

Ο κακός σχεδιασμός οδηγεί σε:

- λάθη στους υπολογισμούς
- ασυνεπή ανάλυση
- αδυναμία επαναχρησιμοποίησης των δεδομένων

Ποιότητα και Συνέπεια δεδομένων

Η υψηλή ποιότητα δεδομένων είναι απαραίτητη για αξιόπιστη ανάλυση και λήψη αποφάσεων. Ακόμη και καλά δομημένα δεδομένα γίνονται αναποτελεσματικά αν δεν διατηρείται η ποιότητά τους.

Βασικές διαστάσεις ποιότητας δεδομένων:

- Ακρίβεια (Accuracy) → οι τιμές είναι σωστές και επαληθευμένες
- Πληρότητα (Completeness) → δεν υπάρχουν ελλείποντα ή μερικά δεδομένα
- Συνέπεια (Consistency) → ίδια μορφή σε όλες τις εγγραφές
- Αξιοπιστία (Reliability) → τα δεδομένα μπορούν να χρησιμοποιηθούν με εμπιστοσύνη για αποφάσεις

Συνήθη προβλήματα στην πράξη:

- μικτές μορφές ημερομηνίας (π.χ. HH/MM vs MM/HH)
- ασυνεπή νομίσματα (€ vs \$ vs κείμενο)
- ελλιπή δεδομένα ή κενές γραμμές
- διπλότυπες ή αντικρουόμενες εγγραφές

Η κακή ποιότητα δεδομένων οδηγεί σε:

- λανθασμένους υπολογισμούς
- παραπλανητικές αναφορές
- κακές ή επικίνδυνες αποφάσεις

Η ποιότητα δεδομένων δεν είναι απλώς τεχνικό ζήτημα. Είναι ζήτημα αξιοπιστίας των αποφάσεων.

Σωστή πρακτική

- τυποποιήστε τις μορφές πριν από τη χρήση
- εφαρμόστε κανόνες επικύρωσης (π.χ. μόνο αριθμητικά πεδία)
- ελέγχετε και καθαρίζετε τα δεδομένα τακτικά
- εντοπίζετε διπλότυπα και ασυνέπειες

Ανθρώπινος παράγοντας στη διαχείριση δεδομένων

Οι περισσότερες προβλήματα που σχετίζονται με τα δεδομένα δεν οφείλονται στα εργαλεία, αλλά στην ανθρώπινη συμπεριφορά και στα πρότυπα λήψης αποφάσεων.

Συνηθισμένες συμπεριφορές:

- βιαστική καταχώρηση δεδομένων
- παράλειψη δομής ή ελέγχων εγκυρότητας
- εξάρτηση από τη μνήμη αντί για συστήματα
- ασυνεπείς τρόποι εργασίας

Υποκείμενες αιτίες:

- πίεση χρόνου
- ρουτίνα («έτσι το κάνουμε πάντα»)
- γνωστική υπερφόρτωση
- έλλειψη ενημέρωσης ή εκπαίδευσης

Επιπτώσεις στον χώρο εργασίας:

- επαναλαμβανόμενα λάθη
- ασυνεπή σύνολα δεδομένων
- μειωμένη εμπιστοσύνη στην πληροφορία
- αυξημένη ανάγκη για διορθώσεις

Η τεχνολογία δεν εξαλείφει τον κίνδυνο — μεταφέρει την ευθύνη στην ανθρώπινη κρίση και συμπεριφορά.

Σωστή πρακτική

- ακολουθείτε σαφείς και συνεπείς διαδικασίες
- εφαρμόζετε τυποποιημένους κανόνες σε όλες τις εργασίες
- επαληθεύετε τα δεδομένα πριν τα χρησιμοποιήσετε
- αναπτύσσετε συνήθειες ελέγχου και επανεξέτασης

Σύνθεση: Από τα δεδομένα σε αξιόπιστες αποφάσεις

Η αποτελεσματική διαχείριση δεδομένων είναι μια δομημένη διαδικασία που συνδέει τη διαχείριση πληροφορίας με τη λήψη επαγγελματικών αποφάσεων.

Ολοκληρωμένη διαδικασία:

1. σωστή δόμηση των δεδομένων
2. διασφάλιση ποιότητας και συνέπειας
3. εντοπισμός και πρόληψη λαθών
4. εφαρμογή πειθαρχημένων πρακτικών εργασίας
5. γρήγορη και αξιόπιστη ανάκτηση πληροφορίας

Λειτουργική ροή:

Δεδομένα → Δομή → Ποιότητα → Ανάλυση → Απόφαση → Δράση

Υποενότητα 4 – Χώρος Cloud & Διαχείριση Δεδομένων



Κατανόηση του χώρου Cloud στον χώρο εργασίας

Ο χώρος cloud αναφέρεται στην αποθήκευση δεδομένων σε ένα διαδικτυακό περιβάλλον, αντί για φυσικό εξοπλισμό όπως οι τοπικοί σκληροί δίσκοι.

Πλατφόρμες όπως το Google Drive, το OneDrive και το Dropbox επιτρέπουν στους χρήστες να αποθηκεύουν, να έχουν πρόσβαση και να μοιράζονται αρχεία εξ αποστάσεως. Με απλά λόγια, το cloud storage σημαίνει αποθήκευση και διαχείριση δεδομένων σε απομακρυσμένους διακομιστές μέσω του διαδικτύου, αντί για τοπικές συσκευές.

Οφέλη του cloud storage:

- **Προσβασιμότητα:** Τα αρχεία είναι διαθέσιμα από οποιαδήποτε συσκευή με σύνδεση στο διαδίκτυο, προσφέροντας ευελιξία για εργασία εξ αποστάσεως και μετακινήσεις.
- **Συνεργασία:** Πολλοί χρήστες μπορούν να έχουν πρόσβαση, να επεξεργάζονται και να συνεργάζονται σε έγγραφα σε πραγματικό χρόνο. Αυτό είναι ιδιαίτερα σημαντικό για ομαδική εργασία, ειδικά σε ΜΜΕ.
- **Επεκτασιμότητα (Scalability):** Οι επιχειρήσεις μπορούν να προσαρμόζουν τον αποθηκευτικό τους χώρο ανάλογα με τις ανάγκες τους, χωρίς να επενδύουν σε επιπλέον φυσικό εξοπλισμό.

Παράδειγμα: Μια ομάδα έργου που εργάζεται σε ένα κοινό έγγραφο στο Google Drive μπορεί να κάνει ενημερώσεις σε πραγματικό χρόνο, διασφαλίζοντας ότι όλοι έχουν πάντα την πιο πρόσφατη έκδοση, χωρίς ανταλλαγή αρχείων μέσω email.

Πώς το Cloud Storage αλλάζει τον τρόπο που εργαζόμαστε

Παραδοσιακή προσέγγιση (Local Storage)

- τα αρχεία αποθηκεύονται σε προσωπικούς υπολογιστές
- περιορισμένη πρόσβαση
- χειροκίνητη κοινοποίηση (email, USB)
- πολλαπλές εκδόσεις του ίδιου αρχείου

Cloud-Based προσέγγιση

- κοινή πρόσβαση σε πραγματικό χρόνο
- μία ενιαία “πηγή αλήθειας”
- συνεχείς ενημερώσεις
- ενσωματωμένη συνεργασία

Παράδειγμα στον χώρο εργασίας:

- *Πριν: Αρχείο_v1 → Αρχείο_v2 → Αρχείο_v3 → Αρχείο_Τελικό*
- *Τώρα: Ένα κοινό έγγραφο → συνεχώς ενημερωμένο*

Το cloud μετατρέπει την εργασία από ατομικές, απομονωμένες ενέργειες σε συνεργατικές και διασυνδεδεμένες διαδικασίες.

Βασικές λειτουργίες, συνεργασία & έλεγχος στη διαχείριση δεδομένων στο Cloud

Τα συστήματα cloud δεν αποτελούν παθητικούς χώρους αποθήκευσης — διαμορφώνουν ενεργά τον τρόπο με τον οποίο εκτελείται η εργασία, η συνεργασία και η λήψη αποφάσεων. Βασικές λειτουργίες (τι επιτρέπουν τα cloud συστήματα):

- Αποθήκευση & Οργάνωση: Δομημένοι φάκελοι, συνεπής ονοματοδοσία και κατηγοριοποίηση
- Πρόσβαση & Δικαιώματα: Έλεγχος του ποιος μπορεί να δει, να επεξεργαστεί ή να μοιραστεί πληροφορίες
- Διαχείριση εκδόσεων: Παρακολούθηση, έλεγχος και επαναφορά αλλαγών με την πάροδο του χρόνου
- Αναζήτηση & Ανάκτηση: Γρήγορη και αξιόπιστη πρόσβαση στα αρχεία όταν χρειάζονται

Συνεργασία στην πράξη:

- πολλοί χρήστες εργάζονται στο ίδιο αρχείο
- ενημερώσεις σε πραγματικό χρόνο και κοινή ορατότητα
- συνεχής παρακολούθηση μέσω ιστορικού εκδόσεων

Σημαντική αρχή:

Η αποδοτικότητα στο cloud εξαρτάται από το πόσο σωστά διαχειρίζεται — όχι απλώς από το ότι χρησιμοποιείται.

Σε περιβάλλον cloud:

Συνεργασία + Έλεγχος = Αξιόπιστα αποτελέσματα

Σωστή πρακτική

- ορίστε σαφείς ρόλους (owner / editor / viewer)
- ελέγχετε και διαχειρίζετε πάντα τα δικαιώματα πρόσβασης
- χρησιμοποιείτε ενεργά το ιστορικό εκδόσεων
- αποφεύγετε την ανεξέλεγκτη ταυτόχρονη επεξεργασία
- διατηρείτε σαφή δομή και συνεπείς συμβάσεις ονοματοδοσίας

Κίνδυνοι στο cloud storage και στην κοινοποίηση δεδομένων

Τα περιβάλλοντα cloud εισάγουν συγκεκριμένους κινδύνους που σχετίζονται με την πρόσβαση, την κοινοποίηση και τον έλεγχο των δεδομένων.

Συνηθισμένοι κίνδυνοι

- μη ελεγχόμενα δικαιώματα πρόσβασης
- τυχαία κοινοποίηση σε λάθος χρήστες
- έκθεση δεδομένων μέσω δημόσιων συνδέσμων
- απώλεια ελέγχου των εκδόσεων αρχείων
- έκθεση δεδομένων
- εξωτερική πρόσβαση

Τα περισσότερα προβλήματα προκύπτουν από:

- παρερμηνεία των δικαιωμάτων πρόσβασης
- βιαστικές ενέργειες κοινοποίησης
- έλλειψη ελέγχου και επαλήθευσης

Σε περιβάλλον cloud: Πρόσβαση = Έλεγχος = Ευθύνη

Σωστή πρακτική

- ελέγχετε πάντα τις ρυθμίσεις πρόσβασης
- αποφεύγετε το “anyone with link” εκτός αν είναι απαραίτητο
- ελέγχετε την κοινοποίηση πριν την αποστολή
- ελέγχετε τακτικά τα κοινόχρηστα αρχεία

Βέλτιστες πρακτικές για τη διαχείριση δεδομένων στο cloud

Για να εργαστείτε αποτελεσματικά με συστήματα cloud, οι επαγγελματίες πρέπει να ακολουθούν δομημένες πρακτικές:

- καθορίζουν ρόλους και ευθύνες
- επικοινωνούν τις αλλαγές με σαφήνεια
- χρησιμοποιούν υπεύθυνα τα κοινόχρηστα έγγραφα

Πειθαρχία στη ροή εργασίας

- επαληθεύουν πριν από την κοινοποίηση
- ενημερώνουν τα αρχεία με συνέπεια
- διατηρούν σαφήνεια στις εκδόσεις

Η αποδοτικότητα στο cloud εξαρτάται από την πειθαρχία, τη συνέπεια και την υπευθυνότητα.

Βασικές πρακτικές

- οργανώστε τους φακέλους με σαφήνεια και συνέπεια
- χρησιμοποιείτε τυποποιημένες συμβάσεις ονοματοδοσίας
- διαχειρίζεστε προσεκτικά τα δικαιώματα πρόσβασης
- αποφεύγετε τον διπλασιασμό αρχείων
- ελέγχετε και καθαρίζετε τακτικά τον αποθηκευτικό χώρο

Υποένότητα 5 – Προχωρημένη εφαρμογή μέσω σεναρίων (Case-Based Application)



Co-funded by
the European Union

Σενάριο περίπτωσης 1: Διαχείριση δεδομένων προμηθευτών για λήψη αποφάσεων

Εργάζεστε ως υπάλληλος γραφείου σε μια μικρή εμπορική εταιρεία.

Οι ευθύνες σας είναι:

- διατήρηση αρχείων προμηθευτών
- ενημέρωση δεδομένων τιμών σε υπολογιστικά φύλλα
- αποθήκευση εγγράφων στο cloud σύστημα της εταιρείας

Ο προϊστάμενός σας σας ζητά να:

- ενημερώσετε τις τιμές προμηθευτών
- ετοιμάσετε μια συγκριτική αναφορά
- ανεβάσετε και να τη μοιραστείτε στο cloud

Εργάζεστε με:

- πολλαπλές εκδόσεις spreadsheets
- emails με ενημερωμένες τιμές
- αρχεία αποθηκευμένα σε διαφορετικούς φακέλους
- ασαφείς συμβάσεις ονοματοδοσίας

Πρέπει να ολοκληρώσετε την εργασία γρήγορα, καθώς μια απόφαση αγορών εξαρτάται από την αναφορά σας. Σε πραγματικές συνθήκες εργασίας, τα δεδομένα είναι συχνά ελλιπή, διάσπαρτα και χρονικά πιεστικά.

Ποια είναι η πρώτη σας προτεραιότητα πριν ξεκινήσετε;

Ανάλυση σεναρίου 1: Διαχείριση δεδομένων προμηθευτών

Για να διαχειριστείτε αυτή την κατάσταση επαγγελματικά, πρέπει να ακολουθήσετε μια δομημένη προσέγγιση:

Βήμα 1 – Διευκρίνιση στόχου

- Τι απαιτείται; → Σύγκριση προμηθευτών για τη λήψη απόφασης
- Τι είναι κρίσιμο; → Ακρίβεια και ενημερωμένες τιμές

Βήμα 2 – Επικύρωση πηγών πληροφορίας

- συγκρίνετε τα δεδομένα των spreadsheets με τις ενημερώσεις από τα emails
- εντοπίστε παρωχημένες ή ασυνεπείς πληροφορίες
- δώστε προτεραιότητα στις πιο πρόσφατες και αξιόπιστες πηγές

Βήμα 3 – Δομή δεδομένων

- δημιουργήστε ένα καθαρό και οργανωμένο υπολογιστικό φύλλο
- ορίστε σαφείς στήλες (προμηθευτής, τιμή, ημερομηνία, όροι)
- διασφαλίστε συνέπεια στη μορφοποίηση

Βήμα 4 – Διασφάλιση ποιότητας δεδομένων

- ελέγξτε για ελλειπείς ή λανθασμένες τιμές
- επαληθεύστε τους υπολογισμούς
- αποφύγετε τα διπλότυπα

Βήμα 5 – Σωστή αποθήκευση και κοινοποίηση

- αποθηκεύστε στο σωστό φάκελο στο cloud
- χρησιμοποιήστε σωστή σύμβαση ονοματοδοσίας
- ελέγξτε τα δικαιώματα πρόσβασης πριν την κοινοποίηση

Ένας επαγγελματίας δεν εργάζεται με τα πρώτα διαθέσιμα δεδομένα, αλλά τα επικυρώνει, τα δομεί και τα επαληθεύει πριν προχωρήσει σε ενέργεια.

Οι αξιόπιστες αποφάσεις βασίζονται σε ελεγχόμενα δεδομένα και όχι σε γρήγορες υποθέσεις.

Σενάριο περίπτωσης 2: Διαχείριση δεδομένων πελατών σε υπολογιστικό φύλλο

Εργάζεστε ως γραμματέας σε μια εταιρεία παροχής υπηρεσιών.

Οι ευθύνες σας είναι:

- ενημέρωση αρχείων πελατών
- διατήρηση ενός υπολογιστικού φύλλου με συναλλαγές
- προετοιμασία βασικών αναφορών απόδοσης

Σας ζητείται να:

- ενημερώσετε τα δεδομένα συναλλαγών πελατών
- υπολογίσετε τα μηνιαία σύνολα
- στείλετε μια συνοπτική αναφορά στον προϊστάμενό σας

Παρατηρείτε:

- ελλιπείς τιμές σε ορισμένες γραμμές
- ασυνεπείς μορφές ημερομηνιών
- διπλότυπες εγγραφές
- ασαφείς τύπους που έχουν ήδη χρησιμοποιηθεί στο υπολογιστικό φύλλο

Η αναφορά θα χρησιμοποιηθεί για οικονομικό προγραμματισμό, επομένως η ακρίβεια είναι κρίσιμη.

Οποιοδήποτε λάθος μπορεί να οδηγήσει σε:

- λανθασμένες οικονομικές αποφάσεις
- απώλεια εμπιστοσύνης

Τα υπολογιστικά φύλλα συχνά θεωρούνται αξιόπιστα ακόμη και όταν περιέχουν κρυφά λάθη.

Ποια είναι η πιο κρίσιμη ενέργεια πριν χρησιμοποιήσετε τα δεδομένα;

Ανάλυση σεναρίου 2: Διαχείριση δεδομένων πελατών

Αυτή η κατάσταση απαιτεί προσεκτική διαχείριση της ποιότητας των δεδομένων και της ακεραιότητας του υπολογιστικού φύλλου.

Βήμα 1 – Εντοπισμός προβλημάτων δεδομένων

- εντοπίστε ελλιπείς τιμές
- ελέγξτε ασυνεπείς μορφές
- εντοπίστε διπλότυπα

Βήμα 2 – Καθαρισμός δεδομένων

- τυποποιήστε τις μορφές (ημερομηνίες, νομίσματα)
- αφαιρέστε τα διπλότυπα
- συμπληρώστε ή επισημάνετε τα ελλιπή δεδομένα

Βήμα 3 – Έλεγχος δομής υπολογιστικού φύλλου

- επιβεβαιώστε ότι οι στήλες είναι σωστά ορισμένες
- διασφαλίστε έναν τύπο δεδομένων ανά στήλη
- αποφύγετε μικτά ή ασαφή πεδία

Βήμα 4 – Επικύρωση υπολογισμών

- ελέγξτε τους τύπους και τα εύρη υπολογισμού
- δοκιμάστε τα αποτελέσματα με δείγμα δεδομένων

Βήμα 5 – Προετοιμασία αξιόπιστου αποτελέσματος

- διασφαλίστε ότι η τελική αναφορά βασίζεται σε σωστά δεδομένα
- ελέγξτε την πριν την κοινοποίηση

Ποτέ μην εμπιστεύεστε ένα υπολογιστικό φύλλο χωρίς να ελέγξετε τη δομή, την ποιότητα και τους τύπους του.

