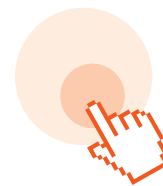


Τεχνητή νοημοσύνη

Κίνδυνοι & πρόληψη



Η σύνδεση του διαδικτύου με την τεχνητή νοημοσύνη (ΤΝ) ανοίγει νέες δυνατότητες, αλλά συνοδεύεται από αυξημένους κινδύνους που αφορούν την ασφάλεια, την ιδιωτικότητα και την αξιοπιστία της πληροφόρησης. Η ενημέρωση, η κριτική σκέψη και η εφαρμογή πρακτικών μέτρων ασφαλείας αποτελούν τα βασικά εργαλεία για την προστασία απέναντι σε αυτούς τους κινδύνους.

1. Παραπληροφόρηση και deepfakes

- **Ψευδείς πληροφορίες:** Η ΤΝ μπορεί να δημιουργεί ρεαλιστικά αλλά ψευδή περιεχόμενα, από άρθρα μέχρι βίντεο. Οι χρήστες πρέπει να επαληθεύουν τις πηγές και να αναζητούν αξιόπιστα μέσα ενημέρωσης.
- **Deepfakes:** Μέσω της ΤΝ είναι πλέον εφικτή η δημιουργία βίντεο ή εικόνων με παραποιημένα πρόσωπα και λόγια, που μπορεί να χρησιμοποιηθούν για παραποίηση της πραγματικότητας ή ακόμη και για σκοπούς εξαπάτησης.

2. Κυβερνοεπιθέσεις και ασφάλεια δεδομένων

- **Phishing και κακόβουλα μηνύματα:** Οι επιτιθέμενοι χρησιμοποιούν τεχνικές που αξιοποιούν την ΤΝ για να δημιουργήσουν πιο πειστικά email ή μηνύματα, προσπαθώντας να αποσπάσουν προσωπικές πληροφορίες ή να εγκαταστήσουν κακόβουλο λογισμικό.
- **Ransomware και hacking:** Η αυτοματοποίηση και οι εξελιγμένες τεχνικές ανίχνευσης αδυναμιών καθιστούν τις επιθέσεις πιο σύνθετες και μπορούν να στοχεύουν τόσο σε ατομικές, όσο και σε εταιρικές πληροφορίες.

3. Παραβίαση ιδιωτικότητας

- **Ασυμβίβαστη συλλογή δεδομένων:** Οι εφαρμογές ΤΝ συχνά συλλέγουν μεγάλες ποσότητες δεδομένων για να "εκπαιδευτούν" μηχανικά. Είναι σημαντικό οι χρήστες να γνωρίζουν τι δεδομένα μοιράζονται και να αξιοποιούν τις ρυθμίσεις ιδιωτικότητας.
- **Εκμετάλλευση προσωπικών πληροφοριών:** Κακόβουλοι φορείς μπορεί να επωφεληθούν από τη δημόσια πληροφόρηση ή τις αδυναμίες προστασίας για να αποσπάσουν ή να πουλήσουν δεδομένα.

4. Εξάρτηση και αποπροσανατολισμός

- **Υπερβολική αυτοματοποίηση:** Η εξάρτηση από τα συστήματα ΤΝ μπορεί να οδηγήσει σε απώλεια κριτικής σκέψης και ανεξαρτησίας. Είναι καλό να χρησιμοποιούμε τα εργαλεία αυτά υποστηρικτικά και όχι ως πλήρη αντικατάσταση της ανθρώπινης κρίσης.
- **Έλλειψη διαφάνειας:** Τα αλγοριθμικά μοντέλα δεν είναι πάντα πλήρως διαφανή στη λειτουργία τους, γεγονός που μπορεί να δημιουργήσει “μαύρο κουτί” στην ανάλυση των αποφάσεων και να δυσχεράνει την ανίχνευση μεροληψιών ή σφαλμάτων.

5. Αναστρέψιμη τεχνολογική εξάρτηση

- **Εξάρτηση από συγκεκριμένες πλατφόρμες:** Η συγκέντρωση ισχύος σε ορισμένα εργαλεία ΤΝ μπορεί να αυξήσει τον κίνδυνο στην ασφάλεια, όπου μια πιθανή ευπάθεια θα μπορούσε να επηρεάσει μεγάλο αριθμό χρηστών.
- **Επίδραση στην αγορά εργασίας:** Ο ανεξέλεγκτος ψηφιακός μετασχηματισμός με τη χρήση ΤΝ μπορεί να οδηγήσει σε ριζικές αλλαγές στην απασχόληση, με πιθανές κοινωνικές και οικονομικές επιπτώσεις.

6. Προληπτικά μέτρα και βέλτιστες πρακτικές

- **Ενημέρωση και Εκπαίδευση:** Ενημερωθείτε σχετικά με τους νέους κινδύνους και συμμετέχετε στα σεμινάρια ή διαδικτυακά μαθήματα για τον ψηφιακό εγγραμματισμό στο Κέντρο Ψηφιακών Δεξιοτήτων της Περιφέρειας Αττικής.
- **Εγκατάσταση αξιόπιστου λογισμικού ασφαλείας:** Χρησιμοποιήστε ενημερωμένα antivirus, firewalls και άλλες λύσεις ασφαλείας που προστατεύουν τις πληροφορίες σας.
- **Έλεγχος των ρυθμίσεων ιδιωτικότητας:** Αναθεωρήστε τις ρυθμίσεις των λογαριασμών σας στα κοινωνικά δίκτυα και άλλα ψηφιακά εργαλεία για να ελαχιστοποιήσετε την ανεξέλεγκτη συλλογή δεδομένων.
- **Κριτική Αντίληψη:** Πριν διαμοιράσετε ή εμπιστευτείτε ψηφιακό περιεχόμενο, ελέγξτε την αξιοπιστία της πηγής και δείτε αν υπάρχουν ανεξάρτητες επιβεβαιώσεις.

7. Συνεργασία και ενημέρωση από το Κέντρο Ψηφιακών Δεξιοτήτων

- **Κοινή δράση:** Ενημερωθείτε σχεδόν καθημερινά από την κοινότητά μας στο Viber, καθώς και τους ειδικούς στον τομέα για να ανταλλάξετε εμπειρίες, προειδοποιήσεις και βέλτιστες πρακτικές.
- **Ενίσχυση της νομοθεσίας:** Υποστηρίξτε πολιτικές και πρωτοβουλίες που αποσκοπούν στη διασφάλιση της διαφάνειας και της προστασίας ειδικά στις εφαρμογές ΤΝ.