SILWERS

SENIORS ARTIFICIAL INTELLIGENCE LEARNING – WELL EDUCATED AND RISK SECURE

Co-funded by the European Union

Expert fora report

Erasmus+ KA220-ADU – Cooperation partnerships in adult education, Project No: ***2024-1-IS01-KA220-ADU-000256952***

Co-funded by the
European Union

Στόχοι της Επιτροπής

1. Συζήτηση των δυσκολιών και των ανησυχιών που αντιμετωπίζει αυτή η ομάδα με τις νέες τεχνολογίες, μαζί με τον εντοπισμό τομέων εφαρμογής της Τεχνητής Νοημοσύνης και των σχετικών κινδύνων.
2. Εντοπισμός τρεχουσών και μελλοντικών διαδικτυακών απειλών για άτομα άνω των 55 ετών.
3. Παρουσίαση παραδειγμάτων από την πραγματική ζωή περιστατικών και οφελών από τη χρήση της Τεχνητής Νοημοσύνης.
4. Ορισμός κρίσιμων ψηφιακών ικανοτήτων για άτομα ηλικίας 55+ ετών.

Co-funded by the
European Union

Γουινίκι - Πολωνία

Co-funded by the European Union

Οι πιο συχνά αναφερόμενες διαδικτυακές απειλές για άτομα άνω των 55 ετών

Τα άτομα ηλικίας 55 ετών και άνω αντιμετωπίζουν μοναδικές προκλήσεις στον ψηφιακό κόσμο, καθιστώντας τα ευάλωτα σε μια ποικιλία διαδικτυακών απειλών.

Η κατανόηση των πιο συνηθισμένων και επιπτωτικών κινδύνων είναι απαραίτητη για τη βελτίωση της ευαισθητοποίησης και της προστασίας τους στον κυβερνοχώρο.

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Ηλεκτρονικό "ψάρεμα" (phishing) με δόλια email, SMS, συνδέσμους, φωνητικές κλήσεις
- Deepfake επιθέσεις ψεύτικου ήχου/βίντεο, μιμούμενοι την οικογένεια
- Ψεύτικα ηλεκτρονικά καταστήματα και απάτες με πλαστούς ιστότοπους
- Συναισθηματική χειραγώγηση και τακτικές εκφοβισμού κοινωνικής μηχανικής
- Κλοπή ταυτότητας με χρήση κλεμμένων προσωπικών δεδομένων

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Απάτη στους απατεώνες των εγγονιών που προσποιούνται ότι είναι η οικογένεια σε κίνδυνο
- Ψεύτικα αιτήματα βοήθειας μέσω WhatsApp ή Messenger
- Ρομαντικές απάτες και απάτες που βασίζονται σε σχέσεις που χτίστηκαν στο διαδίκτυο
- Ψεύτικες διαφημίσεις με διασημότητες, απάτες επενδύσεων
- Αρχεία και συνημμένα που έχουν μολυνθεί από κακόβουλο λογισμικό και ransomware

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Μη επαληθευμένες εφαρμογές και μη ασφαλείς λήψεις λογισμικού
- Κοινοποίηση ευαίσθητων δεδομένων σε αγνώστους, φωτογραφίες και πληροφορίες
- Χρήση παρωχημένων συσκευών ή λογισμικού
- Μαζικές εξατομικευμένες επιθέσεις με χρήση τεχνητής νοημοσύνης, στοχεύοντας προφίλ χρηστών
- Παραπληροφόρηση για την υγεία ή επικίνδυνες ιατρικές συμβουλές από εργαλεία τεχνητής νοημοσύνης

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Απάτες που εκμεταλλεύονται τον ψηφιακό αποκλεισμό σε δημόσιες και τραπεζικές υπηρεσίες
- Η έλλειψη πρακτικών πολυπαραγοντικής επαλήθευσης ταυτότητας απλοποίησε τους κωδικούς πρόσβασης και τις επαναχρήσεις τους
- Απώλεια πρόσβασης σε κρίσιμες υπηρεσίες λόγω τεχνολογικών αλλαγών, πρόσβαση μόνο μέσω εφαρμογής, περιορισμένες εναλλακτικές λύσεις
- Αυτοματοποιημένη χειραγώγηση των ροών των μέσων κοινωνικής δικτύωσης, παραγωγή παραπληροφόρησης και άγχους
- Κωδικός πρόσβασης, αναγνώριση, βιομετρία, 2FA

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

Οι ειδικοί τόνισαν βασικές ανησυχίες που επηρεάζουν περισσότερο άτομα ηλικίας 55 ετών και άνω κατά την αλληλεπίδρασή τους με τις ψηφιακές τεχνολογίες.

Η αντιμετώπιση αυτών των ανησυχιών είναι ζωτικής σημασίας για την ενίσχυση της αυτοπεποίθησης και της ασφάλειάς τους στις καθημερινές διαδικτυακές τους δραστηριότητες.