Τα υπολογιστικά φύλλα δημιουργούν την ψευδαίσθηση ακρίβειας, αλλά η αξιοπιστία εξαρτάται από τον έλεγχο της ποιότητας των δεδομένων.

Σενάριο περίπτωσης 3: Εργασία με κοινόχρηστα αρχεία στο cloud

Εργάζεστε ως team assistant σε μια μικρή εταιρεία που λειτουργεί με βάση έργα (project-based).

- Οι ευθύνες σας είναι:
- υποστήριξη στην προετοιμασία εγγράφων
- συνεργασία με τα μέλη της ομάδας
- διαχείριση αρχείων σε κοινόχρηστο φάκελο στο cloud

Η ομάδα σας ετοιμάζει μια αναφορά έργου.

Πρέπει να:

- ελέγξετε το έγγραφο
- κάνετε ενημερώσεις
- το κοινοποιήσετε στον project manager

Βρίσκετε:

- πολλαπλές εκδόσεις του ίδιου αρχείου
- ασαφή ονόματα αρχείων (Final_v2, Final_NEW, Final_Updated)
- μέλη της ομάδας να επεξεργάζονται διαφορετικές εκδόσεις

Δεν είστε σίγουροι:

- ποια είναι η σωστή έκδοση
- ποιος έκανε τις τελευταίες αλλαγές
- ποιο αρχείο πρέπει να αποσταλεί

Η αναφορά πρέπει να παραδοθεί μέσα στην επόμενη ώρα.

Τα εργαλεία cloud απλοποιούν τη συνεργασία — αλλά χωρίς έλεγχο δημιουργούν σύγχυση.

Ποιο είναι το πρώτο σας βήμα πριν επεξεργαστείτε ή κοινοποιήσετε το αρχείο;

Ανάλυση σεναρίου 3: Συνεργασία στο cloud και διαχείριση εκδόσεων

Αυτή η κατάσταση αναδεικνύει τη σημασία του ελέγχου στα περιβάλλοντα cloud.

Βήμα 1 – Εντοπισμός της σωστής έκδοσης

- ελέγξτε το ιστορικό εκδόσεων
- εντοπίστε την πιο πρόσφατη ενημέρωση
- επιβεβαιώστε με την ομάδα αν χρειάζεται

Βήμα 2 – Καθιέρωση ελέγχου

- εντοπίστε τον υπεύθυνο του αρχείου
- διασφαλίστε ότι μόνο εξουσιοδοτημένοι χρήστες πραγματοποιούν αλλαγές

Βήμα 3 – Αποφυγή διπλότυπων

- σταματήστε την εργασία σε πολλαπλά αρχεία
- συγκεντρώστε τα σε μία κοινή έκδοση

Βήμα 4 – Εφαρμογή σαφούς ονοματοδοσίας

- μετονομάστε το αρχείο με συνεπή τρόπο
- αφαιρέστε τα συγκεχυμένα διπλότυπα

Βήμα 5 – Επαλήθευση πριν την κοινοποίηση

- επιβεβαιώστε τη σωστή έκδοση
- ελέγξτε τα δικαιώματα πρόσβασης
- διασφαλίστε την τελική ακρίβεια

Στα συστήματα cloud, η σαφήνεια και ο έλεγχος είναι πιο σημαντικά από την ταχύτητα. Η συνεργασία απαιτεί δομή, υπευθυνότητα και πειθαρχία.

Σενάριο περίπτωσης 4: Αναζήτηση και αξιολόγηση πληροφορίας για μια εργασία

Εργάζεστε ως υπάλληλος γραφείου σε μια μικρή εταιρεία.

Οι ευθύνες σας είναι:

- αναζήτηση εξωτερικής πληροφορίας
- υποστήριξη λειτουργικών αποφάσεων
- συλλογή και σύνοψη δεδομένων

Σας ζητείται να:

- βρείτε πληροφορίες για έναν νέο προμηθευτή
- ελέγξετε απαιτήσεις συμμόρφωσης
- παρέχετε μια σύσταση (recommendation)

Βρίσκετε:

- διαφορετικές πληροφορίες σε ιστοσελίδες
- ένα blog με χρήσιμες λεπτομέρειες
- ένα κείμενο που δημιουργήθηκε από ΤΝ
- μια επίσημη πηγή με πιο σύνθετο περιεχόμενο

Δυσκολία:

- οι πληροφορίες είναι ασυνεπείς
- ορισμένες πηγές είναι πιο εύκολες στην κατανόηση
- άλλες είναι πιο αξιόπιστες αλλά πιο σύνθετες

Ο προϊστάμενός σας αναμένει μια γρήγορη και σαφή απάντηση.

Η επιλογή λάθος πηγής μπορεί να οδηγήσει σε:

- λανθασμένες αποφάσεις
- προβλήματα συμμόρφωσης

Ποια πηγή θα εμπιστευτείτε πρώτα και γιατί;

Ανάλυση σεναρίου 4: Αξιολόγηση πηγών πληροφορίας

Αυτή η κατάσταση απαιτεί κριτική αξιολόγηση και επαγγελματική κρίση.

Βήμα 1 – Αναγνώριση τύπων πηγών

- επίσημη πηγή → υψηλή αξιοπιστία
- blog / AI → χαμηλότερη αξιοπιστία
- μικτές πηγές → απαιτούν επικύρωση

Βήμα 2 – Αξιολόγηση πληροφορίας

- ελέγξτε την ακρίβεια
- επαληθεύστε τον συγγραφέα και την προέλευση
- επιβεβαιώστε την ημερομηνία ενημέρωσης

Βήμα 3 – Σύγκριση πηγών

- εντοπίστε τις διαφορές
- δώστε προτεραιότητα σε αξιόπιστες και έγκυρες πηγές
- διασταυρώστε τα βασικά στοιχεία

Βήμα 4 – Αποφυγή συνηθισμένων λαθών

- μην επιλέγετε την πιο εύκολη πηγή
- μην βασίζεστε σε μία μόνο πηγή
- μην εμπιστεύεστε μη επαληθευμένο περιεχόμενο από AI

Βήμα 5 – Διαμόρφωση τεκμηριωμένης σύστασης

- βασίστε την απόφαση σε επαληθευμένες πληροφορίες
- εξηγήστε το σκεπτικό σας

Ένας επαγγελματίας δεν επιλέγει πληροφορίες με βάση την ευκολία, αλλά με βάση την αξιοπιστία και τη συνάφεια.

Η κριτική σκέψη είναι η ικανότητα να αμφισβητείς, να συγκρίνεις και να τεκμηριώνεις τις αποφάσεις σου.

- European Commission (2022) *Digital Economy and Society Index (DESI) 2022: Human Capital*. Διαθέσιμο στο:
<https://digital-strategy.ec.europa.eu/en/policies/desi>
- University of North Carolina (UNC) (2023) *Evaluating Information Sources*. Διαθέσιμο στο:
<https://guides.lib.unc.edu/evaluating-info/evaluate>
- IBM (2023) *Data Management: Risks of Poor Information Handling*. Διαθέσιμο στο:
<https://www.ibm.com/topics/data-management>
- Microsoft (2024) *Excel Training: Structuring and Managing Data Effectively*. Διαθέσιμο στο:
<https://support.microsoft.com/en-us/excel>

Ψηφιακά εργαλεία και Τεχνητή Νοημοσύνη για καθημερινές επαγγελματικές εργασίες

Ενότητα 3

Αναγνώριση ψηφιακών αναγκών: Ξεκινώντας από την εργασία

Η αποτελεσματική χρήση εργαλείων ξεκινά από την ανάλυση της εργασίας και όχι από την επιλογή του εργαλείου.

Βασικοί παράγοντες που πρέπει να εξετάσετε:

- **Συχνότητα:** Πόσο συχνά εκτελείται αυτή η εργασία;
- **Συνεργασία:** Περιλαμβάνει περισσότερα από ένα άτομα;
- **Πολυπλοκότητα:** Απαιτεί επεξεργασία μεγάλου όγκου δεδομένων ή απλό κείμενο;
- **Αποτέλεσμα:** Ποια είναι η τελική μορφή του παραδοτέου;

Η χρήση ενός «ισχυρού εργαλείου» (όπως ένα σύνθετο CRM) για μια απλή εργασία (όπως μια λίστα επαφών) αυξάνει την προσπάθεια και μειώνει την αποδοτικότητα.

Σωστό εργαλείο + σωστή εργασία = Αποδοτικότητα

Λάθος εργαλείο + λάθος εργασία = Επιπλέον φόρτος & χαμένος χρόνος

Κατηγορίες ψηφιακής εργασίας

Οι εργασιακές δραστηριότητες μπορούν να κατηγοριοποιηθούν σε τέσσερις βασικές λειτουργικές κατηγορίες:

1. Παραγωγή: Δημιουργία και σύνθεση περιεχομένου

- Ο βασικός «μηχανισμός» όπου οι ιδέες μετατρέπονται σε απτά αποτελέσματα.
- Επεξεργασία κειμένου: Σύνταξη εκτενών εγγράφων, αναφορών και προτάσεων (π.χ. Microsoft Word, Google Docs).
- Οπτική παρουσίαση: Δημιουργία παρουσιάσεων υψηλού αντίκτυπου για ενδιαφερόμενα μέρη (π.χ. PowerPoint, Canva).
- Δημιουργικός σχεδιασμός: Παραγωγή επαγγελματικού επιπέδου γραφικών, πρωτοτύπων και στοιχείων branding (π.χ. Adobe Creative Cloud, Figma).

2. Επικοινωνία: Ροή πληροφορίας και συνδεσιμότητα

- Ο «συνδεδετικός ιστός» που διασφαλίζει ότι το σωστό άτομο έχει τη σωστή πληροφορία τη σωστή στιγμή.
- Σύγχρονη (σε πραγματικό χρόνο): Άμεση επικοινωνία για γρήγορη επίλυση προβλημάτων και καθημερινή συνεργασία (π.χ. Slack, Microsoft Teams).
- Ασύγχρονη (με καθυστέρηση): Επίσημη επικοινωνία και καταγραφή χωρίς ανάγκη άμεσης απάντησης (π.χ. Outlook, Gmail).
- Εικονική παρουσία: Κάλυψη της απόστασης σε απομακρυσμένες ομάδες μέσω πρόσωπο με πρόσωπο επικοινωνίας (π.χ. Zoom, Google Meet).

Κατηγορίες ψηφιακής εργασίας

3. Οργάνωση: Σχεδιασμός & Διαχείριση Πόρων

- Το πλαίσιο που διαχειρίζεται τους δύο πιο περιορισμένους πόρους: τον χρόνο και τη συγκέντρωση.
- Διαχείριση χρόνου: Οργάνωση της διαθεσιμότητας ατόμων και ομάδων (π.χ. Google Calendar, Calendly).
- Διαχείριση έργων & εργασιών: Παρακολούθηση προόδου, ανάθεση ευθυνών και τήρηση προθεσμιών (π.χ. Asana, Trello, Monday.com).
- Διαχείριση γνώσης: Συγκέντρωση εσωτερικής πληροφορίας και τεκμηρίωσης (π.χ. Notion, Obsidian, Confluence).

4. Ανάλυση & Δεδομένα: Πληροφόρηση & Λήψη Αποφάσεων

- Το αναλυτικό επίπεδο που μετατρέπει τα ακατέργαστα δεδομένα σε στρατηγικές ενέργειες.
- Μοντελοποίηση σε υπολογιστικά φύλλα: Ποσοτικοποίηση λογικής, προϋπολογισμών και οργάνωση δομημένων δεδομένων (π.χ. Excel, Google Sheets).
- Επιχειρηματική ευφυΐα (BI): Οπτικοποίηση σύνθετων δεδομένων μέσω διαδραστικών dashboards (π.χ. Tableau, Power BI).

Κάθε κατηγορία απαιτεί διαφορετικά εργαλεία και διαφορετική λογική χρήσης.

Στρατηγική επιλογή εργαλείων παραγωγικότητας

Η επιλογή εργαλείων πρέπει να βασίζεται στη λογική της επιχείρησης και όχι στη δημοφιλία.

Αξιολογήστε κάθε εργαλείο με βάση αυτούς τους τέσσερις κρίσιμους πυλώνες:

- Αποδοτικότητα κόστους σε σχέση με την τιμή αγοράς: Μην εξετάζετε μόνο τη συνδρομή. Υπολογίστε την απόδοση επένδυσης (ROI). Ο χρόνος που εξοικονομείται από την ομάδα δικαιολογεί το μηνιαίο κόστος;
- Διαλειτουργικότητα και ενσωμάτωση: Το εργαλείο «συνεργάζεται» με το υπάρχον σύστημά σας; Ένα εργαλείο είναι παραγωγικό μόνο αν συγχρονίζεται ομαλά με τα βασικά σας συστήματα (π.χ. Google Workspace, Microsoft 365 ή υπάρχον CRM/ERP).
- Καμπύλη εκμάθησης και χρηστικότητα: Πόσο εύχρηστο είναι το περιβάλλον; Εκτιμήστε τον «συνολικό χρόνο με την εξοικείωση». Ένα πολύπλοκο εργαλείο που απαιτεί εβδομάδες εκπαίδευσης μπορεί να μειώσει την παραγωγικότητα της ομάδας.
- Ασφάλεια και συμμόρφωση με τον GDPR: Τα δεδομένα διαχειρίζονται σύμφωνα με τα Ευρωπαϊκά πρότυπα; Ελέγξτε αν το εργαλείο προσφέρει κρυπτογράφηση, πολυπαραγοντική ταυτοποίηση (MFA) και σαφείς πολιτικές διαχείρισης δεδομένων.

Quiz5

Παρακαλώ επιλέξτε τη σωστή απάντηση.

Ποια είναι η σωστή προσέγγιση κατά την επιλογή ενός ψηφιακού εργαλείου;

- ☐ 4. Χρησιμοποιείτε πάντα δωρεάν εργαλεία
- ☐ 2. Επιλέξτε το πιο σύνθετο εργαλείο
- ☐ 3. Αντιστοιχίστε το εργαλείο με τις απαιτήσεις της εργασίας
- ☐ 1. Επιλέξτε το πιο δημοφιλές εργαλείο

Η παγίδα των «δωρεάν» εργαλείων στο επαγγελματικό περιβάλλον

Τα δωρεάν εργαλεία συχνά φαίνονται οικονομικά αποδοτικά, αλλά περιέχουν κρυφούς κινδύνους.

Βασικά προβλήματα των δωρεάν εργαλείων:

1. Έλλειψη βασικών χαρακτηριστικών ασφάλειας

Τα δωρεάν εργαλεία συχνά δεν διαθέτουν τα απαραίτητα μέτρα προστασίας για τα επιχειρησιακά δεδομένα.

Παράδειγμα: Μια δωρεάν πλατφόρμα αποθήκευσης στο cloud μπορεί να μην προσφέρει κρυπτογράφηση δεδομένων, αφήνοντας ευαίσθητες πληροφορίες εκτεθειμένες.

2. Έλλειψη τεχνικής υποστήριξης

Τα δωρεάν εργαλεία συνήθως παρέχουν περιορισμένη ή καθόλου τεχνική υποστήριξη, με αποτέλεσμα τα προβλήματα να παραμένουν άλυτα για μεγαλύτερο χρονικό διάστημα.

Παράδειγμα: Αν παρουσιαστεί κάποιο πρόβλημα, μπορεί να υπάρξει καθυστέρηση στην επίλυσή του χωρίς εξειδικευμένη υποστήριξη, οδηγώντας σε απώλεια παραγωγικότητας.

Η παγίδα των «δωρεάν» εργαλείων στο επαγγελματικό περιβάλλον

3. Δημιουργία «Data Silos» και έλλειψη ενσωμάτωσης

Πολλά δωρεάν εργαλεία δεν ενσωματώνονται με άλλα επιχειρησιακά συστήματα ή λογισμικά. Αυτό δημιουργεί «data silos», δηλαδή απομονωμένα σύνολα δεδομένων που δεν επικοινωνούν μεταξύ τους, οδηγώντας σε αναποτελεσματικότητα και κακή επικοινωνία μέσα στην ομάδα.

Παράδειγμα: Η χρήση ενός δωρεάν εργαλείου διαχείρισης επαφών που δεν συγχρονίζεται με το email ή το CRM σας οδηγεί σε κατακερματισμένα δεδομένα, προκαλώντας λάθη και καθυστερήσεις.

4. Αυξημένα κρυφά κόστη σε χρόνο και κινδύνους ασφάλειας

Παρότι τα δωρεάν εργαλεία φαίνονται αρχικά οικονομικά, τα κρυφά κόστη —όπως κενά στην ασφάλεια και έλλειψη υποστήριξης— μπορούν να οδηγήσουν σε μεγαλύτερα έξοδα μακροπρόθεσμα. Ο χρόνος που δαπανάται για επίλυση προβλημάτων, διαχείριση ενσωματώσεων και αντιμετώπιση κινδύνων ασφάλειας μπορεί να κοστίσει περισσότερο από ένα επί πληρωμή εργαλείο.

Παράδειγμα: Αν ένα δωρεάν εργαλείο δεν καλύπτει πλέον τις ανάγκες καθώς η επιχείρηση αναπτύσσεται, μπορεί να χρειαστεί μετάβαση σε άλλη λύση, δημιουργώντας επιπλέον «κρυφό» κόστος αλλαγής (switching cost).

Σύνδεση χρήσης εργαλείων με την αποδοτικότητα

Η λογική: Αποδοτικότητα = (Αξία αποτελέσματος) / (Χρόνος + Προσπάθεια)

Ο στόχος είναι να διασφαλίσετε ότι τα εργαλεία που χρησιμοποιείτε σας βοηθούν να επιτυγχάνετε αποτελέσματα υψηλής ποιότητας με τον ελάχιστο δυνατό χρόνο και προσπάθεια. Τα εργαλεία πρέπει να βελτιώνουν το αποτέλεσμα χωρίς να προσθέτουν περιττή πολυπλοκότητα.

Τα λειτουργικά λάθη έχουν κόστος και συχνά προκύπτουν από χειροκίνητες διαδικασίες, όπως:

- λάθη κατά την καταχώρηση δεδομένων
- χαμένα emails
- συγκρούσεις εκδόσεων σε συνεργατική εργασία

Παράδειγμα: Με την αυτόματη ενημέρωση των στοιχείων επαφών στο CRM, αποφεύγετε τη χειροκίνητη ενημέρωση εγγραφών, μειώνοντας τα λάθη και εξοικονομώντας χρόνο. Αυτή η ενσωμάτωση διασφαλίζει ότι τα δεδομένα είναι συνεπή και ενημερωμένα σε όλα τα συστήματα.

Κατηγορία	Επαγγελματικά Εργαλεία
Συλλογιστική Τεχνητή Νοημοσύνη & Προηγμένη σύνταξη κειμένου	ChatGPT, Gemini, Claude.ai, MS Word
Έρευνα & σύνθεση πληροφορίας	Perplexity, Google Scholar, Claude (PDF)
Δεδομενοκεντρικός εγγραμματισμός & Ανάλυση δεδομένων	MS Excel, Google Sheets, Power BI
Οπτικός σχεδιασμός & Αφήγηση περιεχομένου	MS PowerPoint, Canva, Adobe Express, Midjourney
Διαχείριση ροής εργασίας & γνώσης	Trello, Asana, Notion, MS Planner
Συνεργασία & Διαχείριση συναντήσεων	MS Teams, Slack, Otter.ai, Fireflies.ai

Λογική βελτιστοποίησης στον χώρο εργασίας

Η βελτιστοποίηση ξεκινά με τον εντοπισμό των «στενωπών» (bottlenecks) στη ροή εργασίας.

Τα bottlenecks είναι τα σημεία που επιβραδύνουν τη συνολική διαδικασία και μπορεί να προκύπτουν από αναποτελεσματικά εργαλεία, χειροκίνητες διαδικασίες ή κακή συνεργασία.

Κανόνας 80/20

- «Το 20% των εργαλείων σας παράγει το 80% της αξίας σας.»
- Εντοπίστε και εστιάστε στα εργαλεία που πραγματικά ενισχύουν την εργασία σας και εξετάστε την αφαίρεση όσων προσφέρουν μικρή αξία.

Αυτοματοποίηση vs Χειροκίνητη εργασία

- Αυτοματοποίηση: Χρήση ψηφιακών εργαλείων για την απλοποίηση διαδικασιών και την εξάλειψη επαναλαμβανόμενων εργασιών.
- Χειροκίνητη εργασία: Εργασίες που απαιτούν ανθρώπινη παρέμβαση, συχνά πιο αργές και με μεγαλύτερη πιθανότητα λαθών.

Ο ρόλος της Τεχνητής Νοημοσύνης στις σύγχρονες ροές εργασίας ως συνεργάτης παραγωγικότητας

Η Τεχνητή Νοημοσύνη δεν είναι πλέον προαιρετική — αποτελεί βασικό επίπεδο παραγωγικότητας.

Για να αξιοποιήσουν αποτελεσματικά την ΤΝ, οι επαγγελματίες πρέπει να αλλάξουν τον τρόπο σκέψης τους: η Παραγωγική ΤΝ (ChatGPT, Claude, Gemini) δεν είναι μηχανή αναζήτησης· είναι μηχανή συλλογισμού (Reasoning Engine).

Βασικές δυνατότητες (Τι μπορεί να κάνει):

- **Σύνθεση:** Σύνοψη σύνθετων αναφορών ή μεγάλων email threads
- **Παραγωγή:** Δημιουργία αρχικών εκδόσεων email, προτάσεων ή περιεχομένου
- **Ιδεασμός:** Παραγωγή ιδεών και σχεδιασμός έργων
- **Τεχνική υποστήριξη:** Δημιουργία, διόρθωση κώδικα ή αναδιαμόρφωση δεδομένων

Κρίσιμοι περιορισμοί (Τι δεν μπορεί να εγγυηθεί):

- **Ακρίβεια:** Δεν εγγυάται την αλήθεια — προβλέπει μοτίβα (κίνδυνος «hallucinations»)
- **Πλαίσιο:** Δεν διαθέτει «κοινή λογική» και δεν κατανοεί εσωτερικό επιχειρησιακό πλαίσιο χωρίς καθοδήγηση
- **Ευθύνη:** Δεν μπορεί να αναλάβει επαγγελματική ευθύνη για το αποτέλεσμα

Βασική αρχή: Αντιμετωπίστε τη Παραγωγική ΤΝ ως έναν πολύ ικανό αλλά όχι πλήρως αξιόπιστο συνεργάτη.

Μπορεί να εκτελέσει το 80% της εργασίας σε δευτερόλεπτα, αλλά απαιτεί ανθρώπινη επίβλεψη για την επαλήθευση, τη βελτίωση και την τελική έγκριση του υπόλοιπου 20%.

Χρήση Τεχνητής Νοημοσύνης για σύνοψη

Η Τεχνητή Νοημοσύνη μειώνει το γνωστικό φορτίο σε επαναλαμβανόμενες εργασίες:

- σύνοψη μεγάλων εγγράφων
- σύνταξη email και αναφορών
- δομή περιεχομένου

Παράδειγμα: Σας παρουσιάζεται μια αναφορά 50 σελίδων, αλλά έχετε μόνο 10 λεπτά πριν από μια κρίσιμη στρατηγική συνάντηση.

Ενέργεια με TN: Ανεβάζετε το έγγραφο ή παρέχετε το κείμενο σε ένα LLM (π.χ. ChatGPT) με ένα στοχευμένο prompt:

«Εξήγαγε τα 5 βασικά συμπεράσματα και τους 3 βασικούς κινδύνους για μια μικρή μεταποιητική επιχείρηση από αυτή την αναφορά.»

Οφέλη: Άμεση μείωση της υπερφόρτωσης πληροφορίας.

Χρησιμοποιήστε την TN για να εξοικονομήσετε χρόνο από εργασίες χαμηλής αξίας — και εστιάστε στις αποφάσεις.

Πόσο χρόνο θα μπορούσατε να εξοικονομήσετε εβδομαδιαία χρησιμοποιώντας TN για σύνοψη;

Χρήση Τεχνητής Νοημοσύνης για οργάνωση εργασίας

Τα εργαλεία Τεχνητής Νοημοσύνης μπορούν να υποστηρίξουν την οργάνωση της εργασίας, μετατρέποντας την πληροφορία, τις εργασίες και τις διαδικασίες σε πιο σαφείς και διαχειρίσιμες μορφές.

Η ΤΝ μπορεί να χρησιμοποιηθεί για τη δόμηση:

- **Λιστών εργασιών** → διάσπαση σύνθετων δραστηριοτήτων σε μικρότερα, εκτελέσιμα βήματα
- **Ροών εργασίας** → οργάνωση διαδικασιών σε λογική ακολουθία (π.χ. βήμα-βήμα)
- **Μορφών δεδομένων** → μετατροπή μη δομημένης πληροφορίας σε πίνακες, σύνοψη ή κατηγορίες

Η ΤΝ υποστηρίζει:

- **Σαφήνεια** → βελτιώνει την κατανόηση εργασιών και ευθυνών
- **Ιεράρχηση** → βοηθά στον εντοπισμό του επείγοντος και του σημαντικού
- **Σχεδιασμό** → ενισχύει τη διαχείριση χρόνου και τον συντονισμό εργασιών

Παράδειγμα: Ένας εργαζόμενος χρησιμοποιεί την ΤΝ για να μετατρέψει σημειώσεις συνάντησης σε μια δομημένη λίστα εργασιών, να ορίσει προτεραιότητες και προθεσμίες.

Αυτό βελτιώνει την αποδοτικότητα και μειώνει τον κίνδυνο παράλειψης ενεργειών.

Χρήση Τεχνητής Νοημοσύνης για σύνταξη και παραγωγή ιδεών

Η Τεχνητή Νοημοσύνη είναι ιδιαίτερα χρήσιμη για:

- υπέρβαση της «λευκής σελίδας» → έναρξη σύνθετων ή απαιτητικών εργασιών
- παραγωγή πολλαπλών εκδοχών → εξερεύνηση τόνου, δομής και προσέγγισης
- υποστήριξη ανάπτυξης ιδεών → δόμηση εννοιών και στρατηγικών επικοινωνίας

Παράδειγμα:

Prompt: «Δημιούργησε 5 εκδοχές ενός ευγενικού αλλά σταθερού email για αίτημα έκπτωσης 10% από έναν μακροχρόνιο προμηθευτή.»

Ο χρήστης μπορεί να συγκρίνει διαφορετικούς τόνους (επίσημο, συνεργατικό, πιο αποφασιστικό) και να επιλέξει τον πιο κατάλληλο.

Οφέλη:

- Γρήγορη δημιουργία εναλλακτικών (Rapid Prototyping) → εξερεύνηση πολλών επιλογών σε δευτερόλεπτα
- Γλωσσική ακρίβεια (Linguistic Precision) → πρόσβαση σε επαγγελματική διατύπωση και λεξιλόγιο
- Μείωση γνωστικού φορτίου (Cognitive Offloading) → λιγότερη προσπάθεια στη σύνταξη, περισσότερη εστίαση στις αποφάσεις

Το Μοντέλο Συνεργασίας Ανθρώπου–Τεχνητής Νοημοσύνης(διάγραμμα ροής εργασίας)

Εσείς είστε ο «πιλότος» και η Τεχνητή Νοημοσύνη ο «συγκυβερνήτης».Ο πιλότος έχει πάντα την ευθύνη για την προσγείωση.

1. Άνθρωπος: Καθορίζει τον στόχο, παρέχει το πλαίσιο και ορίζει τους περιορισμούς.

2. Τεχνητή Νοημοσύνη: Δημιουργεί προσχέδια, προτείνει εναλλακτικές και επεξεργάζεται μεγάλο όγκο δεδομένων.

3. Άνθρωπος: Αξιολογεί, επαληθεύει τα δεδομένα, βελτιώνει και αναλαμβάνει την ευθύνη.

Prompt Engineering: Η τέχνη της σωστής καθοδήγησης

Ένα prompt δεν είναι απλώς μια ερώτηση, αλλά μια εντολή. Στην εποχή της Τεχνητής Νοημοσύνης, η ποιότητα του αποτελέσματος καθορίζεται άμεσα από την ακρίβεια της εισόδου σας.

Στοιχείο	Η «Ασαφής» Προσέγγιση (Αδύναμη)	Η «Αρχιτεκτονική» Προσέγγιση (Ισχυρή)
To Prompt	«Γράψε ένα επιχειρηματικό πλάνο.»	"Λειτουργήσε ως Σύμβουλος Επιχειρήσεων. Δημιούργησε μια στρατηγική εισόδου στην αγορά σε 3 φάσεις για μια εταιρεία που λανσάρεται στην ΕΕ. Εστίασε στη συμμόρφωση με τον GDPR και στο τοπικό marketing."
Το Αποτέλεσμα	Γενικό, «επιφανειακό» κείμενο που απαιτεί σημαντική επεξεργασία. Στρατηγική υψηλού επιπέδου, άμεσα εφαρμόσιμη και προσαρμοσμένη στους συγκεκριμένους περιορισμούς.	Στρατηγική υψηλού επιπέδου, άμεσα εφαρμόσιμη και προσαρμοσμένη στους συγκεκριμένους περιορισμούς.
Η Διαφορά	Έλλειψη πλαισίου, ρόλου και συγκεκριμένων στόχων.	Ιδιότητα + Πλαίσιο + Συγκεκριμένος στόχος + Περιορισμοί

Quiz6

Παρακαλώ επιλέξτε τη σωστή απάντηση.

Ποιος είναι ο κύριος κίνδυνος από τη χρήση δημόσιων εργαλείων AI με πραγματικά δεδομένα;

- ☐ 3. Καλύτερη αυτοματοποίηση
- ☐ 1. Μειωμένη ταχύτητα
- ☐ 2. Έκθεση δεδομένων και απώλεια ελέγχου
- ☐ 4. Ευκολότερη ροή εργασίας

Το Πλαίσιο CREATE για τη διαμόρφωση prompts

- **Charter:** Ποιος πρέπει να είναι ο ρόλος της ΤΝ; (π.χ. «Λογιστής»)
- **Request:** Ποια είναι η εργασία; (π.χ. «Ανάλυσε αυτόν τον προϋπολογισμό»)
- **Examples:** Παρέχετε πρότυπο ή στυλ.
- **Audience:** Σε ποιον απευθύνεται; (π.χ. «Διοικητικό Συμβούλιο»)
- **Type:** Ποια είναι η μορφή; (π.χ. «Πίνακας», «Email»)
- **Extras:** Περιορισμοί (π.χ. «Κάτω από 200 λέξεις», «Χωρίς τεχνική ορολογία»)

Η χρήση ενός πλαισίου όπως το CREATE διασφαλίζει ότι δεν παραλείπετε το απαραίτητο πλαίσιο που κάνει την ΤΝ πραγματικά χρήσιμη.

Εξασκηθείτε σε αυτό το πλαίσιο μέχρι να γίνει δεύτερη φύση.

Παράδειγμα ενός σωστά δομημένου prompt με χρήση του πλαισίου CREATE

- **Character:** "Assistant Manager"
- **Request:** «Σύνοψη της απόδοσης πωλήσεων του μήνα.»
- **Examples:** «Παρουσίασε τη σύνοψη σε bullets με βασικούς δείκτες όπως συνολικές πωλήσεις, προϊόντα με την καλύτερη απόδοση και σημεία προς βελτίωση.»
- **Audience:** «Ομάδα πωλήσεων»
- **Type:** "Bullet λίστα"
- **Extras:** «Κράτησε τη σύνοψη κάτω από 150 λέξεις. Χρησιμοποίησε σαφή και απλή γλώσσα.»

Επεξήγηση:

- **Character:** Ορίζουμε τον ρόλο της ΤΝ («Assistant Manager») ώστε να έχει το κατάλληλο πλαίσιο και επαγγελματική οπτική.
- **Request:** Η εργασία είναι σαφής: σύνοψη της απόδοσης πωλήσεων για τον μήνα.
- **Examples:** Καθορίζουμε πώς θέλουμε το αποτέλεσμα (bullets με βασικούς δείκτες απόδοσης).
- **Audience:** Ορίζουμε το κοινό-στόχο («Ομάδα πωλήσεων») ώστε η ΤΝ να προσαρμόσει τον τόνο και το περιεχόμενο.
- **Type:** Ζητάμε συγκεκριμένη μορφή (bullet λίστα), που είναι εύκολη στην ανάγνωση και κατανόηση.
- **Extras:** Οι περιορισμοί (όριο λέξεων και απλή γλώσσα) διασφαλίζουν ότι το αποτέλεσμα είναι σύντομο, σαφές και πρακτικό.

Αξιολόγηση αποτελέσματος ΤΝ: Η τετραπλή επαλήθευση

Για να διασφαλιστούν παραδοτέα επαγγελματικού επιπέδου, τα αποτελέσματα της ΤΝ δεν πρέπει ποτέ να χρησιμοποιούνται αυτούσια.

Εφαρμόστε μια αυστηρή λίστα τετραπλής επαλήθευσης πριν οριστικοποιηθεί οποιοδήποτε αποτέλεσμα:

- **Εμπειρική ακρίβεια & ακεραιότητα δεδομένων:** Είναι σωστά τα συγκεκριμένα αριθμητικά στοιχεία, οι ημερομηνίες και τα κύρια ονόματα;
- **Ύφος & τόνος:** Ακούγεται το κείμενο «ρομποτικό» ή υπερβολικά γενικό;
- **Συνάφεια με το πλαίσιο & χρησιμότητα:** Λύνει πράγματι το αποτέλεσμα το συγκεκριμένο εργασιακό πρόβλημα ή είναι μια γενική απάντηση;
- **Συμμόρφωση με ηθικές αρχές & ασφάλεια:** Συμμορφώνεται το περιεχόμενο με τις ηθικές κατευθυντήριες γραμμές της εταιρείας και τα πρότυπα του GDPR;

Πλοήγηση στην Καμπύλη Ωριμότητας της Τεχνητής Νοημοσύνης: Ευχέρεια vs. Εξειδίκευση

- Ευχέρεια (Το «Πώς»): Ανάπτυξη της γλωσσικής και τεχνικής ικανότητας επικοινωνίας με το μοντέλο TN (εξοικείωση με το Prompt Engineering και το πλαίσιο CREATE).
- ΑΙ Εξειδίκευση (Το «Πρέπει» & «Γιατί»): Κατανόηση του πότε η TN αποτελεί το κατάλληλο εργαλείο και πότε μια καθαρά ανθρώπινη προσέγγιση είναι προτιμότερη.
- Ικανότητα συστηματικής επαλήθευσης των αποτελεσμάτων και εντοπισμού «παραισθήσεων» (hallucinations) — δηλαδή πληροφοριών που φαίνονται στατιστικά εύλογες αλλά είναι στην πραγματικότητα λανθασμένες.
Η TN συχνά παράγει σφάλματα σε συγκεκριμένα οικονομικά στοιχεία, νομικές αναφορές, κύρια ονόματα και γεγονότα που συνέβησαν μετά την τελευταία ενημέρωση της εκπαίδευσής της.

«Σοφία στη χρήση της TN» (AI-Wisdom): Οι περισσότεροι χρήστες σταματούν στο επίπεδο της ευχέρειας, αποδεχόμενοι τα αποτελέσματα της TN χωρίς αμφισβήτηση. Ένας επαγγελματίας σε επίπεδο Εξειδίκευσης αναγνωρίζει ότι τα LLMs είναι μηχανές πιθανοτήτων και όχι μηχανές αναζήτησης βάσεων δεδομένων. Το να είναι κανείς «σοφός» στη χρήση της TN σημαίνει να διατηρεί μια υγιή δόση σκεπτικισμού και να εφαρμόζει μια ισχυρή διαδικασία επαλήθευσης.

Ηθική της Τεχνητής Νοημοσύνης: Διαφάνεια και Υπευθυνότητα (Ιδιοκτησία)

Βασικές αρχές:

- **Διαφάνεια:** Να είστε ειλικρινείς όταν ένα παραδοτέο έχει δημιουργηθεί 100% από ΤΝ.
- **Μεροληψία:** Η ΤΝ μπορεί να αναπαράγει κοινωνικές προκαταλήψεις (φύλο, φυλή). Ένας επαγγελματίας οφείλει να τις εντοπίζει και να τις διορθώνει.
- **Υπευθυνότητα (Ιδιοκτησία):** Αναλαμβάνετε την ιδιοκτησία του αποτελέσματος μόνο εφόσον το έχετε επεξεργαστεί ουσιαστικά και το έχετε επαληθεύσει.
Η επαγγελματική σας «υπογραφή» σημαίνει ότι αναλαμβάνετε πλήρως την ευθύνη για το περιεχόμενο, ανεξάρτητα από το πώς δημιουργήθηκε.

Θα πρέπει ένας φοιτητής να επιτρέπεται να χρησιμοποιεί ΤΝ για μια εργασία; Θα πρέπει ένας εργαζόμενος να τη χρησιμοποιεί για μια αναφορά που περιλαμβάνει πραγματικά δεδομένα; Υπάρχει διαφορά;

Η ηθική σχετίζεται με την οικοδόμηση εμπιστοσύνης. Αν αποκρύπτετε τη χρήση της ΤΝ, υπονομεύετε την επαγγελματική σας αξιοπιστία.