Κίνητρο

Ανάπτυξη στοχευμένων προγραμμάτων υποστήριξης και εκπαίδευσης.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

- **Τεχνολογική αλλαγή** και πολυπλοκότητα: Ο ταχύς ρυθμός της τεχνολογίας δυσκολεύει την προσαρμογή των ηλικιωμένων, ειδικά με τις ενημερώσεις και τις νέες συσκευές.
- Φόβος και **συναισθηματική χειραγώγηση:**Οι απάτες συχνά εκμεταλλεύονται συναισθήματα, όπως ο φόβος ή η επείγουσα ανάγκη, καθιστώντας τους ηλικιωμένους πιο ευάλωτους.
- **Κοινωνικός αποκλεισμός** και μοναξιά: Μειωμένη επαφή με την οικογένεια και τους φίλους, που συχνά αυξάνεται με την ψηφιακή επικοινωνία που αντικαθιστά τις άμεσες αλληλεπιδράσεις.
- **Δισταγμός να ζητήσετε βοήθεια:** Οι ηλικιωμένοι συχνά αισθάνονται ντροπή ή αμηχανία όταν ζητούν βοήθεια από νεότερους ανθρώπους με την τεχνολογία.
- **Οικονομικοί περιορισμοί**: Απροθυμία ή αδυναμία δαπανών σε νέες συσκευές ή λογισμικό, με αποτέλεσμα την απαρχαιωμένη, μη ασφαλή τεχνολογία.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

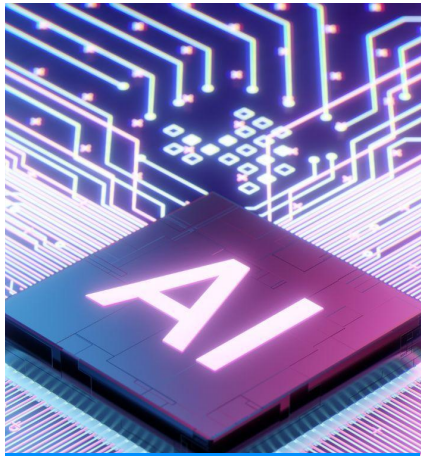
- **Ψηφιακός αποκλεισμός** στις υπηρεσίες: Οι καθημερινές εργασίες (όπως η αγορά εισιτηρίων, οι τραπεζικές συναλλαγές, τα ιατρικά ραντεβού) μεταφέρονται ολοένα και περισσότερο στο διαδίκτυο, αφήνοντας τους ηλικιωμένους χωρίς εναλλακτικές λύσεις.
- Χαμηλή **ψηφιακή ικανότητα** *:*Έλλειψη βασικών δεξιοτήτων και εμπειρίας, η οποία μερικές φορές επιδεινώνεται από την έλλειψη εκπαίδευσης στους υπολογιστές σε πρώιμο στάδιο της ζωής.
- Παρορμητικότητα και **επικίνδυνες αποφάσεις**: Η τάση να ενεργεί κανείς γρήγορα όταν αντιμετωπίζει τεχνολογικά προβλήματα—κάτι που μερικές φορές οδηγεί σε λάθη ή σε απάτες.
- **Τρωτό** σε παραπληροφόρηση: Δυσκολία στη διάκριση των αληθινών πληροφοριών από την ψηφιακή χειραγώγηση, ειδικά στο διαδίκτυο.
- Συσκευή και **προβλήματα συντήρησης λογισμικού:** Προβλήματα με την ενημέρωση συσκευών, τη διαχείριση κωδικών πρόσβασης και την κατανόηση των βέλτιστων πρακτικών ψηφιακής ασφάλειας, αυξάνοντας τον κίνδυνο.

Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

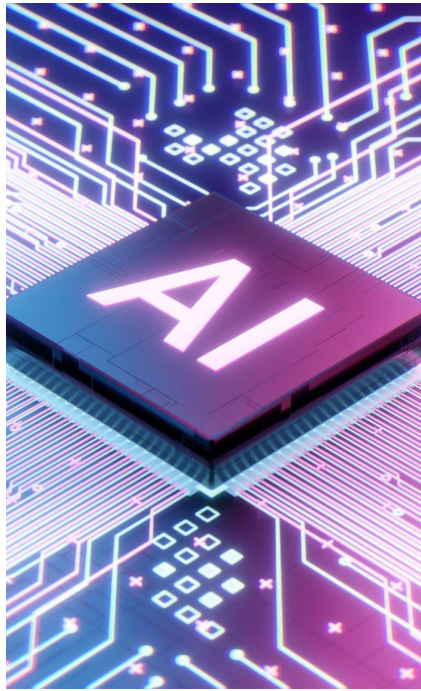
Η τεχνητή νοημοσύνη ενσωματώνεται ολοένα και περισσότερο σε πολλές πτυχές της καθημερινής ζωής, προσφέροντας σημαντικά οφέλη αλλά και εισάγοντας νέους κινδύνους για την κυβερνοασφάλεια.

Η κατανόηση των κύριων τομέων εφαρμογής της Τεχνητής Νοημοσύνης και των συναφών απειλών είναι απαραίτητη για την προστασία ευάλωτων ομάδων, όπως τα άτομα ηλικίας 55 ετών και άνω.



Υποστήριξη

Η παροχή αποτελεσματικής υποστήριξης απαιτεί την ευαισθητοποίηση σχετικά με τους κινδύνους που σχετίζονται με την Τεχνητή Νοημοσύνη.



Co-funded by the European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

- **Προσωπικοί βοηθοί** σε τηλέφωνα και συσκευές (π.χ., φωνητικούς βοηθούς όπως η Alexa) που υποστηρίζουν τους ηλικιωμένους σε καθημερινές εργασίες, αλλά απαιτούν κατανόηση της ιδιωτικότητας και της ασφάλειας.
- Τεχνητή Νοημοσύνη στην **παρακολούθηση της υγειονομικής περίθαλψης**(φορητές συσκευές, ανίχνευση ανωμαλιών στον καρδιακό ρυθμό) που παρέχει έγκαιρες προειδοποιήσεις αλλά χρειάζεται εμπιστοσύνη και βασικές ψηφιακές δεξιότητες για να λειτουργήσει.
- Απάτη με την υποστήριξη της τεχνητής νοημοσύνης και **ανίχνευση απάτης**(αναγνώριση ηλεκτρονικού "ψαρέματος" (phishing), αναγνώριση deepfake) για την προστασία των ηλικιωμένων από στοχευμένες επιθέσεις, αλλά απαιτώντας γνώση αναγνώρισης ύποπτου περιεχομένου.
- Δημιουργείται από τεχνητή νοημοσύνη **εξατομικευμένες επιθέσεις** που προσαρμόζονται στη συμπεριφορά και τα συναισθήματα των ηλικιωμένων, καθιστώντας πιο δύσκολο τον εντοπισμό των διαδικτυακών απειλών.
- **Δημιουργία περιεχομένου** και παραπληροφόρηση μέσω της Τεχνητής Νοημοσύνης (deepfakes, ψευδείς διαφημίσεις, ψεύτικες ειδήσεις) που επηρεάζουν τις αποφάσεις και προκαλούν σύγχυση μεταξύ των ηλικιωμένων που δεν έχουν δεξιότητες κριτικής αξιολόγησης.

Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

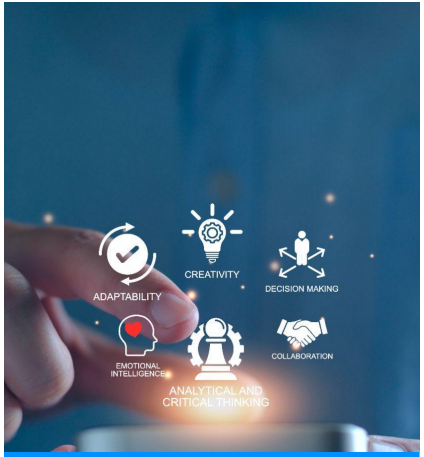
- Τεχνητή Νοημοσύνη μέσα σε **έξυπνο σπίτι** και οι συσκευές IoT βοηθούν στην καθημερινή ζωή, αλλά θέτουν σε κίνδυνο εάν οι συσκευές δεν είναι ασφαλείς ή δεν διαχειρίζονται σωστά.
- Ταξίδια με υποβοήθηση από τεχνητή νοημοσύνη και **σχεδιασμός αναψυχής** βοηθώντας στην οργάνωση ταξιδιών και δραστηριοτήτων, βελτιώνοντας την άνεση αλλά απαιτώντας κάποια ψηφιακή παιδεία για ασφαλή χρήση.
- Αυτοματοποιημένη **κοινωνική αλληλεπίδραση** ρομπότ που προσομοιώνουν ανθρώπινη συνομιλία, που χρησιμοποιούνται συχνά σε απάτες ή σε μέτρα μείωσης της απομόνωσης, και χρειάζονται επίγνωση για την αποφυγή εξαπάτησης.
- Τεχνητή Νοημοσύνη στην ψηφιακή εποχή **χρηματοοικονομικές υπηρεσίες** αυτοματοποίηση συναλλαγών και τραπεζικών εργασιών που μπορούν να βελτιώσουν την προσβασιμότητα αλλά απαιτούν γνώση των πρακτικών ασφαλείας και της πρόληψης της απάτης.
- Εργαλεία Τεχνητής Νοημοσύνης σε **συνεννόηση** με την οικογένεια και τους φροντιστές (παρακολούθηση σε πραγματικό χρόνο, συστήματα ειδοποίησης έκτακτης ανάγκης) που ενισχύουν την ασφάλεια, αλλά απαιτούν ικανότητα στη ρύθμιση και την ερμηνεία.

Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

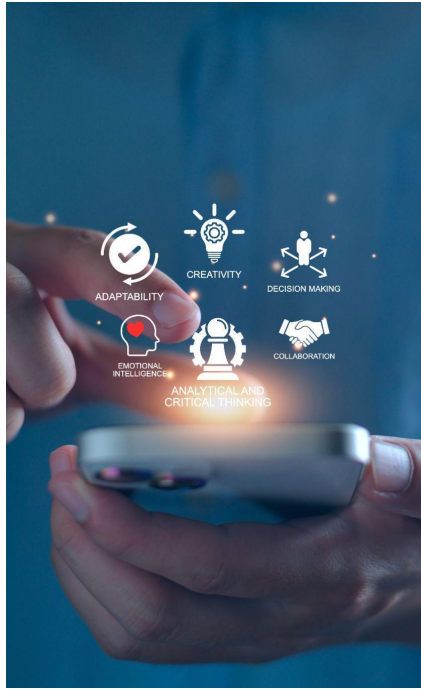
Η ανάπτυξη βασικών ψηφιακών ικανοτήτων είναι ζωτικής σημασίας για να ενδυναμωθούν οι ηλικιωμένοι ώστε να πλοηγούνται στον διαδικτυακό κόσμο με ασφάλεια και αυτοπεποίθηση.

Αυτές οι δεξιότητες τους βοηθούν να αξιοποιούν αποτελεσματικά την τεχνολογία για να βελτιώσουν την καθημερινότητά τους και την ανθεκτικότητά τους έναντι των κυβερνοαπειλών.



Ικανότητες

Δώστε τη δυνατότητα στους ηλικιωμένους να προστατεύουν καλύτερα τον εαυτό τους και να αξιοποιούν με σιγουριά τις σύγχρονες τεχνολογίες.



Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

- **Κατανόηση** της βασικής λειτουργίας ψηφιακής συσκευής και ρυθμίσεις ασφαλείας.
- **Αναγνώριση** χειραγώγησης που βασίζεται στην Τεχνητή Νοημοσύνη και δόλιου περιεχομένου.
- **Ψηφιακός γραμματισμός** για ασφαλή αλληλεπίδραση με βοηθούς τεχνητής νοημοσύνης και έξυπνες συσκευές.
- **Επίγνωση** μέτρων προστασίας και απορρήτου δεδομένων σε εφαρμογές τεχνητής νοημοσύνης.
- **Ικανότητα** να αναζητούν αξιόπιστες πληροφορίες και να επικυρώνουν περιεχόμενο που δημιουργείται από τεχνητή νοημοσύνη.

Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

- Συναισθηματική **ανθεκτικότητα** για την αποφυγή χειραγώγησης από απάτες που βασίζονται στην Τεχνητή Νοημοσύνη.
- **Άνεση** με την βασική αντιμετώπιση προβλημάτων και συντήρηση ψηφιακών εργαλείων.
- **Γνώση** ασφαλών πρακτικών διαχείρισης κωδικών πρόσβασης και ελέγχου ταυτότητας.
- Ικανότητα **χρήσης** εργαλείων τεχνητής νοημοσύνης για την υγεία, την ασφάλεια και την επικοινωνία.
- **Ειλικρίνεια** στη συνεχή μάθηση λόγω της ραγδαίας ανάπτυξης των τεχνολογιών Τεχνητής Νοημοσύνης.

Co-funded by the European Union

Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τις συνήθεις κυβερνοαπειλές της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.

Απειλές

Παραδείγματα από την πραγματική ζωή υπογραμμίζουν τη σημασία της αναγνώρισης και του μετριασμού των απειλών στον κυβερνοχώρο.

Co-funded by the
European Union

Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

- Χρήση τεχνολογίας **deepfake** για την πλαστοπροσωπία ενός μέλους της οικογένειας: Ένας ηλικιωμένος λαμβάνει ένα τηλεφώνημα όπου ο καλών, χρησιμοποιώντας μια πειστικά προσομοιωμένη φωνή εγγονιού ή παιδιού, ισχυρίζεται ότι χρειάζεται άμεσα χρήματα (π.χ., για ένα ατύχημα). Ο ηλικιωμένος, πεπεισμένος από τη συναισθηματική χειραγώγηση και την οικειότητα της φωνής, μεταφέρει χρήματα, συχνά χρησιμοποιώντας BLIK ή τραπεζική μεταφορά.
- **Απάτες** ερωτικών σχέσεων που αφορούν την Τεχνητή Νοημοσύνη: Οι ηλικιωμένοι στοχοποιούνται στο διαδίκτυο από άτομα (μερικές φορές chatbots ή αυτοματοποιημένα προφίλ) που αναπτύσσουν συναισθηματικές «σχέσεις» και στη συνέχεια ζητούν χρήματα με ψευδή προσχήματα, εκμεταλλευόμενοι τη μοναξιά και την εμπιστοσύνη.
- Ψεύτικη **λαχειοφόρος** αγορά ή κέρδος: Ένας ηλικιωμένος ενημερώνεται, συχνά μέσω κλήσης ή email που χρησιμοποιεί περιεχόμενο που δημιουργείται από τεχνητή νοημοσύνη, ότι έχει κερδίσει ένα μεγάλο χρηματικό ποσό. Για να το διεκδικήσει, του ζητείται προκαταβολή ή προσωπικά στοιχεία, με αποτέλεσμα οικονομική απώλεια και μερικές φορές κλοπή ταυτότητας.

Co-funded by the
European Union

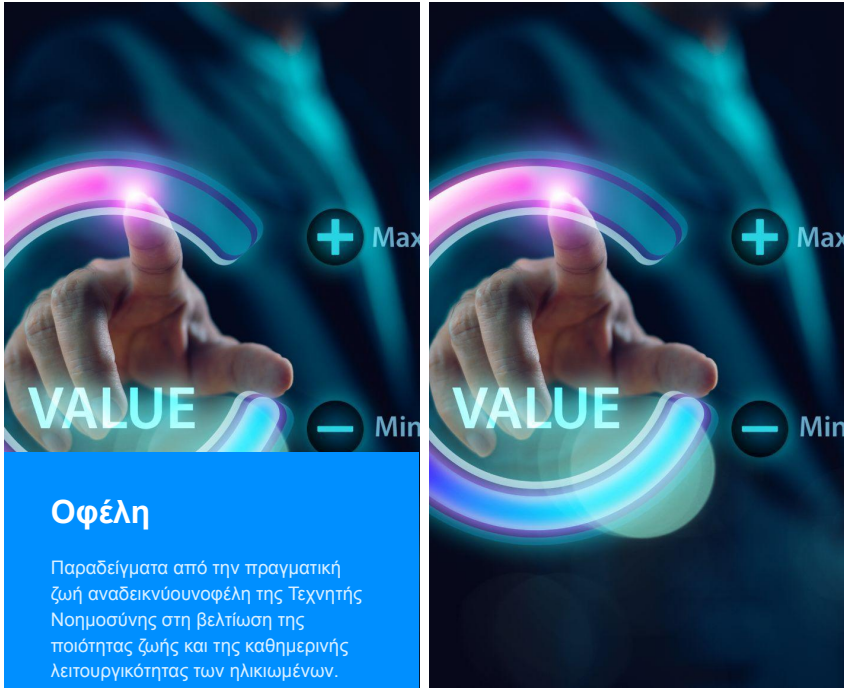
Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

- **Χειραγώγηση** μέσω ψεύτικων ηλεκτρονικών καταστημάτων: Οι ηλικιωμένοι αγοράζουν εν αγνοία τους αγαθά από ιστότοπους που είναι σχεδόν πανομοιότυποι με τα νόμιμα καταστήματα (με μια μικρή ορθογραφική αλλαγή στη διεύθυνση ή το όνομα). Πληρώνουν για αγαθά που δεν φτάνουν ποτέ, πέφτοντας θύματα εξελιγμένων ιστότοπων ηλεκτρονικού "ψαρέματος" (phishing) που βασίζονται σε τεχνητή νοημοσύνη.
- Ιατρική **παραπληροφόρηση** που διευκολύνεται από την Τεχνητή Νοημοσύνη: Οι ηλικιωμένοι συμβουλεύονται chatbots τεχνητής νοημοσύνης ή διαδικτυακά εργαλεία για συμβουλές υγείας. Μερικές φορές, οι συμβουλές είναι παραπλανητικές, με αποτέλεσμα να παραλείπουν να συμβουλευτούν τον γιατρό τους ή ακόμα και να λαμβάνουν λανθασμένα φάρμακα, κάτι που μπορεί να είναι επικίνδυνο για την υγεία τους.

Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τα οφέλη
της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.



Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

- Ένας ηλικιωμένος χρησιμοποίησε ένα εργαλείο **σχεδιασμού** ταξιδιών με τεχνητή νοημοσύνη για να οργανώσει ένα ταξίδι, καθορίζοντας ημερομηνίες και προσωπικά ενδιαφέροντα (όπως μουσεία ή υπαίθριες δραστηριότητες), λαμβάνοντας ένα λεπτομερές, προσαρμοσμένο δρομολόγιο—καθιστώντας το ταξίδι ευκολότερο και πιο ευχάριστο.
- Ιατρικά **διαγνωστικά** εργαλεία που βασίζονται σε τεχνητή νοημοσύνη εντόπισαν πρώιμα προειδοποιητικά σημάδια προβλημάτων υγείας(όπως ακανόνιστους καρδιακούς ρυθμούς σε ασθενείς με βηματοδότη και διαβήτη), οδηγώντας σε έγκαιρη ιατρική παρέμβαση και βελτιωμένη ευεξία.
- Οι ηλικιωμένοι αξιοποίησαν προσωπικούς **βοηθούς** τεχνητής νοημοσύνης (όπως η Alexa) για καθημερινές υπενθυμίσεις (π.χ., ώρες λήψης φαρμάκων και ραντεβού), διαχείριση του νοικοκυριού και διατήρηση κοινωνικής επαφής, μειώνοντας τη μοναξιά και αυξάνοντας την ανεξαρτησία.

Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

- Ένα παράδειγμα που αφορούσε τις έξυπνες **φορητές** συσκευές (βραχιόλια με τεχνητή νοημοσύνη) που παρακολουθούσαν συνεχώς βασικές μετρήσεις υγείας για ηλικιωμένους που ζουν μόνοι, ειδοποιώντας αυτόματα τους φροντιστές ή τις υπηρεσίες έκτακτης ανάγκης σε περίπτωση ανωμαλιών ή έκτακτων περιστατικών.
- **Η αναγνώριση** και η αναζήτηση εικόνων με τεχνητή νοημοσύνη βοήθησαν έναν ηλικιωμένο να αναγνωρίσει ένα άγνωστο φυτό στον κήπο του, παρέχοντας άμεση καθοδήγηση σχετικά με τη φροντίδα του, βελτιώνοντας έτσι τις δεξιότητες κηπουρικής και την αυτοπεποίθησή του.

Co-funded by the
European Union

Αποτελέσματα - Τσεχική Δημοκρατία

Co-funded by the European Union

Οι πιο συχνά αναφερόμενες διαδικτυακές απειλές για άτομα άνω των 55 ετών

Τα άτομα ηλικίας 55 ετών και άνω αντιμετωπίζουν μοναδικές προκλήσεις στον ψηφιακό κόσμο, καθιστώντας τα ευάλωτα σε μια ποικιλία διαδικτυακών απειλών.

Η κατανόηση των πιο συνηθισμένων και επιπτωτικών κινδύνων είναι απαραίτητη για τη βελτίωση της ευαισθητοποίησης και της προστασίας τους στον κυβερνοχώρο.

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing), συμπεριλαμβανομένων email, SMS και τηλεφωνικών κλήσεων όπου οι εισβολείς μιμούνται τράπεζες ή αξιόπιστα ιδρύματα για να κλέψουν ευαίσθητα δεδομένα.
- Ψεύτικα ηλεκτρονικά καταστήματα και απάτες που στοχεύουν ηλικιωμένους με δόλιες προσφορές και ιστότοπους.
- Κλοπή ταυτότητας, όπου προσωπικά δεδομένα χρησιμοποιούνται με σκοπό την απόκτηση χρημάτων ή την πλαστοπροσωπία του θύματος.
- Χειραγώγηση μέσω σύντομων βίντεο και παραπληροφόρησης, συμπεριλαμβανομένων κατασκευασμένων ειδήσεων και υποσυνείδητων μηνυμάτων.

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- Ανεπαρκής συντήρηση IT, όπως παρωχημένο υλικολογισμικό και αγνοημένες ενημερώσεις ασφαλείας, με αποτέλεσμα τα συστήματα να είναι ευάλωτα.
- Απάτη που εκμεταλλεύεται τη μοναξιά—απατεώνες που ξεκινούν ψεύτικες φιλίες ή ρομαντικές σχέσεις.
- Μη ασφαλής συγχρονισμός μεταξύ συσκευών και μη ασφαλής αποθήκευση κωδικών πρόσβασης σε προγράμματα περιήγησης.
- Αυξανόμενη απειλή απάτης μέσω τεχνητής νοημοσύνης, συμπεριλαμβανομένων κλωνοποιημένων φωνών που μιμούνται συγγενείς για επείγουσα οικονομική βοήθεια.
- Αυξανόμενοι κίνδυνοι λόγω της τεχνητής νοημοσύνης στα προγράμματα προστασίας από ιούς, καθιστώντας τη διαμόρφωση και την ασφαλή χρήση κρίσιμη για τους ηλικιωμένους.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

Οι ειδικοί τόνισαν βασικές ανησυχίες που επηρεάζουν περισσότερο άτομα ηλικίας 55 ετών και άνω κατά την αλληλεπίδρασή τους με τις ψηφιακές τεχνολογίες.