Αυτοαξιολόγηση: Εντοπισμός των Ψηφιακών σας Κενών

Οι Μικρομεσαίες Επιχειρήσεις (ΜΜΕ) αντιμετωπίζουν μοναδικές ψηφιακές προκλήσεις:

- Περιορισμένη υποστήριξη IT (συχνά είστε ο ίδιος η τεχνική υποστήριξη).
- Ανάγκη για υψηλή ευελιξία (πολλαπλές εργασίες σε διαφορετικά εργαλεία).
- Άμεσος αντίκτυπος στα έσοδα (η αναποτελεσματικότητα κοστίζει άμεσα στην επιχείρηση).



Δεν μπορείτε να βελτιώσετε κάτι που δεν μπορείτε να μετρήσετε. Πριν ξεκινήσουμε, πρέπει να εντοπίσουμε το «κενό».

- Χρησιμοποιείτε μόνο τα εργαλεία που ήδη γνωρίζετε ή αυτά που είναι πραγματικά τα καταλληλότερα;
- Μπορώ να αυτοματοποιήσω μια επαναλαμβανόμενη αναφορά;
- Μπορώ να διακρίνω μια «παραισθητική» απάντηση της ΤΝ από ένα πραγματικό γεγονός;

Η πραγματική επαγγελματική ανάπτυξη ξεκινά όταν αναγνωρίζουμε ποιους τεχνικούς τομείς αποφεύγουμε. Οι περισσότεροι επαγγελματίες αξιοποιούν μόλις το 10% των δυνατοτήτων του λογισμικού που χρησιμοποιούν.

Το Σχέδιο Ψηφιακής Βελτίωσης (DIP) – (Μέρος 1: Εργαλεία & Τεχνητή Νοημοσύνη)

Φάση 1: Εντοπισμός

- Καταγράψτε 3 ψηφιακές εργασίες που αποτελούν αυτή τη στιγμή σημεία συμφόρησης, δηλαδή εργασίες που σας παίρνουν υπερβολικά πολύ χρόνο ή προκαλούν σημαντική απογοήτευση.

Φάση 2: Έρευνα Εργαλείων

- Εντοπίστε ένα συγκεκριμένο εργαλείο (είτε πρόκειται για εργαλείο ΤΝ είτε για συμβατικό λογισμικό) που έχει τη δυνατότητα να επιλύσει ή να αυτοματοποιήσει καθεμία από αυτές τις εργασίες.

Φάση 3: Στόχοι Μάθησης

- Θέστε έναν συγκεκριμένο στόχο «micro-learning» για αυτή την εβδομάδα.
- Παράδειγμα: Παρακολουθήστε 3 εκπαιδευτικά βίντεο για Excel Macros ώστε να αυτοματοποιήσετε την εβδομαδιαία αναφορά.

Ένα Σχέδιο Ψηφιακής Βελτίωσης είναι ένα δυναμικό έγγραφο που αποτυπώνει την επαγγελματική σας εξέλιξη. Δεν πρέπει να είναι στατικό, αλλά να εξελίσσεται καθώς εξελίσσονται και οι δεξιότητές σας.

Σενάριο Περίπτωσης: Η Ροή Εργασίας «Γρήγορα αλλά Λάθος»

Η Μαρία εργάζεται σε μια μικρή επιχείρηση ως διοικητική βοηθός. Πρέπει να ετοιμάσει ένα ενημερωτικό email προς πελάτη και μια σύντομη αναφορά βασισμένη σε εσωτερικά δεδομένα.

Για να εξοικονομήσει χρόνο:

- Χρησιμοποιεί TN για να συντάξει το email και την αναφορά
- Αντιγράφει δεδομένα πελατών απευθείας στο εργαλείο TN
- Χρησιμοποιεί ένα δωρεάν εργαλείο διαμοιρασμού αρχείων για να στείλει την αναφορά
- Δεν ελέγχει προσεκτικά το αποτέλεσμα της TN

Η εργασία ολοκληρώνεται σε 15 λεπτά αντί για 1 ώρα.

Τι συμβαίνει στη συνέχεια:

- Το email περιέχει ανακριβείς πληροφορίες (παραισθήσεις της TN)
- Ευαίσθητα δεδομένα πελατών εκτέθηκαν μέσω του εργαλείου TN
- Το αρχείο στάλθηκε σε λάθος έκδοση
- Ο πελάτης εντοπίζει ασυνέπειες και αμφισβητεί την αξιοπιστία

Τι πήγε λάθος σε αυτή τη ροή εργασίας; Εντοπίστε τουλάχιστον 3 κρίσιμα λάθη.



Παρακαλώ επιλέξτε τη σωστή απάντηση.

Ποιο είναι το βασικό στοιχείο ενός επαγγελματικού email;

- ☐ 3. Σαφής σκοπός και δομημένο μήνυμα
- ☐ 2. Ανεπίσημος τόνος
- ☐ 4. Χρήση emojis
- ☐ 1. Μακροσκελής εισαγωγή

Ανάλυση Σεναρίου: Τι Έπρεπε να Είχε Γίνει;

1. Αποτυχία Ανάλυσης Εργασίας

- Δεν έγινε αξιολόγηση της ευαισθησίας των δεδομένων και του απαιτούμενου επιπέδου ακρίβειας.
- Λανθασμένη υπόθεση: «Η TN = ασφαλής συντόμευση»

2. Λανθασμένη Χρήση της TN

- Εισαγωγή ευαίσθητων δεδομένων σε δημόσιο εργαλείο TN

3. Κακή Επιλογή Εργαλείων

- Χρήση δωρεάν, μη ενσωματωμένου εργαλείου
- Αποτέλεσμα: σύγχυση εκδόσεων και έλλειψη ελέγχου

4. Έλλειψη Επαλήθευσης Αποτελέσματος

- Μη διενέργεια τελικού ελέγχου πριν την αποστολή, οδηγώντας σε κίνδυνο για την επαγγελματική αξιοπιστία

Σωστή Επαγγελματική Ροή Εργασίας:

- ✓ Αφαίρεση ή ανωνυμοποίηση ευαίσθητων δεδομένων πριν τη χρήση TN
- ✓ Χρήση μόνο εγκεκριμένων εργαλείων
- ✓ Επαλήθευση αποτελέσματος TN (ακρίβεια + τόνος)
- ✓ Επιβεβαίωση τελικής έκδοσης πριν την αποστολή

Η επαγγελματική εργασία δεν αφορά την ταχύτητα. Αφορά ελεγχόμενα και αξιόπιστα αποτελέσματα.

Πηγές & Περαιτέρω Μελέτη

Για να ενισχύσετε τις δεξιότητές σας στα ψηφιακά εργαλεία και την Τεχνητή Νοημοσύνη, εξερευνήστε τις ακόλουθες πηγές:

- [OECD AI Principles](#)
- [5 AI for Work Tips and Tricks – YouTube](#)

Αυτό το βίντεο παρουσιάζει πώς τα εργαλεία ΤΝ μπορούν να υποστηρίξουν καθημερινές επαγγελματικές εργασίες, όπως η σύνταξη κειμένων, η σύνοψη πληροφοριών και η οργάνωση της εργασίας. Αναδεικνύει πρακτικούς τρόπους ενσωμάτωσης της ΤΝ στις καθημερινές ροές εργασίας, διατηρώντας παράλληλα τον έλεγχο και την ποιότητα.

Ψηφιακή Επικοινωνία, Συνεργασία & Επαγγελματική Ταυτότητα

Ενότητα 4



Co-funded by
the European Union

Το Κόστος της Κακής Ψηφιακής Επικοινωνίας

Η κακή ψηφιακή επικοινωνία δημιουργεί λειτουργικές αναποτελεσματικότητες και επηρεάζει τόσο τη ροή εργασίας όσο και τις επαγγελματικές σχέσεις.

Επιπτώσεις της Κακής Επικοινωνίας

- **Παρερμηνεία** → ασαφή μηνύματα οδηγούν σε λανθασμένη κατανόηση
- **Καθυστερήσεις** → οι εργασίες απαιτούν διευκρινίσεις ή επανεκτέλεση
- **Σφάλματα** → λανθασμένη εκτέλεση οδηγιών
- **Απώλεια εμπιστοσύνης** → μειωμένη εμπιστοσύνη στην ποιότητα της επικοινωνίας

Παράδειγμα:

Ασαφές email → παρεξήγηση της εργασίας → λανθασμένο αποτέλεσμα → απώλεια χρόνου

Ένα μόνο ασαφές μήνυμα μπορεί να επηρεάσει πολλούς ανθρώπους.

Η ασαφής επικοινωνία δημιουργεί κρυφό λειτουργικό κόστος.

Αρχές Επαγγελματικής Ψηφιακής Επικοινωνίας

Βασικές Αρχές

- **Σαφήνεια** → χωρίς ασάφειες
- **Συντομία** → χωρίς περιττές πληροφορίες
- **Δομή** → εύκολη κατανόηση και παρακολούθηση
- **Στοχοκεντρική προσέγγιση** → εστίαση στο αποτέλεσμα

Ορθή Πρακτική

- Καθορίστε το μήνυμά σας πριν ξεκινήσετε να γράφετε
- Εστιάστε σε αυτό που χρειάζεται ο αποδέκτης

Παράδειγμα:

Καλά δομημένο μήνυμα → ταχύτερη λήψη αποφάσεων → λιγότερα λάθη

Αν ο αποδέκτης πρέπει να μαντέψει, η επικοινωνία έχει αποτύχει.

Δομή Επαγγελματικού Email

- Σαφής γραμμή θέματος (subject)
 - Ο σκοπός αναφέρεται στην πρώτη πρόταση
 - Δομημένο μήνυμα (σύντομες παράγραφοι)
 - Ξεκάθαρη ενέργεια ή προσδοκία
- Παράδειγμα: Θέμα: Απαιτείται Ενημέρωση – Project X. Παρακαλώ ελέγξτε και επιβεβαιώστε τις αλλαγές έως την Παρασκευή.
- **Προτεινόμενα Εργαλεία**
- Outlook / Gmail (για διαχείριση email)
 - Grammarly (εργαλείο TN για τόνο και σαφήνεια)

Κίνδυνοι

- Ασαφή email → καθυστερήσεις και σύγχυση
- Μακροσκελή μηνύματα → μειωμένη προσοχή

Σύνταξη Επαγγελματικού Email

Βασική Δομή

- **Χαιρετισμός** → επαγγελματικός και προσαρμοσμένος στο πλαίσιο (Αγαπητή/έ [Όνομα], Καλησπέρα/Καλημέρα [Όνομα])
- **Σκοπός («Γιατί»)** → αναφέρετε τον λόγο του email στις πρώτες 1–2 προτάσεις
- **Αίτημα («Τι ζητάω»)** → ορίστε ξεκάθαρα τι χρειάζεται και χρησιμοποιήστε bullets για πολλαπλά αιτήματα
- **Κλείσιμο** → επαγγελματικό κλείσιμο + υπογραφή (Όνομα, Ρόλος, Οργανισμός, Στοιχεία επικοινωνίας / LinkedIn)

- Παράδειγμα:

“Καλησπέρα Μαρία,

Επικοινωνώ για να ζητήσω το επικαιροποιημένο αρχείο του έργου για έλεγχο.

Μπορείς να στείλεις:

- *την τελική έκδοση*
- *το πιο πρόσφατο αρχείο προϋπολογισμού”*

Ψηφιακή Γλώσσα Σώματος: Τόνος στη Γραπτή Επικοινωνία

In digital communication, tone is conveyed through wording, punctuation and visual cues, not voice or facial expression.

Key Elements

- **Emojis**
 - αποδεκτά σε ανεπίσημη εσωτερική επικοινωνία (Teams, Slack)
 - αποφεύγονται σε επίσημα ή εξωτερικά emails
- **Στίξη** → η υπερβολική χρήση (!!!, ???) φαίνεται αντιεπαγγελματική
- **Επιλογή λέξεων** → σύντομα ή απότομα μηνύματα μπορεί να παρερμηνευτούν

Παράδειγμα:

- “Εντάξει.” → μπορεί να εκληφθεί ως απότομο ή αρνητικό
- “Συμφωνώ, μου φαίνεται εντάξει.” → πιο σαφές και ουδέτερο

Κανόνες Ψηφιακής Συμπεριφοράς (Netiquette) σε Επαγγελματικά Περιβάλλοντα

Το Netiquette ορίζει τη σωστή συμπεριφορά στην ψηφιακή επικοινωνία.

Βασικοί Κανόνες

- Χρησιμοποιείτε επαγγελματικό τόνο
- Αποφεύγετε ανεπίσημη γλώσσα σε επίσημα πλαίσια
- Σέβεστε τον χρόνο απόκρισης

Ο τόνος συχνά παρερμηνεύεται στην ψηφιακή επικοινωνία

Κίνδυνοι

- Παρερμηνεία του τόνου
- Αντίληψη αντιεπαγγελματικής συμπεριφοράς

Ορθή Πρακτική

- Ελέγξτε τον τόνο πριν την αποστολή
- Προσαρμόστε την επικοινωνία στο εκάστοτε πλαίσιο

Κανάλια Επικοινωνίας – Επιλογή του Κατάλληλου

Διαφορετικά εργαλεία επικοινωνίας εξυπηρετούν διαφορετικούς σκοπούς.

- Επιλογή Καναλιού
 - Email → επίσημη επικοινωνία
 - Chat (Teams, Slack) → γρήγορος συντονισμός
 - Συναντήσεις → σύνθετες συζητήσεις
- Το εργαλείο διαμορφώνει το μήνυμα.

Κίνδυνος

Λάθος κανάλι → λάθος αποτέλεσμα

Ορθή Πρακτική

Επιλέξτε το κατάλληλο κανάλι με βάση τον σκοπό και το επίπεδο επείγοντος

Συνεργασία σε Ψηφιακά Περιβάλλοντα Εργασίας

Η σύγχρονη εργασία βασίζεται σε κοινόχρηστα και διασυνδεδεμένα ψηφιακά εργαλεία.

Βασικά Στοιχεία

- Κοινόχρηστα έγγραφα
- Συνεργασία σε πραγματικό χρόνο
- Συστήματα βασισμένα στο cloud

Οφέλη

- Ταχύτητα
- Διαφάνεια
- Συντονισμός

Προτεινόμενα Εργαλεία

- Google Workspace
- Microsoft Teams / SharePoint
- Notion

Κίνδυνοι στη Ψηφιακή Συνεργασία

Συνήθεις Κίνδυνοι

- Συγκρούσεις εκδόσεων (version conflicts)
- Ασαφής κατανομή ευθυνών (ownership)
- Αντικατάσταση/υπεργραφή περιεχομένου
- Έκθεση δεδομένων
- Παράδειγμα: Πολλοί χρήστες επεξεργάζονται ταυτόχρονα → χάνονται αλλαγές

Ορθή Πρακτική

- Ανάθεση υπευθυνότητας
- Παρακολούθηση αλλαγών
- Χρήση ελεγχόμενης πρόσβασης

Η συνεργασία χωρίς έλεγχο δημιουργεί χάος

Έλεγχος Πρόσβασης: Ποιος Μπορεί να Κάνει Τι

Επίπεδα Πρόσβασης

- **Viewer** (Προβολή) → μόνο ανάγνωση
- **Commenter** (Σχολιασμός) → παροχή σχολίων
- **Editor** (Επεξεργασία) → πλήρης πρόσβαση

Κίνδυνοι

- Υπερβολική πρόσβαση → έκθεση δεδομένων
- Περιορισμένη πρόσβαση → αναποτελεσματικότητα

Ορθή Πρακτική

- Αναθέστε δικαιώματα πρόσβασης με προσοχή

Ασφαλείς Πρακτικές στη Διαμοίραση Δεδομένων

Η ασφαλής διαμοίραση αρχείων διασφαλίζει ότι τα δεδομένα του οργανισμού προσπελούνται, χρησιμοποιούνται και διανέμονται με ελεγχόμενο και προστατευμένο τρόπο.

Η λανθασμένη διαμοίραση αρχείων μπορεί να οδηγήσει σε:

- Μη εξουσιοδοτημένη πρόσβαση
- Διαρροή δεδομένων
- Απώλεια ελέγχου των πληροφοριών

Βέλτιστες Πρακτικές

- Χρήση εγκεκριμένων πλατφορμών του οργανισμού → διασφαλίζει ασφάλεια, καταγραφή ενεργειών (logging) και συμμόρφωση
- Αποφυγή μη ασφαλών καναλιών → π.χ. προσωπικό email, εφαρμογές μηνυμάτων
- Έλεγχος ρυθμίσεων κοινοποίησης → περιορισμός πρόσβασης, απενεργοποίηση λήψης όπου απαιτείται

Προτεινόμενα Εργαλεία

- OneDrive / SharePoint → έλεγχος σε επίπεδο επιχείρησης
- Google Drive → ευέλικτη διαμοίραση και συνεργασία

Διατήρηση Ακρίβειας στη Συνεργατική Εργασία

Ο έλεγχος εκδόσεων (version control) διασφαλίζει ότι όλοι οι χρήστες εργάζονται στη σωστή και πιο πρόσφατη έκδοση ενός εγγράφου.

Χωρίς Έλεγχο Εκδόσεων

- Σύγχυση σχετικά με την τελευταία έκδοση
- Διπλά αρχεία
- Αντικατάσταση ή απώλεια εργασίας

Ορθή Πρακτική

- Χρήση κοινόχρηστων εγγράφων αντί για συνημμένα αρχεία
- Ενεργοποίηση παρακολούθησης αλλαγών / ιστορικού εκδόσεων
- Αποφυγή λήψης και επαναφόρτωσης αρχείων

Εργαλεία

- Google Docs (συνεργασία σε πραγματικό χρόνο)
- Microsoft 365 (ιστορικό εκδόσεων και συνεργασία)

Quiz8

Ποιο είναι το κύριο όφελος του ελέγχου εκδόσεων (version control) σε κοινόχρηστα έγγραφα;

- ☐ 4. Βελτίωση σχεδιασμού
- ☐ 2. Αποφυγή σύγχυσης σχετικά με την τελευταία έκδοση
- ☐ 3. Μείωση μεγέθους αρχείου
- ☐ 1. Ταχύτερη πληκτρολόγηση

Πώς Αντιλαμβάνονται οι Άλλοι την Παρουσία σας στα Ψηφιακά Περιβάλλοντα

Η ψηφιακή σας ταυτότητα είναι η επαγγελματική εικόνα που προβάλλετε μέσω της συμπεριφοράς σας, της επικοινωνίας σας και της διαδικτυακής σας παρουσίας.

Βασικά Στοιχεία

- Στυλ επικοινωνίας → σαφήνεια, τόνος, επαγγελματισμός
- Διαδικτυακή παρουσία → προφίλ, αναρτήσεις, κοινοποιημένο περιεχόμενο
- Συμπεριφορά στα εργαλεία → συνήθειες συνεργασίας, ανταπόκριση

Παράδειγμα (Επαγγελματικό Περιβάλλον)

- Συνεπής και σαφής επικοινωνία → αξιόπιστος επαγγελματίας
- Ασαφής ή ανεπίσημη συμπεριφορά → μειωμένη αξιοπιστία

Διαχείριση του Ψηφιακού σας Αποτυπώματος

Κάθε ψηφιακή ενέργεια αφήνει ένα αποτύπωμα που μπορεί να επηρεάσει την επαγγελματική σας φήμη.

Τι Περιλαμβάνει

- Emails και συνημμένα αρχεία
- Εσωτερικά μηνύματα (Teams, Slack)
- Δραστηριότητα στα μέσα κοινωνικής δικτύωσης

Παράδειγμα:

Μη επαγγελματικό σχόλιο σε εσωτερικό chat → κοινοποίηση εκτός οργανισμού → αρνητικός αντίκτυπος στη φήμη

Όρια στην Ψηφιακή Επικοινωνία

Τα υγιή όρια στην ψηφιακή επικοινωνία υποστηρίζουν την παραγωγικότητα, την ευεξία και τη λήψη ασφαλέστερων αποφάσεων.

Κίνδυνοι της κουλτούρας «Always-On»

- Εξουθένωση και κόπωση
- Μειωμένη συγκέντρωση
- Αυξημένα λάθη

Παράδειγμα:

- *Συνεχείς ειδοποιήσεις → διάσπαση προσοχής → απρόσεκτα λάθη*

Ορθή Πρακτική

- Καθορίστε διαθεσιμότητα και χρόνους απόκρισης
- Διαχειριστείτε τις ειδοποιήσεις
- Αποφύγετε μη επείγουσα επικοινωνία εκτός ωραρίου εργασίας

Επαγγελματική Ευθύνη στην Επικοινωνία

Η ηθική επικοινωνία διασφαλίζει ότι η πληροφορία διαμοιράζεται με υπευθυνότητα, σεβασμό και με τρόπο που προστατεύει τα άτομα, τους οργανισμούς και τα δεδομένα.

Βασικές Αρχές

- **Σεβασμός** → επικοινωνείτε επαγγελματικά, αποφεύγοντας προσβλητική, ανεπίσημη ή ακατάλληλη γλώσσα
- **Διαφάνεια** → παρέχετε σαφή, ειλικρινή και πλήρη πληροφόρηση, αποφεύγοντας παραπλανητικά ή ελλιπή μηνύματα
- **Εμπιστευτικότητα** → προστατεύετε ευαίσθητα, προσωπικά ή εταιρικά δεδομένα και μοιράζεστε πληροφορίες μόνο με εξουσιοδοτημένα άτομα

Παράδειγμα: Κοινοποίηση εσωτερικών πληροφοριών της εταιρείας σε δημόσιο κανάλι ή προώθηση email χωρίς έλεγχο δικαιωμάτων πρόσβασης

Κίνδυνοι

- Παραβίαση εμπιστευτικότητας
- Ζημιά στη φήμη
- Απώλεια εμπιστοσύνης μεταξύ ομάδων ή πελατών
- Πιθανές νομικές συνέπειες

Ορθή Πρακτική

- Επικοινωνείτε με σαφήνεια και ειλικρίνεια
- Επαληθεύετε τους παραλήπτες πριν τη διαμοίραση πληροφοριών
- Σέβεστε την ευαισθησία των δεδομένων και τους κανόνες προστασίας ιδιωτικότητας

Κοινή Ευθύνη σε Ψηφιακά Περιβάλλοντα Εργασίας

Η συνεργασία απαιτεί από κάθε συμμετέχοντα να αναλαμβάνει ευθύνη για τις ενέργειες, τη συμβολή και την επικοινωνία του.

Βασικές Ευθύνες

Κάθε χρήστης είναι υπεύθυνος για:

- Ακρίβεια → διασφάλιση ότι οι πληροφορίες που κοινοποιούνται είναι σωστές και αξιόπιστες
- Διαχείριση Δεδομένων → υπεύθυνη χρήση, αποθήκευση και διαμοίραση δεδομένων
- Σαφήνεια Επικοινωνίας → παροχή ξεκάθαρων οδηγιών και ενημερώσεων
- Παράδειγμα: Ένα μέλος της ομάδας ανεβάζει λανθασμένα δεδομένα σε κοινόχρηστο αρχείο χωρίς έλεγχο. Αυτό επηρεάζει την εργασία ολόκληρης της ομάδας.

Κίνδυνοι

- Διάδοση σφαλμάτων σε όλη την ομάδα
- Σύγχυση και ανάγκη επανεργασίας
- Μειωμένη εμπιστοσύνη στα κοινά αποτελέσματα

Ορθή Πρακτική

- Επαληθεύετε τις πληροφορίες πριν τις κοινοποιήσετε
- Επικοινωνείτε ξεκάθαρα τις αλλαγές
- Αναλαμβάνετε την ευθύνη για τη συνεισφορά σας
- Υποστηρίζετε τον συντονισμό της ομάδας

Στη συνεργατική εργασία, οι ατομικές ενέργειες επηρεάζουν τα συλλογικά αποτελέσματα

Κατανόηση των Λόγων που Οδηγούν σε Αποτυχία της Επικοινωνίας

Οι αποτυχίες στην επικοινωνία συχνά προκύπτουν από ανθρώπινη συμπεριφορά, κακή δομή ή ακατάλληλη επιλογή εργαλείων.

Συνήθεις Αιτίες

- Υποθέσεις → αναμένεται από τους άλλους να κατανοήσουν χωρίς επεξήγηση
- Έλλειψη σαφήνειας → ασαφή ή ελλιπή μηνύματα
- Κακή δομή → μη οργανωμένη πληροφορία
- Λανθασμένα εργαλεία → χρήση ακατάλληλων καναλιών επικοινωνίας

Παράδειγμα: Αποστολή σύνθετης εργασίας μέσω chat αντί για δομημένο email → οδηγεί σε σύγχυση και απώλεια σημαντικών πληροφοριών

Κίνδυνοι

- Παρεξηγήσεις
- Καθυστερήσεις στην εκτέλεση
- Λανθασμένα αποτελέσματα
- Μειωμένη αποδοτικότητα

Ορθή Πρακτική

- Επικοινωνείτε με σαφήνεια και ακρίβεια
- Δομείτε την πληροφορία λογικά
- Επιλέγετε το κατάλληλο κανάλι επικοινωνίας

Οι περισσότερες αποτυχίες στην επικοινωνία μπορούν να προληφθούν



Τι χαρακτηρίζει το επαγγελματικό ψηφιακό περιεχόμενο;

- ☐ 3. Σαφής δομή, σκοπός και ακρίβεια
- ☐ 2. Περίπλοκη γλώσσα
- ☐ 1. Μακροσκελές και λεπτομερές κείμενο
- ☐ 4. Χρήση πολλών οπτικών μέσων

Βέλτιστες Πρακτικές για Συνεργασία

Βασικές Κατευθυντήριες Γραμμές

- ✓ **Ορισμός ρόλων** → ανάθεση ευθυνών για εργασίες και περιεχόμενο
- ✓ **Χρήση κοινόχρηστων εργαλείων** → διασφάλιση ότι όλα τα μέλη εργάζονται στο ίδιο περιβάλλον
- ✓ **Επικοινωνία αλλαγών** → ενημέρωση της ομάδας για τροποποιήσεις ή ενημερώσεις
- ✓ **Παρακολούθηση εκδόσεων** → διατήρηση ελέγχου στην εξέλιξη των εγγράφων

Κίνδυνοι Κακών Πρακτικών

- Σύγχυση και διπλή εργασία
- Ασυνεπής πληροφορία
- Απώλεια ελέγχου περιεχομένου

Η συνεργασία είναι αποτελεσματική μόνο όταν είναι δομημένη και ελεγχόμενη

Επαγγελματική Συμπεριφορά σε Online Συναντήσεις

Οι εικονικές συναντήσεις απαιτούν το ίδιο επίπεδο επαγγελματισμού με τις διαζώσης αλληλεπιδράσεις.

Βασικές Πρακτικές

- Προετοιμασία → ελέγξτε μικρόφωνο, κάμερα και σύνδεση πριν από τη συνάντηση
- Περιβάλλον → χρησιμοποιήστε καθαρό ή θολωμένο φόντο → διασφαλίστε κατάλληλο φωτισμό και σωστή τοποθέτηση
- Συμμετοχή → αποφύγετε τις διακοπές → χρησιμοποιήστε λειτουργίες όπως «Raise Hand»
- Πειθαρχία Μικροφώνου → παραμείνετε σε σίγαση όταν δεν μιλάτε για αποφυγή περισπασμών

Παράδειγμα:

Ανοιχτό μικρόφωνο → θόρυβος στο παρασκήνιο → διακοπή της συνάντησης

Σενάριο Περίπτωσης – Κακή Επικοινωνία

Σενάριο

- Μια ομάδα συνεργάζεται σε ένα κοινόχρηστο έγγραφο:
- Δεν υπάρχει σαφής υπεύθυνος
- Πολλοί χρήστες επεξεργάζονται ταυτόχρονα
- Δεν υπάρχει επικοινωνία σχετικά με τις αλλαγές

Τι Συμβαίνει

- Επικαλυπτόμενες αλλαγές
- Συγκρούσεις εκδόσεων
- Απώλεια πληροφοριών

Αποτέλεσμα

- Σύγχυση μεταξύ των μελών της ομάδας
- Σφάλματα στο περιεχόμενο
- Καθυστερήσεις στην ολοκλήρωση του έργου

Lack of structure leads to operational inefficiency

Η έλλειψη δομής οδηγεί σε λειτουργική αναποτελεσματικότητα

Ανάλυση Σεναρίου – Τι Πήγε Λάθος;

Βασικά Προβλήματα

- Έλλειψη υπευθυνότητας → δεν υπάρχει σαφής ευθύνη για το περιεχόμενο
- Έλλειψη δομής → απουσία οργανωμένης ροής εργασίας
- Κακή επικοινωνία → δεν υπάρχουν ενημερώσεις ή συντονισμός

Επιπτώσεις

- Διπλή προσπάθεια
- Ασυνεπή αποτελέσματα
- Μειωμένη παραγωγικότητα

Ορθή Πρακτική

- ✓ Ανάθεση σαφών ρόλων και ευθυνών
- ✓ Χρήση εργαλείων ελέγχου εκδόσεων
- ✓ Επικοινωνία ενημερώσεων και αλλαγών
- ✓ Καθορισμός ροής εργασίας πριν τη συνεργασία

Η αποτελεσματική συνεργασία απαιτεί δομή, όχι απλώς συμμετοχή

Τελικός Έλεγχος πριν την Κοινοποίηση ή τη Συνεργασία

Ένας τελικός έλεγχος διασφαλίζει ότι η επικοινωνία και η συνεργασία είναι σαφείς, ακριβείς και κατάλληλες.

Λίστα Ελέγχου

Πριν από την αποστολή ή την κοινοποίηση:

- ✓ **Είναι σαφές;** → είναι το μήνυμα κατανοητό;
- ✓ **Είναι πλήρες;** → περιλαμβάνει όλες τις απαραίτητες πληροφορίες;
- ✓ **Είναι κατάλληλο;** → είναι ο τόνος και η μορφή σωστά;
- ✓ **Είναι σωστή η πρόσβαση;** → έχουν οι σωστοί άνθρωποι τα κατάλληλα δικαιώματα;

Παράδειγμα:

Πριν την κοινοποίηση ενός αρχείου:

- Ελέγξτε τη σαφήνεια
- Επαληθεύστε το περιεχόμενο
- Επιβεβαιώστε τα δικαιώματα πρόσβασης

Προλαμβάνει λάθη και παρεξηγήσεις.

Δημιουργία & Επεξεργασία Ψηφιακού Περιεχομένου για Επαγγελματικά Παραδοτέα

Ενότητα 5



Co-funded by
the European Union

Τι Καθορίζει το Επαγγελματικό Ψηφιακό Περιεχόμενο;

Το επαγγελματικό ψηφιακό περιεχόμενο καθορίζεται από τα εξής χαρακτηριστικά:

- Σαφήνεια → εύκολα κατανοητό, χωρίς ασάφειες ή περιττή πολυπλοκότητα
- Δομή → λογικά οργανωμένο, με ξεκάθαρη ροή και σειρά
- Ακρίβεια → σωστό και επαληθευμένο, βασισμένο σε αξιόπιστες πληροφορίες
- Σκοπός → ευθυγραμμισμένο με τον στόχο της εργασίας, το κοινό και το επιθυμητό αποτέλεσμα

Κακό περιεχόμενο οδηγεί σε:

- Παρερμηνεία
- Λανθασμένες αποφάσεις
- Απώλεια αξιοπιστίας
- Σύγχυση στη ροή εργασίας

Αν το περιεχόμενό σας δεν είναι σαφές, τότε και η εργασία σας δεν είναι σαφής. Η επαγγελματική επικοινωνία αντικατοπτρίζει την επαγγελματική επάρκεια και επηρεάζει άμεσα την εμπιστοσύνη και την απόδοση.

Δομή Περιεχομένου για Μέγιστη Αποτελεσματικότητα

Το επαγγελματικό περιεχόμενο πρέπει να ακολουθεί μια απλή και συνεπή δομή:

- **Σκοπός** → Τι επιδιώκει να πετύχει αυτό το έγγραφο ή μήνυμα;
- **Κύριο Μήνυμα** → Ποιο είναι το πιο σημαντικό σημείο που πρέπει να κατανοήσει ο αναγνώστης;
- **Υποστηρικτική Πληροφορία** → Ποια δεδομένα, εξηγήσεις ή αποδείξεις υποστηρίζουν το μήνυμα;
- **Συμπέρασμα / Ενέργεια** → Τι πρέπει να συμβεί στη συνέχεια; Τι αναμένεται από τον αναγνώστη;

Παράδειγμα::

- **Κακή δομή** → μακροσκελές, μη οργανωμένο κείμενο χωρίς τίτλους ή σαφή εστίαση
- **Αποτελεσματική δομή** → ξεκάθαρες ενότητες, λογική ροή, ανάδειξη βασικών σημείων

Η δεύτερη προσέγγιση επιτρέπει ταχύτερη κατανόηση και καλύτερη λήψη αποφάσεων.

Ισορροπία Κειμένου και Οπτικού Περιεχομένου

Το αποτελεσματικό περιεχόμενο αξιοποιεί:

- **Κείμενο** → για την επεξήγηση ιδεών, την παροχή λεπτομερειών και τη διασφάλιση ακρίβειας
- **Οπτικά στοιχεία** → για την ανάδειξη βασικών σημείων, την απλοποίηση σύνθετων πληροφοριών και την καθοδήγηση της προσοχής

Ο στόχος είναι η συμπληρωματικότητα και όχι ο ανταγωνισμός.

Παράδειγμα:

- Αναφορά μόνο με πυκνό κείμενο → δύσκολη στην ανάγνωση και κατανόηση
- Αναφορά με δομημένο κείμενο και απλά οπτικά στοιχεία (εικονίδια, διαγράμματα) → πιο εύκολη στην κατανόηση και στη λήψη αποφάσεων

Κίνδυνοι ανισορροπίας

- **Υπερβολικό κείμενο** → γνωστική υπερφόρτωση, μειωμένη προσοχή, απώλεια σημαντικών πληροφοριών
- **Υπερβολικά οπτικά στοιχεία** → απόσπαση προσοχής, απώλεια εστίασης, ασάφεια μηνύματος

Ορθή Πρακτική

- Χρησιμοποιείτε οπτικά στοιχεία για να διευκρινίζετε βασικές ιδέες, όχι απλώς για διακόσμηση
- Διατηρείτε το κείμενο σύντομο και δομημένο
- Αναδεικνύετε οπτικά τις βασικές πληροφορίες
- Διασφαλίζετε ότι τα οπτικά στοιχεία υποστηρίζουν άμεσα το μήνυμα

Σχεδιασμός Ευανάγνωστων Εγγράφων

Βασικές Αρχές Αναγνωσιμότητας

Για τη βελτίωση της αναγνωσιμότητας:

- **Σύντομες παράγραφοι** → κάνουν το περιεχόμενο πιο εύκολο στην ανάγνωση και κατανόηση
- **Σαφείς τίτλοι** → καθοδηγούν τον αναγνώστη στη δομή του κειμένου
- **Κουκκίδες (bullet points)** → αναδεικνύουν βασικές πληροφορίες και ενισχύουν τη σαφήνεια
- **Συνεπής μορφοποίηση** → δημιουργεί μια επαγγελματική και προβλέψιμη εμπειρία ανάγνωσης

Παράδειγμα:

- Έγγραφο με μεγάλα, συνεχόμενα κείμενα χωρίς δομή → δύσκολο στην παρακολούθηση
- Έγγραφο με τίτλους, κενά και κουκκίδες → εύκολο στην ανάγνωση και κατανόηση

Δημιουργία Επαγγελματικών Παρουσιάσεων

Βασικές Αρχές

Οι αποτελεσματικές παρουσιάσεις:

- **Εστιάζουν στα βασικά μηνύματα** → αναδεικνύουν το ουσιώδες, όχι όλη τη διαθέσιμη πληροφορία
- **Αποφεύγουν την υπερφόρτωση πληροφοριών** → περιορίζουν το περιεχόμενο σε αυτό που μπορεί να κατανοηθεί εύκολα
- **Χρησιμοποιούν οπτική ιεραρχία** → καθοδηγούν την προσοχή μέσω τίτλων, αποστάσεων και έμφασης

Προτεινόμενα Εργαλεία

- **Microsoft PowerPoint** → το βασικό επαγγελματικό εργαλείο παρουσιάσεων
- **Canva** → εύχρηστα πρότυπα και υποστήριξη οπτικού σχεδιασμού
- **Google Slides** → συνεργατική δημιουργία παρουσιάσεων στο cloud

Κίνδυνοι Κακού Σχεδιασμού Παρουσίασης

- Σύγχυση ή αποσύνδεση του κοινού
- Απώλεια ή παρερμηνεία βασικών μηνυμάτων
- Μειωμένη αξιοπιστία και αντίκτυπος

Ορθή Πρακτική

- Απλοποιείτε το περιεχόμενο στα βασικά σημεία
- Δομείτε τις διαφάνειες με σαφήνεια και συνέπεια
- Υποστηρίζετε το κείμενο με ουσιαστικά οπτικά στοιχεία
- Σχεδιάζετε παρουσιάσεις που καθοδηγούν την κατανόηση, όχι απλώς προβάλλουν πληροφορία

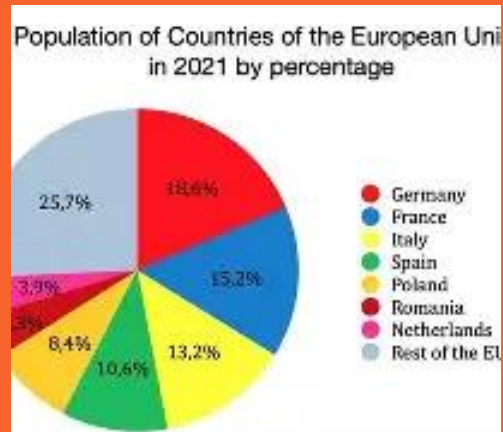
Σχεδιασμός και Δόμηση Εγγράφων

Η αποτελεσματική σχεδίαση και δόμηση εγγράφων περιλαμβάνει:

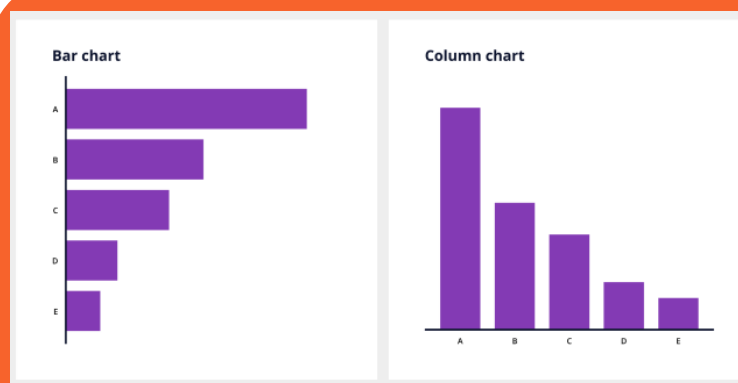
- **Πρότυπα (Templates)** → προκαθορισμένες μορφές που διασφαλίζουν συνέπεια σε όλα τα έγγραφα
- **Τυποποιημένες δομές** → σαφής οργάνωση (π.χ. εισαγωγή, κύριο μέρος, συμπέρασμα)
- **Συνεπής μορφοποίηση** → ομοιόμορφες γραμματοσειρές, αποστάσεις, τίτλοι και διάταξη
- Παράδειγμα:
 - **Τυχαίο έγγραφο** → ασυνεπής διάταξη, ασαφής δομή, δύσκολο στην κατανόηση
 - **Αναφορά βασισμένη σε εταιρικό πρότυπο** → δομημένες ενότητες, συνεπής σχεδιασμός, εύκολη πλοήγηση

Τα δομημένα έγγραφα βελτιώνουν τη χρηστικότητα και τον επαγγελματισμό.