Η αντιμετώπιση αυτών των ανησυχιών είναι ζωτικής σημασίας για την ενίσχυση της αυτοπεποίθησης και της ασφάλειάς τους στις καθημερινές διαδικτυακές τους δραστηριότητες.

Κίνητρο

Ανάπτυξη στοχευμένων προγραμμάτων υποστήριξης και εκπαίδευσης.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

- **Δυσκολία στην παρακολούθηση** με την πολυπλοκότητα και την ραγδαία εξέλιξη της τεχνολογίας.
- **Φόβος απώλειας πρόσβασης** σε προσωπικά δεδομένα ή οικονομικά και πέφτοντας θύματα απάτης.
- **Αμηχανία** ή απώλεια αυτοπεποίθησης όταν δεν είναι δυνατή η χρήση της τεχνολογίας μπροστά στην οικογένεια.
- **Εξάρτηση** από άλλους (συγγενείς ή τεχνικούς) που εμποδίζει την οικοδόμηση ανεξαρτησίας.
- Δημόσιο Wi-Fi ασφαλείας, που χρησιμοποιείται συχνά από ηλικιωμένους χωρίς **επίγνωση ασφαλείας.**

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

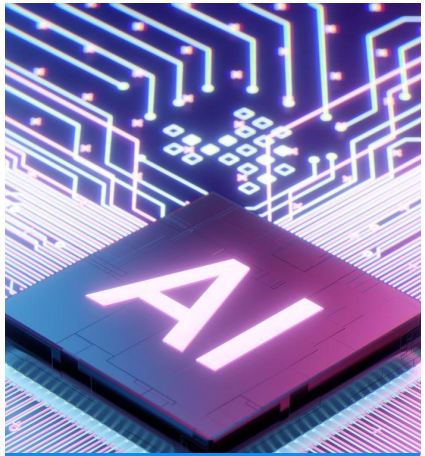
- **Μη ασφαλής αποθήκευση κωδικών πρόσβασης,** όπως η χρήση προγραμμάτων περιήγησης αντί για διαχειριστές κωδικών πρόσβασης.
- **Η ψηφιακή επικοινωνία** αντικαθιστά την πολύτιμη επαφή πρόσωπο με πρόσωπο, οδηγώντας σε κοινωνική απομόνωση.
- Απενεργοποίηση ενημερώσεων ή λειτουργιών ασφαλείας λόγω **έλλειψη κατανόησης**, εκθέτοντας τις συσκευές σε ευπάθειες.
- **Δυσκολία με την αλλαγή των διατάξεων του συστήματος,** των εικονιδίων ή των απροσδόκητων νέων λειτουργιών.
- Αδυναμία αναγνώρισης **ύποπτου ή παραποιημένου περιεχομένου**, καθιστώντας τους ηλικιωμένους πιο ευάλωτους στην εξαπάτηση.

Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

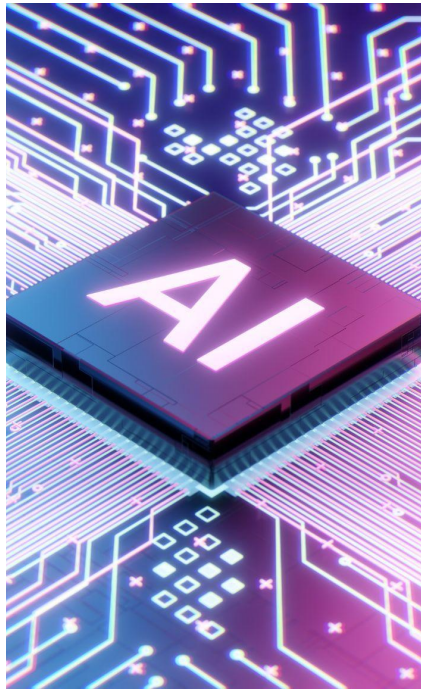
Η τεχνητή νοημοσύνη ενσωματώνεται ολοένα και περισσότερο σε πολλές πτυχές της καθημερινής ζωής, προσφέροντας σημαντικά οφέλη αλλά και εισάγοντας νέους κινδύνους για την κυβερνοασφάλεια.

Η κατανόηση των κύριων τομέων εφαρμογής της Τεχνητής Νοημοσύνης και των συναφών απειλών είναι απαραίτητη για την προστασία ευάλωτων ομάδων, όπως τα άτομα ηλικίας 55 ετών και άνω.



Υποστήριξη

Η παροχή αποτελεσματικής υποστήριξης απαιτεί την ευαισθητοποίηση σχετικά με τους κινδύνους που σχετίζονται με την Τεχνητή Νοημοσύνη.



Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

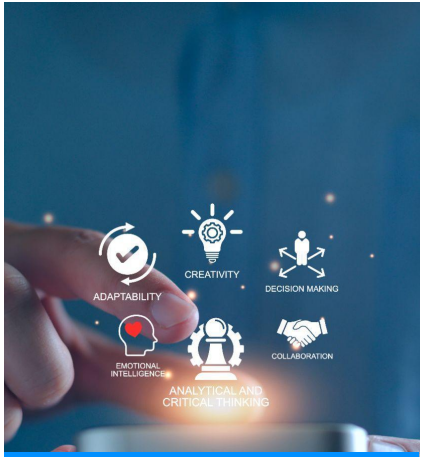
- **Τεχνητή Νοημοσύνη στην υγειονομική περίθαλψη:** τηλεϊατρική, παρακολούθηση υγείας και μετάφραση για επικοινωνία με την οικογένεια.
- **Καθημερινή υποστήριξη:** Φωνητικοί βοηθοί τεχνητής νοημοσύνης, έξυπνες οικιακές συσκευές, εργαλεία προστασίας από ιούς.
- Κίνδυνος του **χειρισμού δεδομένων**, επιθέσεις deepfake και διάδοση παραπληροφόρησης.
- Με δυνατότητα τεχνητής νοημοσύνης **κλωνοποίηση φωνής** πλαστοπροσωπία συγγενών, που οδηγεί σε οικονομική απάτη.
- **Υπερβολική εξάρτηση από εργαλεία τεχνητής νοημοσύνης** χωρίς να κατανοούν τους περιορισμούς τους—η Τεχνητή Νοημοσύνη θα πρέπει να θεωρείται εργαλείο, όχι αλάνθαστη αυθεντία.

Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

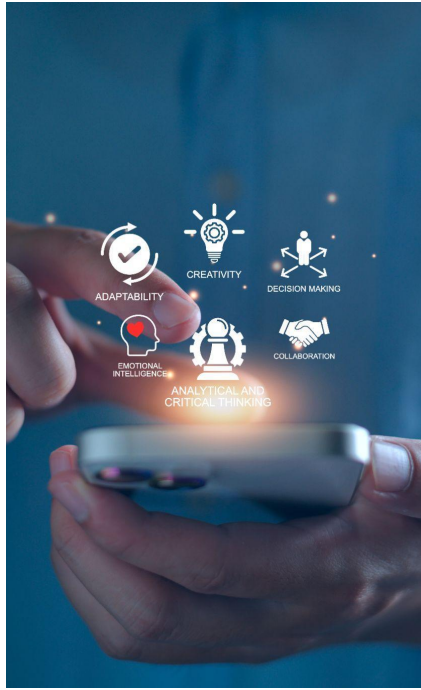
Η ανάπτυξη βασικών ψηφιακών ικανοτήτων είναι ζωτικής σημασίας για να ενδυναμωθούν οι ηλικιωμένοι ώστε να πλοηγούνται στον διαδικτυακό κόσμο με ασφάλεια και αυτοπεποίθηση.

Αυτές οι δεξιότητες τους βοηθούν να αξιοποιούν αποτελεσματικά την τεχνολογία για να βελτιώσουν την καθημερινότητά τους και την ανθεκτικότητά τους έναντι των κυβερνοαπειλών.



Ικανότητες

Δώστε τη δυνατότητα στους ηλικιωμένους να προστατεύουν καλύτερα τον εαυτό τους και να αξιοποιούν με σιγουριά τις σύγχρονες τεχνολογίες.



Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

- Καθιέρωση ισχυρών, μοναδικών κωδικών πρόσβασης και **διαχείριση ασφάλειας**(αποφύγετε την αποθήκευση στο πρόγραμμα περιήγησης, χρησιμοποιήστε έναν διαχειριστή κωδικών πρόσβασης).
- Ενεργοποίηση **ελέγχου ταυτότητας δύο παραγόντων** για την ασφάλιση λογαριασμών.
- Κατανόηση και **ρύθμιση παραμέτρων προγραμμάτων προστασίας από ιούς**, ειδικά εργαλεία που βασίζονται στην Τεχνητή Νοημοσύνη.
- **Αναγνωρίζοντας** ύποπτο, χειραγωγημένο ή **δόλιο διαδικτυακό περιεχόμενο**.
- **Χρήση βοηθών τεχνητής νοημοσύνης** πρακτικά, αλλά παραμένοντας επικριτικός απέναντι στα αποτελέσματα.
- Βασικός **ψηφιακός γραμματισμός**: ενημέρωση συσκευών, ασφαλής περιήγηση, ασφαλής χρήση Wi-Fi.
- **Οικοδόμηση αυτοπεποίθησης** για τη μείωση της εξάρτησης από τους άλλους και την υποστήριξη της συνεχιζόμενης ψηφιακής εκπαίδευσης.

Co-funded by the European Union

Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τις συνήθεις κυβερνοαπειλές της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.

Απειλές

Παραδείγματα από την πραγματική ζωή υπογραμμίζουν τη σημασία της αναγνώρισης και του μετριασμού των απειλών στον κυβερνοχώρο.

Co-funded by the
European Union

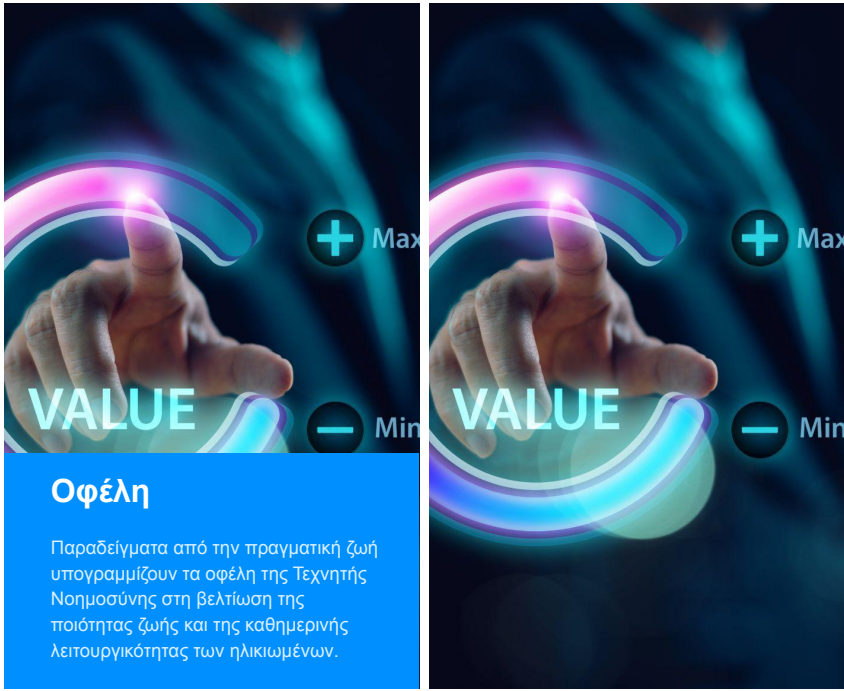
Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