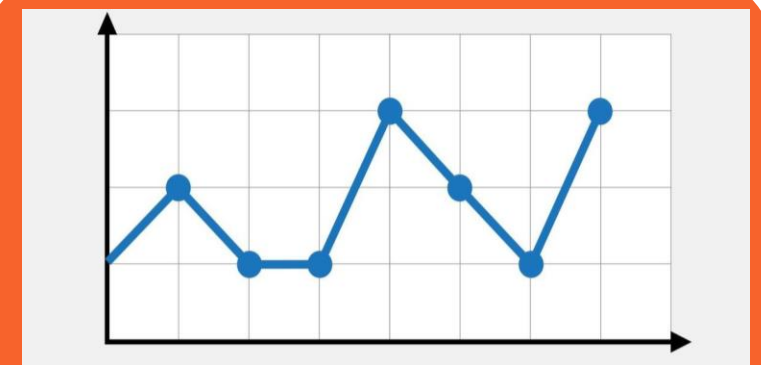
Οπτικοποίηση Δεδομένων: Μετατροπή Αριθμών σε Χρήσιμες Πληροφορίες



Κυκλικά Διαγράμματα (Pie Charts – Πίτα): Κατάλληλα για την απεικόνιση μερών ενός συνόλου (περιορίστε σε λιγότερες από 5 κατηγορίες).



Διαγράμματα Ράβδων / Σηλών (Bar/Column Charts): Κατάλληλα για συγκρίσεις μεταξύ διαφορετικών ομάδων ή χρονικών περιόδων.



Γραμμικά Διαγράμματα (Line Graphs): Κατάλληλα για την απεικόνιση τάσεων με την πάροδο του χρόνου.

Επεξεργασία για Ποιότητα

Η αποτελεσματική επεξεργασία περιλαμβάνει:

- **Γραμματική** → σωστή χρήση της γλώσσας για διασφάλιση επαγγελματισμού και αξιοπιστίας
- **Σαφήνεια** → ξεκάθαρη και κατανοητή διατύπωση χωρίς ασάφειες
- **Ακρίβεια** → ορθότητα σε στοιχεία, δεδομένα και πληροφορίες
- **Τόνος** → κατάλληλο ύφος ανάλογα με το κοινό και το πλαίσιο
- Παράδειγμα:
 - *Email πρόχειρου σχεδίου χωρίς έλεγχο* → ασαφές μήνυμα και πιθανή παρεξήγηση
 - *Email μετά από έλεγχο και επιμέλεια* → σαφής, ακριβής και επαγγελματική επικοινωνία

Η επεξεργασία βελτιώνει τόσο την κατανόηση όσο και τον αντίκτυπο.

Η συγγραφή είναι το προσχέδιο — η επεξεργασία είναι ο επαγγελματισμός.

Υπεύθυνη Χρήση Τεχνητής Νοημοσύνης στη Δημιουργία Επαγγελματικού Περιεχομένου

Η Τεχνητή Νοημοσύνη μπορεί να υποστηρίξει:

- **Σύνταξη (Drafting)** → δημιουργία αρχικών εκδόσεων περιεχομένου
- **Επαναδιατύπωση (Rewriting)** → βελτίωση σαφήνειας, τόνου ή δομής
- **Δομή (Structuring)** → οργάνωση ιδεών σε λογικά σχήματα

Αρχές Ηθικής Χρήσης

- **Μην αντιγράφετε άκριτα** → πάντα να ελέγχετε και να προσαρμόζετε το περιεχόμενο
- **Επαληθεύετε την ακρίβεια** → διασταυρώνετε με αξιόπιστες πηγές
- **Αποφεύγετε μεροληψία** → αξιολογείτε κριτικά το περιεχόμενο που παράγει η ΤΝ

Σεβασμός στην Πνευματική Ιδιοκτησία στο Επαγγελματικό Ψηφιακό Περιεχόμενο

Τα πνευματικά δικαιώματα (copyright) παρέχουν αυτόματη νομική προστασία σε πρωτότυπα έργα (κείμενα, εικόνες, κώδικα, μουσική) από τη στιγμή της δημιουργίας τους. Στην Ευρωπαϊκή Ένωση, κάθε πρωτότυπο περιεχόμενο προστατεύεται εξ ορισμού.

- Η επαγγελματική χρήση περιεχομένου απαιτεί:
 - **Σεβασμό στην ιδιοκτησία** → αναγνώριση ότι το περιεχόμενο ανήκει στον δημιουργό του
 - **Αποφυγή λογοκλοπής** → μη αντιγραφή ή παρουσίαση έργου άλλων ως δικό σας
 - **Χρήση αδειοδοτημένου υλικού** → διασφάλιση ότι υπάρχει άδεια για επαγγελματική χρήση

Ο μύθος των «δημόσιων» εικόνων: Το γεγονός ότι μια εικόνα εμφανίζεται στο Google δεν σημαίνει ότι είναι ελεύθερη για επαγγελματική χρήση.

Παράδειγμα: Ένας εργαζόμενος χρησιμοποιεί μια εικόνα από το διαδίκτυο σε εταιρική παρουσίαση χωρίς να ελέγξει τα δικαιώματα χρήσης.

Αυτό μπορεί να οδηγήσει σε νομικές και ζητήματα φήμης για τον οργανισμό.

Κίνδυνοι

- Νομικές ενέργειες ή οικονομικές κυρώσεις
- Παραβίαση πνευματικών δικαιωμάτων
- Ζημιά στη φήμη του οργανισμού
- Απώλεια επαγγελματικής αξιοπιστίας

Ορθή Πρακτική

- Χρησιμοποιείτε αδειοδοτημένο ή royalty-free περιεχόμενο
- Ελέγχετε πάντα τα δικαιώματα χρήσης πριν αξιοποιήσετε υλικό
- Αναφέρετε τις πηγές όπου απαιτείται
- Θεωρείτε το περιεχόμενο προστατευμένο εκτός αν δηλώνεται ρητά το αντίθετο

Πλοήγηση στις Άδειες Creative Commons (CC)

- **CC-BY (Αναφορά Δημιουργού)** → το περιεχόμενο μπορεί να χρησιμοποιηθεί, αλλά πρέπει να αναφέρεται ο δημιουργός
- **CC-NC (Μη Εμπορική Χρήση)** → δεν μπορεί να χρησιμοποιηθεί για επιχειρηματικές, διαφημιστικές ή κερδοσκοπικές δραστηριότητες
- **CC-ND (Χωρίς Παράγωγα Έργα)** → το περιεχόμενο μπορεί να χρησιμοποιηθεί, αλλά δεν επιτρέπεται να τροποποιηθεί ή να επεξεργαστεί
- **CC0 (Δημόσιος Τομέας)** → χωρίς περιορισμούς· ελεύθερη χρήση χωρίς υποχρέωση αναφοράς

Παράδειγμα: Μια μικρομεσαία επιχείρηση (ΜΜΕ) χρησιμοποιεί μια εικόνα με άδεια CC-NC σε διαφημιστική καμπάνια. Αυτό παραβιάζει την άδεια, επειδή η χρήση είναι εμπορική.

Πλοήγηση στις Άδειες Creative Commons (CC)



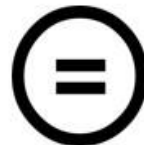
BY (attribute)



Share Alike



Non-Commercial



No Derivatives



MOST OPEN



LEAST OPEN

Ηθική Αναζήτηση Πόρων: Επαγγελματικές Βιβλιοθήκες Υλικού

Επιλογές Υψηλής Ποιότητας για Αναζήτηση Υλικού:

- **Εικόνες:** Unsplash, Pexels, Pixabay (πάντα να ελέγχετε την άδεια χρήσης για κάθε εικόνα ξεχωριστά)
- **Εικονίδια:** The Noun Project, Flaticon, Icons8 (συχνά απαιτείται αναφορά δημιουργού)
- **Γραμματοσειρές:** Google Fonts (ανοιχτού κώδικα και ασφαλείς για επαγγελματική χρήση)
- **Εσωτερικές Βιβλιοθήκες:** Δημιουργία κοινόχρηστου φακέλου με προεγκεκριμένα και αδειοδοτημένα στοιχεία για την ομάδα, ώστε να αποφεύγονται λάθη

Παράδειγμα: Μια ομάδα ετοιμάζει μια παρουσίαση χρησιμοποιώντας:

- Αδειοδοτημένες εικόνες από το Unsplash
- Εικονίδια από το Flaticon (με αναφορά δημιουργού)
- Εταιρικά εγκεκριμένα πρότυπα

Αυτό διασφαλίζει τόσο τη νομική συμμόρφωση όσο και τη συνεπή, επαγγελματική οπτική ταυτότητα.

Αποφυγή Λογοκλοπής

Η λογοκλοπή αναφέρεται στην αντιγραφή κειμένου ή ιδεών χωρίς αναφορά στην πηγή.

- Επαγγελματική Παράφραση → διατύπωση ιδεών με δικά σας λόγια, συνοδευόμενη από αναφορά στην πηγή (π.χ. «Σύμφωνα με το ENISA (2024)...»)
- Παράθεση (Quoting) → χρήση των ακριβών λέξεων με εισαγωγικά και αναφορά στον δημιουργό (χρησιμοποιείται επιλεκτικά για έμφαση)
- Αυτο-λογοκλοπή → επαναχρησιμοποίηση δικής σας εργασίας σε διαφορετικό πλαίσιο χωρίς σχετική δήλωση

Παράδειγμα:

Ένας εργαζόμενος αντιγράφει περιεχόμενο από μια διαδικτυακή αναφορά σε εταιρικό έγγραφο χωρίς να αναφέρει την πηγή.

Αυτό αποτελεί λογοκλοπή και μπορεί να επηρεάσει αρνητικά την αξιοπιστία και την εμπιστοσύνη.

Ηθικός Έλεγχος – Παράφραση vs Παραγωγή από Τεχνητή Νοημοσύνη

Η δημιουργία επαγγελματικού περιεχομένου απαιτεί διαφάνεια σχετικά με τον τρόπο παραγωγής του, ιδιαίτερα όταν χρησιμοποιούνται εργαλεία Τεχνητής Νοημοσύνης.

Το Επαγγελματικό Πρότυπο

- Πρωτότυπη Έρευνα (Original Research) → περιεχόμενο που βασίζεται σε ανθρώπινη ανάλυση και τεκμηριωμένες πηγές
- Παραφρασμένο Περιεχόμενο (Paraphrased Content) → ανθρώπινη ερμηνεία υπαρχουσών πληροφοριών με σωστή αναφορά
- Περιεχόμενο που Παράγεται από ΤΝ (AI-Generated Content) → αποτέλεσμα υποβοηθούμενο από μηχανή, το οποίο πρέπει να ελέγχεται, να προσαρμόζεται και—όταν είναι ουσιαστικό—να δηλώνεται

Ο Κανόνας της Διαφάνειας

Όταν ένας πελάτης ή οργανισμός αναμένει επαγγελματική κρίση, η παράδοση πλήρως παραγόμενου από ΤΝ περιεχομένου χωρίς δήλωση:

- παρουσιάζει λανθασμένα τη φύση της εργασίας
- ενδέχεται να παραβιάζει την επαγγελματική εμπιστοσύνη ή ακόμη και συμβατικούς όρους

Η διαφάνεια δεν είναι απλώς καλή πρακτική—είναι βασική προϋπόθεση επαγγελματικής αξιοπιστίας.

Ροή Εργασίας για Δημιουργία Περιεχομένου

Βήμα προς Βήμα Ροή Εργασίας

1. **Καθορισμός Σκοπού** → Ποιος είναι ο στόχος του περιεχομένου; Σε ποιο κοινό απευθύνεται;
2. **Σύνταξη Περιεχομένου** → Δημιουργήστε την αρχική εκδοχή, εστιάζοντας στις βασικές ιδέες
3. **Δόμηση Περιεχομένου** → Οργανώστε τις πληροφορίες λογικά (τίτλοι, ενότητες, ροή)
4. **Επεξεργασία και Βελτίωση** → Βελτιώστε τη σαφήνεια, τον τόνο, τη γραμματική και τη συνοχή
5. **Επικύρωση** → Επαληθεύστε την ακρίβεια, ελέγξτε τις πηγές και διασφαλίστε την καταλληλότητα για χρήση

Quiz10

Ποιο είναι το σωστό πρώτο βήμα όταν αντιμετωπίζετε ένα τεχνικό ζήτημα;

- ☐ 1. Δοκιμή τυχαίων λύσεων
- ☐ 4. Άμεση κλιμάκωση (escalation) σε ανώτερο επίπεδο
- ☐ 3. Ακολουθία μιας δομημένης διαδικασίας αντιμετώπισης προβλημάτων
- ☐ 2. Αγνόηση του ζητήματος

Έλεγχος Ποιότητας & Αυτοαξιολόγηση

Ο έλεγχος ποιότητας αποτελεί το τελικό στάδιο στη δημιουργία περιεχομένου και διασφαλίζει ότι το αποτέλεσμα ανταποκρίνεται σε επαγγελματικά, οργανωσιακά και επικοινωνιακά πρότυπα.

Πριν την κοινοποίηση, επιβεβαιώστε ότι το περιεχόμενό σας είναι:

- ✓ **Σαφές** → εύκολα κατανοητό, χωρίς ασάφειες
- ✓ **Ακριβές** → σωστό, επαληθευμένο και ενημερωμένο
- ✓ **Δομημένο** → λογικά οργανωμένο με ξεκάθαρη ροή
- ✓ **Κατάλληλο για το κοινό** → ο τόνος και το επίπεδο προσαρμόζονται στο κοινό-στόχο

Αυτοαξιολόγηση (Επαγγελματικός Έλεγχος)

- Χρησιμοποιώ πρότυπα και δομημένες μορφές ή τυχαία μορφοποίηση;
- Μπορώ να παρουσιάσω πληροφορίες με σαφή και λογικό τρόπο;
- Επαληθεύω πηγές, δεδομένα και δικαιώματα πριν από τη χρήση;
- Είναι το περιεχόμενό μου προσβάσιμο και κατανοητό από άλλους;
- Ακολουθώ μια διαδικασία τελικού ελέγχου πριν την κοινοποίηση;

Σενάριο Περίπτωσης: Κακό vs Επαγγελματικό Περιεχόμενο

Ο Νίκος εργάζεται σε μια μικρή εταιρεία και του ανατίθεται να ετοιμάσει μια παρουσίαση για πελάτη σχετικά με μια νέα υπηρεσία.

Δημιουργεί την παρουσίαση με τον εξής τρόπο:

- Αντιγράφει κείμενο απευθείας από διαφορετικές πηγές
- Χρησιμοποιεί ΤΝ για τη δημιουργία διαφανειών χωρίς επεξεργασία
- Προσθέτει υπερβολικό κείμενο σε κάθε διαφάνεια
- Χρησιμοποιεί ασυνεπείς γραμματοσειρές, χρώματα και διάταξη
- Ενσωματώνει εικόνες χωρίς έλεγχο πνευματικών δικαιωμάτων

Η παρουσίαση παραδίδεται στην ώρα της.

Τι συμβαίνει στη συνέχεια:

- Ο πελάτης τη βρίσκει συγκεχυμένη και δύσκολη στην κατανόηση
- Ορισμένες πληροφορίες φαίνονται ανακριβείς ή άσχετες
- Ο οπτικός σχεδιασμός δείχνει αντιεπαγγελματικός
- Η αξιοπιστία της εταιρείας μειώνεται

Ανάλυση Σεναρίου: Τι Έπρεπε να Είχε Γίνει;

1. Έλλειψη Δομής

- Δεν υπάρχει σαφές μήνυμα ή ροή
- Υπερβολική πληροφορία σε κάθε διαφάνεια
- ✓ Ορθή Πρακτική: Μία ιδέα ανά διαφάνεια + λογική ακολουθία

2. Κακή Χρήση Τεχνητής Νοημοσύνης

- Χρήση περιεχομένου TN χωρίς επαλήθευση
- Καμία προσαρμογή στο πλαίσιο
- ✓ Ορθή Πρακτική: TN = προσχέδιο → Άνθρωπος = βελτίωση + επικύρωση

3. Κακός Οπτικός Σχεδιασμός

- Ασυνεπής μορφοποίηση
- Υπερφορτωμένες διαφάνειες
- ✓ Ορθή Πρακτική: Χρήση προτύπων + οπτική ιεραρχία

4. Ηθικά Ζητήματα

- Μη επαληθευμένο περιεχόμενο
- Πιθανές παραβιάσεις πνευματικών δικαιωμάτων
- ✓ Ορθή Πρακτική: Χρήση αδειοδοτημένου υλικού + έλεγχος ακρίβειας

Επίλυση Βασικών Τεχνικών Προβλημάτων

Ενότητα 6



Co-funded by
the European Union

Το Κόστος των Τεχνικών Προβλημάτων

Τα τεχνικά προβλήματα επηρεάζουν άμεσα την παραγωγικότητα, τη ροή εργασίας και τη συνολική απόδοση ενός οργανισμού.

Αρνητικές επιπτώσεις:

- Απώλεια παραγωγικότητας
- Καθυστερήσεις σε προθεσμίες
- Απογοήτευση και άγχος
- Αρνητικός αντίκτυπος στη φήμη

Παράδειγμα:

Ένα αρχείο δεν συγχρονίζεται σωστά → αποστέλλεται λάθος έκδοση στον πελάτη → επηρεάζεται η ακρίβεια και η εμπιστοσύνη

Ακόμη και μικρά τεχνικά προβλήματα μπορούν να οδηγήσουν σε σημαντικές επιχειρησιακές συνέπειες.

Τύποι Συνηθισμένων Τεχνικών Προβλημάτων

Τα περισσότερα τεχνικά προβλήματα στον χώρο εργασίας ανήκουν σε συγκεκριμένες κατηγορίες, οι οποίες μπορούν να εντοπιστούν και να αντιμετωπιστούν συστηματικά.

Κύριες Κατηγορίες

- **Προβλήματα Συνδεσιμότητας** → ζητήματα με το διαδίκτυο, το Wi-Fi ή την πρόσβαση μέσω VPN
- **Προβλήματα Πρόσβασης** → σφάλματα σύνδεσης, περιορισμοί δικαιωμάτων, ζητήματα λογαριασμού
- **Σφάλματα Λογισμικού** → «κρashaρίσματα» εφαρμογών, bugs ή προβλήματα απόδοσης
- **Προβλήματα Δεδομένων** → αρχεία που λείπουν, προβλήματα συγχρονισμού, συγκρούσεις εκδόσεων

Παράδειγμα:

Ένας χρήστης δεν μπορεί να αποκτήσει πρόσβαση σε ένα κοινόχρηστο έγγραφο → το πρόβλημα μπορεί να σχετίζεται με δικαιώματα, συγχρονισμό ή συνδεσιμότητα

Αν μπορείτε να κατηγοριοποιήσετε το πρόβλημα, μπορείτε να το λύσετε πιο γρήγορα.

Η Νοοτροπία Επίλυσης Προβλημάτων

Η αποτελεσματική επίλυση τεχνικών προβλημάτων απαιτεί λογική σκέψη και δομημένη προσέγγιση.

Βασικές Αρχές

- Ψύχραιμη σκέψη
- Βήμα-βήμα λογική
- Αποφυγή υποθέσεων

Λανθασμένη Προσέγγιση

- Τυχαία κλικ
- Δοκιμή χωρίς σχέδιο (trial-and-error)

Ορθή Προσέγγιση

- Δομημένη διάγνωση
- Ελεγχόμενες δοκιμές

Παράδειγμα: Τυχαία αλλαγή ρυθμίσεων → το πρόβλημα επιδεινώνεται

Οι εικασίες δημιουργούν περισσότερα προβλήματα — η λογική τα επιλύει.

Η Βασική Λογική Επίλυσης Προβλημάτων

Βήμα προς Βήμα Διαδικασία

1. Εντοπίστε ξεκάθαρα το πρόβλημα
2. Ελέγξτε τις βασικές αιτίες (σύνδεση, πρόσβαση, σύστημα)
3. Δοκιμάστε λύσεις βήμα προς βήμα
4. Επιβεβαιώστε ότι το πρόβλημα επιλύθηκε

Παράδειγμα:

Δεν ανοίγει ένα αρχείο → έλεγχος πρόσβασης → δοκιμή εναλλακτικής λύσης → επιβεβαίωση αποκατάστασης

Να ξεκινάτε πάντα από τα απλά πριν προχωρήσετε σε πιο σύνθετες λύσεις.

Ο Κανόνας RRU (Restart – Reconnect – Update)

Πολλά τεχνικά προβλήματα μπορούν να επιλυθούν με απλές βασικές ενέργειες στο σύστημα.

Βασικές Ενέργειες

- **Επανεκκίνηση (Restart)** → καθαρίζει προσωρινά προβλήματα μνήμης και «κολλήματα»
- **Επανασύνδεση (Reconnect)** → αποκαθιστά τη σύνδεση στο δίκτυο
- **Ενημέρωση (Update)** → διορθώνει σφάλματα και βελτιώνει τη συμβατότητα

Παράδειγμα:

Μια εφαρμογή δεν ανταποκρίνεται → επανεκκίνηση → το πρόβλημα επιλύεται

Οι απλές λύσεις επιλύουν τα περισσότερα προβλήματα.

Διάγνωση Πριν την Ενέργεια – Ρώτησε πριν Διορθώσεις

Βασικές Ερωτήσεις

- Τι άλλαξε;
- Πότε ξεκίνησε το πρόβλημα;
- Επηρεάζει μόνο εμένα ή είναι γενικό;

Παράδειγμα:

Αν επηρεάζεται μόνο ένας χρήστης → πιθανό τοπικό πρόβλημα

Αν επηρεάζονται πολλοί χρήστες → πιθανό πρόβλημα συστήματος

Υλικό vs Λογισμικό vs Δίκτυο (Hardware vs Software vs Network)

Διάκριση

- **Υλικό (Hardware – Το Φυσικό)** → Είναι τα απτά στοιχεία που μπορείτε να αγγίξετε, όπως καλώδια, συσκευές, οθόνες και περιφερειακά (ποντίκι, πληκτρολόγιο).
- **Λογισμικό (Software – Το Ψηφιακό)** → Είναι οι εφαρμογές, τα λειτουργικά συστήματα και τα προγράμματα που εκτελούνται πάνω στο υλικό.
- **Δίκτυο (Network – Το «Αόρατο»)** → Είναι η σύνδεση που ενώνει τις συσκευές σας με τα εσωτερικά συστήματα της εταιρείας ή το διαδίκτυο.

Παράδειγμα:

Το ποντίκι δεν λειτουργεί → ελέγξτε πρώτα το καλώδιο ή την μπαταρία (Υλικό)

Το «μυστικό» της επαγγελματικής επίλυσης προβλημάτων είναι η απομόνωση. Ελέγχοντας μία κατηγορία κάθε φορά (Υλικό, Λογισμικό, Δίκτυο), μπορείτε να εντοπίσετε με ακρίβεια την αιτία του προβλήματος.

Επίλυση Προβλημάτων Συνδεσιμότητας

Έλεγχοι που Πρέπει να Πραγματοποιήσετε

- Σύνδεση στο Διαδίκτυο → Ξεκινήστε από την πηγή. Είναι εκτός λειτουργίας όλο το δίκτυο ή μόνο η δική σας συσκευή; Ελέγξτε αν φορτώνουν άλλες ιστοσελίδες ή αν αντιμετωπίζουν το ίδιο πρόβλημα και οι συνάδελφοί σας.
- Κατάσταση Wi-Fi → Βεβαιωθείτε ότι το Wi-Fi είναι ενεργοποιημένο. Μερικές φορές, μια απλή απενεργοποίηση και επανενεργοποίηση αρκεί για να επανασυνδεθεί στη σωστή σύνδεση.
- Κατάσταση Router → Αν εργάζεστε από το σπίτι ή μικρό γραφείο, ελέγξτε τη συσκευή. Τα φωτάκια είναι πράσινα; Ένα κόκκινο ή αναβοσβήνον φως συνήθως δείχνει πρόβλημα σύνδεσης ή ανάγκη επανεκκίνησης
- Ρυθμίσεις VPN → Για πολλούς επαγγελματίες, το VPN είναι το τελευταίο «φίλτρο». Αν το internet λειτουργεί αλλά όχι τα εταιρικά εργαλεία, πιθανόν το VPN να έχει αποσυνδεθεί ή «λήξει». Αποσυνδεθείτε και συνδεθείτε ξανά.

Παράδειγμα:

Προσπαθείτε να ανοίξετε μια cloud αναφορά και εμφανίζεται μήνυμα «No Internet». Αντί να καλέσετε άμεσα την τεχνική υποστήριξη, ελέγχετε το router, βλέπετε ότι αναβοσβήνει και κάνετε επανεκκίνηση. Μέσα σε λίγα λεπτά, η σύνδεση αποκαθίσταται χωρίς εξωτερική βοήθεια.

Προκλήσεις Απομακρυσμένης Συνδεσιμότητας

Ζητήματα

- Αδύναμο Wi-Fi στο σπίτι → Η απόσταση από το router, τα φυσικά εμπόδια ή η υψηλή χρήση από άλλες συσκευές μπορούν να προκαλέσουν καθυστερήσεις σε βιντεοκλήσεις ή αργή μεταφορά αρχείων
- Αστάθεια VPN → Τα εταιρικά VPN είναι απαραίτητα για την ασφάλεια, αλλά μπορεί να παρουσιάζουν αποσυνδέσεις λόγω ασυμβατότητας με τον πάροχο internet ή το δίκτυο
- Κίνδυνοι δημόσιων δικτύων → Τα Wi-Fi σε καφετέριες ή αεροδρόμια συχνά δεν είναι ασφαλή, εκθέτοντας δεδομένα σε υποκλοπές και κυβερνοεπιθέσεις

Ορθή Πρακτική

- Χρήση ασφαλών δικτύων → Προτιμάτε πάντα το προστατευμένο οικιακό σας δίκτυο. Διασφαλίστε ότι το router είναι ενημερωμένο και τοποθετημένο σε κεντρικό σημείο
- Αποφυγή δημόσιου Wi-Fi για ευαίσθητα δεδομένα → Μην έχετε πρόσβαση σε εταιρικά ή προσωπικά δεδομένα μέσω μη ασφαλών δικτύων. Αν είναι απαραίτητο, χρησιμοποιείτε πάντα VPN
- Χρήση mobile hotspot ως εναλλακτική → Σε περίπτωση διακοπής του internet, το hotspot του κινητού αποτελεί ασφαλή και αξιόπιστη λύση

Συνδεσιμότητα = επαγγελματική αξιοπιστία

Επίλυση Προβλημάτων Πρόσβασης – Δικαιώματα και Πιστοποίηση (Authentication)

Τα προβλήματα πρόσβασης εμφανίζονται όταν οι χρήστες δεν μπορούν να εισέλθουν σε συστήματα, αρχεία ή πλατφόρμες λόγω ζητημάτων πιστοποίησης ή δικαιωμάτων.

Συνήθως σχετίζονται με τα εξής:

- Λανθασμένα δικαιώματα (Permissions) → είναι η πιο συχνή αιτία. Μπορεί να έχετε το link ενός αρχείου, αλλά να μην έχετε τα απαραίτητα δικαιώματα προβολής ή επεξεργασίας.
- Ληγμένη σύνδεση (Expired Login) → για λόγους ασφάλειας, τα συστήματα απαιτούν περιοδική επανασύνδεση. Αν έχετε αφήσει μια εφαρμογή ανοιχτή για ώρες ή ημέρες, η συνεδρία πιθανόν έχει λήξει.
- Λάθος λογαριασμός (Wrong Account) → η χρήση πολλαπλών λογαριασμών (προσωπικός, εταιρικός, πελάτη) μπορεί να δημιουργήσει σύγχυση. Αν είστε συνδεδεμένοι με λάθος προφίλ, η πρόσβαση θα απορριφθεί.

Παράδειγμα:

Ένας χρήστης δεν μπορεί να ανοίξει ένα κοινόχρηστο αρχείο → το αρχείο υπάρχει, αλλά δεν έχουν δοθεί τα κατάλληλα δικαιώματα πρόσβασης.

Τα περισσότερα προβλήματα πρόσβασης δεν είναι τεχνικές βλάβες, αλλά ζητήματα δικαιωμάτων και διαχείρισης λογαριασμών.

Διαχείριση Προβλημάτων Cloud & Συγχρονισμού

Τα συστήματα cloud βασίζονται στον συνεχή συγχρονισμό μεταξύ της τοπικής συσκευής και του online αποθηκευτικού χώρου.

Συνηθισμένα Προβλήματα

- Αρχεία που δεν ενημερώνονται
- Συγκρούσεις εκδόσεων (διπλές εκδόσεις αρχείων)
- Απώλεια ή μη εμφάνιση δεδομένων

Ορθή Πρακτική

- Ελέγχετε την κατάσταση συγχρονισμού (sync status)
- Χρησιμοποιείτε κοινόχρηστες εκδόσεις αντί για τοπικά αντίγραφα
- Αποφεύγετε τη δημιουργία διπλών αρχείων

Το «αποθηκεύτηκε» δεν σημαίνει πάντα «συγχρονίστηκε».

Βαθύτερη Κατανόηση Συγχρονισμού Cloud – Αναγνώριση Ενδείξεων Συγχρονισμού

Τα συστήματα cloud χρησιμοποιούν οπτικές ενδείξεις για να δείξουν την κατάσταση των αρχείων.

Ενδείξεις Συγχρονισμού

- Μπλε εικονίδιο → συγχρονισμός σε εξέλιξη
- Πράσινο check → πλήρως συγχρονισμένο
- Κόκκινο σφάλμα → πρόβλημα συγχρονισμού

Παράδειγμα: Κλείσιμο του υπολογιστή πριν ολοκληρωθεί ο συγχρονισμός → το αρχείο δεν ενημερώνεται

Κίνδυνοι

- Απώλεια δεδομένων
- Χρήση παλιάς έκδοσης
- Έλλειψη αρχείων

Ορθή Πρακτική

- Επιβεβαιώνετε την ολοκλήρωση του συγχρονισμού πριν κλείσετε την εργασία
- Παρακολουθείτε και διορθώνετε άμεσα τυχόν σφάλματα συγχρονισμού

Κατανόηση Σφαλμάτων Λογισμικού

Τα σφάλματα λογισμικού εμφανίζονται συνήθως λόγω περιορισμών του συστήματος ή μη ενημερωμένων εφαρμογών.

Συνηθισμένες Αιτίες

- Μη ενημερωμένο λογισμικό
- Υπερφόρτωση συστήματος
- Προβλήματα συμβατότητας

Παράδειγμα: Μια εφαρμογή «κρασάρει» → η έκδοση δεν είναι συμβατή με το σύστημα

Κίνδυνοι

- Διακοπή εργασίας
- Απώλεια δεδομένων
- Μείωση παραγωγικότητας

Ορθή Πρακτική

- Ενημερώνετε τακτικά το λογισμικό
- Κλείνετε περιττές εφαρμογές
- Κάνετε επανεκκίνηση του συστήματος όταν χρειάζεται

Τα περισσότερα προβλήματα λογισμικού είναι προβλέψιμα και μπορούν να προληφθούν.

Αντιμετώπιση Προβλημάτων Περιφερειακών – Συσκευές & Υλικό

Πολλά τεχνικά προβλήματα προέρχονται από φυσικές συσκευές και όχι από το λογισμικό.

Βασικοί Έλεγχοι

- Καλώδια → Βεβαιωθείτε ότι είναι σωστά συνδεδεμένα
- Τροφοδοσία → Ελέγξτε αν η συσκευή είναι ενεργοποιημένη
- Drivers → Επιβεβαιώστε ότι είναι εγκατεστημένοι και ενημερωμένοι

Παράδειγμα:

Στέλνετε ένα έγγραφο στον εκτυπωτή, αλλά δεν συμβαίνει τίποτα. Αντί να ελέγξετε αμέσως τις ρυθμίσεις του αρχείου, κάνετε επανεκκίνηση της συσκευής και ελέγχετε τα καλώδια. Συχνά, αυτό το «φυσικό reset» αποκαθιστά την επικοινωνία και ο εκτυπωτής λειτουργεί κανονικά.

Πολλά προβλήματα είναι φυσικά, όχι ψηφιακά. Ξεκινάτε πάντα από τους απλούς, πρακτικούς ελέγχους πριν προχωρήσετε σε πιο σύνθετες λύσεις.

Προληπτική Συντήρηση – Αποφυγή Προβλημάτων πριν Εμφανιστούν

Ενέργειες

- **Τακτικές ενημερώσεις συστήματος** → Οι ενημερώσεις δεν αφορούν μόνο νέες λειτουργίες· περιλαμβάνουν κρίσιμα patches ασφαλείας και βελτιώσεις απόδοσης. Η καθυστέρησή τους είναι σαν να αφήνετε «ξεκλείδωτη» την ψηφιακή σας εργασία.
- **Οργάνωση αρχείων** → Ένα χαοτικό desktop και μια ασύντακτη δομή φακέλων δεν καθυστερούν μόνο εσάς αλλά και το σύστημα. Η σωστή οργάνωση μειώνει το φορτίο και βελτιώνει την αποδοτικότητα.
- **Καθαρισμός αποθηκευτικού χώρου** → Η ύπαρξη πολλών άχρηστων αρχείων επιβαρύνει το σύστημα και μειώνει την απόδοση. Διατηρείτε μόνο τα απαραίτητα και αρχειοθετείτε τα υπόλοιπα.

Παράδειγμα: Συγκρίνετε δύο εργαζόμενους. Ο ένας έχει 500 αρχεία στο desktop χωρίς οργάνωση, ενώ ο άλλος χρησιμοποιεί δομημένους φακέλους. Ο δεύτερος βρίσκει πιο γρήγορα τις πληροφορίες, κάνει λιγότερα λάθη και εργάζεται με λιγότερη πίεση.

Οργανωμένα αρχεία → ταχύτερη πρόσβαση → λιγότερα λάθη

Η πρόληψη είναι πιο αποδοτική από την επιδιόρθωση.

Ψηφιακή Υγιεινή

Η ψηφιακή υγιεινή αναφέρεται στη σωστή συντήρηση των συστημάτων, ώστε να διασφαλίζεται η βέλτιστη απόδοση και η σταθερή λειτουργία τους.

Βασικές Πρακτικές

- **Αφαίρεση περιττών αρχείων** → Ελέγχετε τακτικά τους φακέλους «Downloads» και «Desktop». Διαγράψτε προσωρινά αρχεία, παλιά installations και έγγραφα που δεν χρειάζεστε. Αν δεν έχετε ανοίξει ένα αρχείο για μεγάλο χρονικό διάστημα, εξετάστε την αρχειοθέτηση ή διαγραφή του.
- **Διαχείριση αποθηκευτικού χώρου** → Το σύστημα χρειάζεται ελεύθερο χώρο για να λειτουργεί σωστά. Αν ο δίσκος είναι σχεδόν γεμάτος, μειώνεται η απόδοση. Διατηρείτε τουλάχιστον 15% ελεύθερο χώρο.
- **Απενεργοποίηση εφαρμογών εκκίνησης** → Πολλά προγράμματα ξεκινούν αυτόματα με την εκκίνηση του υπολογιστή, καταναλώνοντας μνήμη (RAM) χωρίς λόγο. Απενεργοποιήστε όσα δεν χρειάζεστε.

Παράδειγμα:

Πολλές εφαρμογές στην εκκίνηση → αργό σύστημα

Τα «καθαρά» και οργανωμένα συστήματα λειτουργούν πιο γρήγορα, πιο σταθερά και με λιγότερα προβλήματα.

Αντίγραφα Ασφαλείας & Προστασία Δεδομένων

Τα αντίγραφα ασφαλείας (backups) διασφαλίζουν ότι τα δεδομένα μπορούν να ανακτηθούν σε περίπτωση βλάβης ή απώλειας.

Βασικές Πρακτικές

- **Τακτική Αποθήκευση (Save Regularly):** Μην βασίζεστε μόνο στο “Autosave”. Αποθηκεύετε χειροκίνητα την εργασία σας σε τακτά διαστήματα, ιδιαίτερα σε φυσικά σημεία παύσης. Έτσι, ακόμη και σε περίπτωση διακοπής ρεύματος, η απώλεια περιορίζεται σε λίγα λεπτά εργασίας.
- **Χρήση Cloud Backup:** Πλατφόρμες όπως OneDrive, Google Drive ή Dropbox λειτουργούν ως συνεχές «δίκτυ ασφαλείας». Αποθηκεύοντας αρχεία σε αυτές, διατηρούνται αυτόματα αντίγραφα σε απομακρυσμένους servers.
- **Διατήρηση Τοπικών Αντιγράφων:** Για κρίσιμα έργα, εφαρμόστε τον κανόνα “3-2-1”: 3 αντίγραφα δεδομένων, 2 διαφορετικά μέσα αποθήκευσης, 1 αντίγραφο εκτός τοποθεσίας (cloud) Ένα τοπικό backup (π.χ. σε εξωτερικό δίσκο) σας επιτρέπει να συνεχίσετε να εργάζεστε ακόμη και χωρίς internet.

Παράδειγμα:

Ο υπολογιστής σας καταρρέει μία ώρα πριν από μια σημαντική προθεσμία. Επειδή έχετε κρατήσει αντίγραφα ασφαλείας, συνδέεστε από άλλη συσκευή και επαναφέρετε το αρχείο. Αυτό που θα μπορούσε να είναι καταστροφή μετατρέπεται σε μια μικρή καθυστέρηση λίγων λεπτών.

Η απώλεια δεδομένων ισοδυναμεί με απώλεια εργασίας και αξιοπιστίας. Χαμένες ώρες, καθυστερήσεις και μειωμένη εμπιστοσύνη πελατών έχουν πάντα μεγαλύτερο κόστος από την πρόληψη.

Στη σύγχρονη δημιουργία περιεχομένου, τα backups δεν είναι προαιρετικά—είναι απαραίτητα.

Στρατηγική Αντιγράφων Ασφαλείας (Κανόνας 3-2-1)

Για να επιτύχετε πλήρη ασφάλεια δεδομένων, η στρατηγική σας πρέπει να βασίζεται στον κανόνα 3-2-1:

- **3 Αντίγραφα Δεδομένων:** Πρέπει να έχετε τουλάχιστον τρία αντίγραφα: το αρχικό αρχείο στο οποίο εργάζεστε και δύο επιπλέον αντίγραφα ασφαλείας.
- **2 Διαφορετικά Μέσα Αποθήκευσης:** Μην αποθηκεύετε όλα τα αντίγραφα στο ίδιο μέσο. Χρησιμοποιήστε δύο διαφορετικούς τύπους αποθήκευσης, όπως ο εσωτερικός δίσκος του υπολογιστή και ένας εξωτερικός δίσκος. Έτσι προστατεύετε σε περίπτωση βλάβης εξοπλισμού.
- **1 Αντίγραφο Εκτός Τοποθεσίας (Off-site):** Τουλάχιστον ένα αντίγραφο πρέπει να βρίσκεται σε διαφορετική τοποθεσία—συνήθως στο cloud. Αυτό διασφαλίζει ότι ακόμη και σε περιπτώσεις όπως κλοπή, φωτιά ή φυσική καταστροφή, τα δεδομένα σας παραμένουν ασφαλή.

Παράδειγμα:

Ένα αρχείο αποθηκεύεται στον τοπικό υπολογιστή, ένα αντίγραφο σε εξωτερικό SSD και ένα τρίτο συγχρονίζεται στο cloud (π.χ. OneDrive ή Dropbox).

Η αποτυχία είναι αναπόφευκτη — η προετοιμασία αποτρέπει την καταστροφή.

Ανθρώπινος Παράγοντας στα Τεχνικά Προβλήματα

Ο ανθρώπινος παράγοντας αποτελεί συχνά τη βασική αιτία πίσω από τα τεχνικά προβλήματα.

Κύριες Αιτίες

Most "user errors" can be traced back to three psychological states:

- **Βιασύνη (Rushing)** → Η πίεση χρόνου οδηγεί στην παράλειψη βασικών βημάτων, όπως ο έλεγχος συγχρονισμού ή η επιβεβαίωση του σωστού αρχείου.
- **Διάσπαση Προσοχής (Distraction)** → Το multitasking ή ένα ακατάστατο περιβάλλον αυξάνει την πιθανότητα λανθασμένων ενεργειών, όπως λάθος κλικ ή διαγραφή αρχείων.
- **Παρεξήγηση (Misunderstanding)** → Η χρήση εργαλείων χωρίς κατανόηση της λειτουργίας τους οδηγεί σε προβλέψιμα λάθη και αποτυχίες.

Παράδειγμα:

- Κλικ σε λάθος αρχείο → αντικατάσταση δεδομένων
- Οι άνθρωποι συχνά δημιουργούν τεχνικά προβλήματα
- Η τεχνολογία μπορεί να αποτύχει — αλλά η ανθρώπινη συμπεριφορά είναι συχνά ο βασικός παράγοντας που τα προκαλεί

Επικοινωνία Τεχνικών Προβλημάτων

Η σαφής επικοινωνία μειώνει σημαντικά τον χρόνο επίλυσης τεχνικών προβλημάτων.

Τι Πρέπει να Περιλαμβάνει η Αναφορά

- **Περιγραφή Προβλήματος (Problem Description):** Να είστε συγκεκριμένοι. Αντί για «δεν μπορώ να συνδεθώ», πείτε: «Εμφανίζεται μήνυμα “Error 404” όταν προσπαθώ να μπω στο Client Portal». Περιγράψτε ακριβώς τι βλέπετε στην οθόνη.
- **Ενέργειες που Έχουν Ήδη Γίνει (Actions Already Taken):** Αναφέρετε τι έχετε ήδη δοκιμάσει. Για παράδειγμα, αν εφαρμόσατε τον κανόνα RRU (Restart, Reconnect, Update), δηλώστε το. Αυτό αποτρέπει επανάληψη ενεργειών και εξοικονομεί χρόνο.
- **Screenshots ή Αποδείξεις (Evidence):** Μια εικόνα βοηθά σημαντικά στη διάγνωση. Καταγράψτε το μήνυμα σφάλματος ή το πρόβλημα όπως εμφανίζεται.

Παράδειγμα:

- “Δεν μπορώ να ανοίξω το αρχείο – έχω ελέγξει σύνδεση και δικαιώματα πρόσβασης”
- Σαφής αναφορά = ταχύτερη λύση.

Πρωτόκολλα Κλιμάκωσης (Escalation Protocols)

Η κλιμάκωση αποτελεί βασικό μέρος της επαγγελματικής επίλυσης προβλημάτων.

Πότε να Κλιμακώσετε

- Δεν μπορείτε να επιλύσετε το πρόβλημα
- Το πρόβλημα επηρεάζει πολλούς χρήστες
- Αφορά ευαίσθητα ή κρίσιμα δεδομένα

Κανόνας των 30 Λεπτών

Αν δεν μπορείτε να λύσετε ένα τεχνικό πρόβλημα μέσα σε 30 λεπτά συγκεντρωμένης προσπάθειας, σταματήστε. Η συνέχιση πέρα από αυτό το σημείο συνήθως οδηγεί σε χαμένο χρόνο και μειωμένη παραγωγικότητα.

Το να γνωρίζετε πότε να σταματήσετε και να ζητήσετε βοήθεια είναι επαγγελματική δεξιότητα. Η σωστή κλιμάκωση επιταχύνει τη λύση και προστατεύει τον χρόνο και την απόδοσή σας.

Επικοινωνία με το τμήμα Πληροφορικής – Σύνταξη μιας Σαφούς Αναφοράς Περιστατικού

Τι πρέπει να περιλαμβάνει η αναφορά:

- **Σύστημα/Περιβάλλον** (System/Environment)
- **Ενέργεια που επιχειρήθηκε** (Action attempted)
- **Μήνυμα σφάλματος** (Error message)
- **Ενέργειες που έγιναν** (Steps taken)

Παράδειγμα

«Windows 11 – αδυναμία μεταφόρτωσης αρχείου – σφάλμα 404 – έγινε προσπάθεια επανεκκίνησης»

Η σαφής αναφορά ισοδυναμεί με ταχύτερες λύσεις. Μετατρέπει ένα εκνευριστικό τεχνικό κόλλημα σε μια απλοποιημένη διοικητική εργασία.

Σενάριο Περίπτωσης – Αποτυχία Συστήματος

Σενάριο

Ο χρήστης δεν έχει πρόσβαση σε κοινόχρηστα αρχεία πριν από τη λήξη μιας προθεσμίας

Η Αλυσιδωτή Αντίδραση

- **Πανικός:** Ο χρήστης βιώνει «ψηφιακό πανικό», χάνοντας την ικανότητα να σκέφτεται καθαρά ή να διαγνώσει το πρόβλημα.
- **Τυχαίες Ενέργειες:** Χωρίς σχέδιο, αρχίζει να αλλάζει τυχαίες ρυθμίσεις, να κάνει κλικ σε διάφορα μενού και να αποσυνδέει καλώδια.
- **Διαγραφή Αρχείων:** Σε μια λανθασμένη προσπάθεια να «ελευθερώσει χώρο» ή να «επαναφέρει» τον φάκελο, αρχίζει να διαγράφει αρχεία, ελπίζοντας ότι αυτό θα διορθώσει τη σύνδεση.

Οι συνέπειες αυτών των ενεργειών ξεπερνούν κατά πολύ ένα απλό ζήτημα πρόσβασης:

- **Απώλεια Δεδομένων:** Οι τυχαίες διαγραφές οδηγούν σε μόνιμη απώλεια εργασίας.
- **Σημαντικές Καθυστερήσεις:** Ο χρόνος που δαπανήθηκε σε τυχαίες ενέργειες ήταν χρόνος που θα μπορούσε να είχε χρησιμοποιηθεί για σωστή αντιμετώπιση προβλημάτων ή κλιμάκωση του ζητήματος.
- **Αναστάτωση Ομάδας:** Οι συνάδελφοι πρέπει τώρα να σταματήσουν τη δική τους εργασία για να βοηθήσουν στην ανάκτηση όσων χάθηκαν, επηρεάζοντας την απόδοση ολόκληρου του τμήματος.

Οι κακές αποφάσεις υπό πίεση αυξάνουν τη ζημιά.

Ανάλυση Σεναρίου

Βήματα

- ✓ έλεγχος σύνδεσης
- ✓ επαλήθευση πρόσβασης
- ✓ έλεγχος συγχρονισμού
- ✓ αποφυγή καταστροφικών ενεργειών

Ορθή Πρακτική

- ενεργήστε λογικά
- αποφύγετε μη αναστρέψιμες ενέργειες

Η ψύχραιμη λογική αποτρέπει την κλιμάκωση.

Λίστα Ελέγχου Αντιμετώπισης Προβλημάτων

Ο Τελικός Έλεγχος 5 Βημάτων

- ✓ επανεκκίνηση
- ✓ έλεγχος σύνδεσης
- ✓ επαλήθευση πρόσβασης
- ✓ έλεγχος ενημερώσεων
- ✓ δοκιμή απλών λύσεων

Η ψηφιακή ανθεκτικότητα είναι μια βασική επαγγελματική δεξιότητα.

Κύρια σημεία

1. Ψηφιακή Ασφάλεια

1. Προστατεύει τα δεδομένα, τα συστήματα και την εμπιστοσύνη.
2. Κύριοι κίνδυνοι: Phishing (Ηλεκτρονικό ψάρεμα), Κακόβουλο λογισμικό (Malware), Κοινωνική Μηχανική (Social Engineering), Αδύναμη Ταυτοποίηση.

2. GDPR & Διαχείριση Δεδομένων

1. Η τήρηση του GDPR είναι κρίσιμη για την προστασία των προσωπικών δεδομένων και τη νομική συμμόρφωση.
2. Απαιτούνται ασφαλείς πρακτικές χειρισμού και αποθήκευσης.

3. Ταυτοποίηση & Προστασία Συσκευών

1. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) και η ασφάλεια των συσκευών είναι ζωτικής σημασίας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
2. Οι τακτικές ενημερώσεις και η κρυπτογράφηση είναι απαραίτητες για την προστασία των συσκευών.

4. Διαχείριση Αρχείων

1. Οργανώστε τα αρχεία με σαφείς δομές για την αποφυγή απώλειας ή μη εξουσιοδοτημένης πρόσβασης.
2. Χρησιμοποιήστε ελεγχόμενη κοινή χρήση αρχείων και μέτρα προστασίας δεδομένων.

5. Υπευθυνότητα στην Τεχνητή Νοημοσύνη (AI)

1. Χρησιμοποιήστε τα εργαλεία AI υπεύθυνα, διασφαλίζοντας τη συμμόρφωση με τον GDPR και την προστασία των δεδομένων.
2. Επαληθεύστε τα αποτελέσματα της AI για την αποφυγή λαθών και παραπλανητικών αποτελεσμάτων.

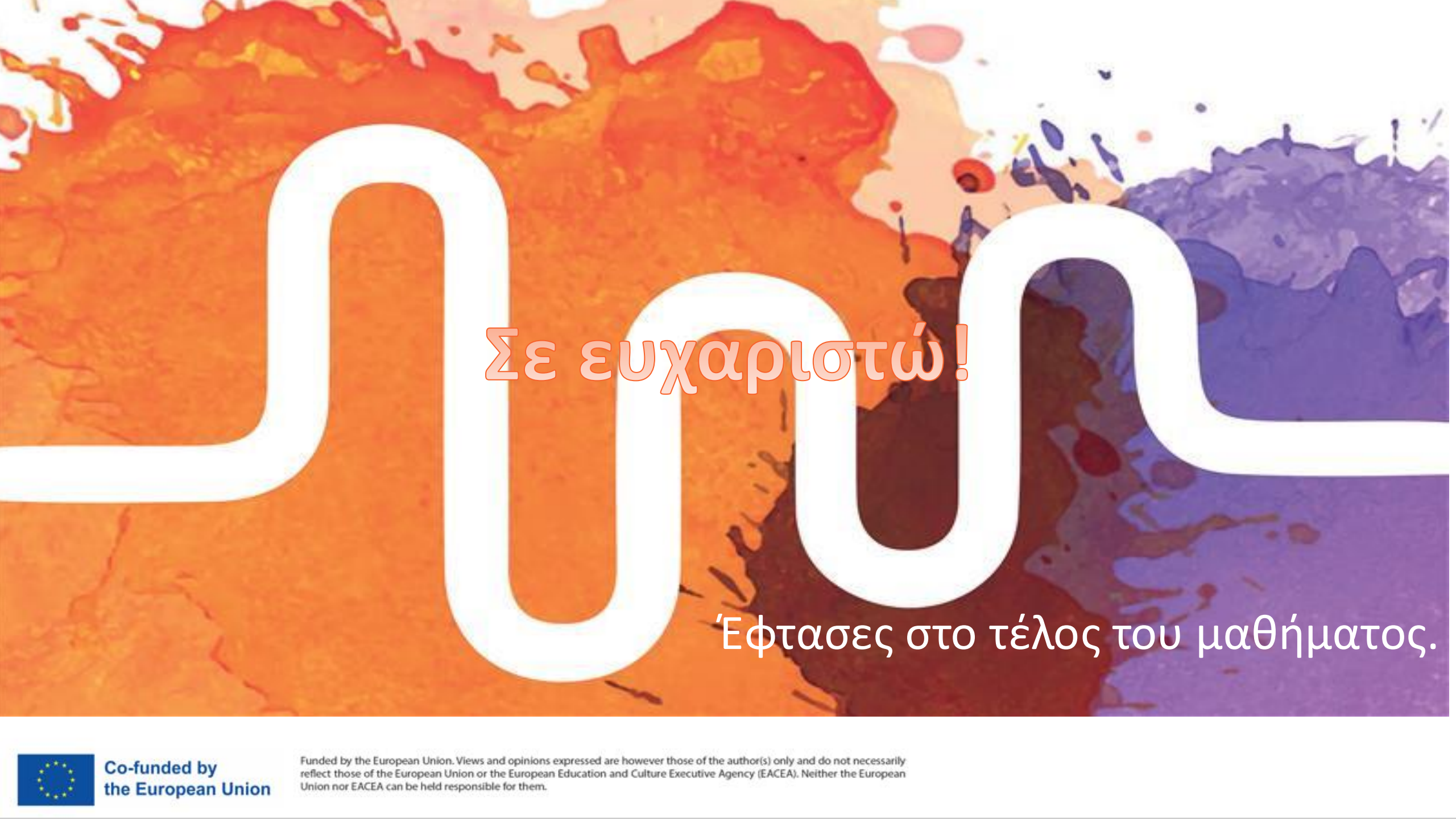
6. Τηλεργασία & Ευεξία

1. Χρησιμοποιήστε ασφαλή δίκτυα και συσκευές για απομακρυσμένη εργασία.
2. Δώστε προτεραιότητα στην ψηφιακή ευεξία για την πρόληψη της υπερφόρτωσης και του στρες.

7. Επίλυση Τεχνικών Προβλημάτων

1. Ακολουθήστε τη λογική «Επανεκκίνηση – Επανασύνδεση – Ενημέρωση» για την αντιμετώπιση προβλημάτων.
2. Η σαφής επικοινωνία με τις ομάδες IT είναι το κλειδί για τη γρήγορη επίλυση ζητημάτων.





Σε ευχαριστώ!

Έφτασες στο τέλος του μαθήματος.



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.