- Παράδειγμα: Μια ηλικιωμένη γυναίκα έπεσε θύμα απάτης όταν ένας καλών χρησιμοποίησε τεχνολογία deepfake για να κλωνοποιήσει τη φωνή του εγγονού της και ζήτησε επειγόντως μετρητά, τα οποία παρέδωσε σε έναν courier.
- Απάτες ρομαντικού ή φιλικού περιεχομένου που εκμεταλλεύονται τη συναισθηματική προσκόλληση, συχνά μέσω μηνυμάτων ή κλήσεων.
- Παραπληροφόρηση που διαδίδεται μέσω βίντεο ή σύντομων μηνυμάτων, γεγονός που δυσχεραίνει την επαλήθευση της αυθεντικότητας από τους ηλικιωμένους.
- Κακή συντήρηση IT ή χρήση μη ασφαλών δικτύων που οδηγεί σε πραγματικές παραβιάσεις.

Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τα οφέλη
της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.



Co-funded by the European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

- Μια 72χρονη γυναίκα χρησιμοποίησε έναν βοηθό τεχνητής νοημοσύνης που βασίζεται στη φωνή για μετάφραση, επιτρέποντάς της να συμμετέχει και να κατανοεί οικογενειακές βιντεοκλήσεις και να αισθάνεται ότι συμπεριλαμβάνεται σε διεθνείς συνομιλίες.
- Οι ηλικιωμένοι χρησιμοποιούν την Τεχνητή Νοημοσύνη για προγραμματισμό (π.χ. συμβουλές των Windows, οικιακές εργασίες DIY) ή chatbots σε κέντρα φροντίδας Αλτσχάιμερ.
- Η Τεχνητή Νοημοσύνη προσφέρει εξατομικευμένες συμβουλές και υποστηρίζει την καθημερινή ανεξαρτησία, αλλά λειτουργεί καλύτερα όταν συνδυάζεται με ισχυρές βασικές δεξιότητες.

Co-funded by the
European Union

Αποτελέσματα - Ισλανδία

Co-funded by the European Union

Οι πιο συχνά αναφερόμενες διαδικτυακές απειλές για άτομα άνω των 55 ετών

Τα άτομα ηλικίας 55 ετών και άνω αντιμετωπίζουν μοναδικές προκλήσεις στον ψηφιακό κόσμο, καθιστώντας τα ευάλωτα σε μια ποικιλία διαδικτυακών απειλών.

Η κατανόηση των πιο συνηθισμένων και επιπτωτικών κινδύνων είναι απαραίτητη για τη βελτίωση της ευαισθητοποίησης και της προστασίας τους στον κυβερνοχώρο.

Co-funded by the
European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών

- **Deepfake απάτες** που παρουσιάζουν ψεύτικες εικόνες και βίντεο, ειδικά στο WhatsApp, όπου οι εγκληματίες παριστάνουν μέλη οικογένειας ισχυριζόμενοι ότι χρειάζονται επειγόντως χρήματα.
- Πολύπειρο **ηλεκτρονικό ψάρεμα (phishing)** εξελίχθηκε σε κοινωνική μηχανική μέσω εφαρμογών ανταλλαγής μηνυμάτων με πειστικά ψεύτικα τηλεφωνήματα και μηνύματα.
- **Απάτες αγάπης** σε πλατφόρμες γνωριμιών που στοχεύουν σε μοναχικούς ηλικιωμένους παγκοσμίως, συμπεριλαμβανομένης της Ισλανδίας, με αποτέλεσμα οικονομική και συναισθηματική βλάβη.
- Φυσική **πλαστοπροσωπία από εγκληματίες** παριστάνοντας την τεχνική υποστήριξη ή τους εκπροσώπους τραπεζών που επισκέπτονται οίκους ηλικιωμένων.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

Οι ειδικοί τόνισαν βασικές ανησυχίες που επηρεάζουν περισσότερο άτομα ηλικίας 55 ετών και άνω κατά την αλληλεπίδρασή τους με τις ψηφιακές τεχνολογίες.

Η αντιμετώπιση αυτών των ανησυχιών είναι ζωτικής σημασίας για την ενίσχυση της αυτοπεποίθησης και της ασφάλειάς τους στις καθημερινές διαδικτυακές τους δραστηριότητες.

Κίνητρο

Ανάπτυξη στοχευμένων προγραμμάτων υποστήριξης και εκπαίδευσης.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

- Δυσκολία με σύνθετες **διαδικασίες σύνδεσης**συμπεριλαμβανομένων των απαιτήσεων κωδικού πρόσβασης και των συχνών επαναφορών.
- Σύγχυση και **αντίσταση στην επαλήθευση δύο παραγόντων** μεταξύ των παλαιότερων χρηστών.
- **Κακή γνώση ηλεκτρονικού ταχυδρομείου και** παρεμπόδιση της ανάκτησης κωδικού πρόσβασης.
- **Μικρό μέγεθος κειμένου** και παλαιότερα τηλέφωνα που περιορίζουν τη χρηστικότητα και τις λειτουργίες ασφαλείας.
- **Έλλειψη σαφών οδηγιών** από υπηρεσίες που απαιτούν ηλεκτρονική ταυτότητα ή παρόμοια επαλήθευση ταυτότητας.

Co-funded by the
European Union

Οι 10 κορυφαίες ανησυχίες σύμφωνα με τους ειδικούς

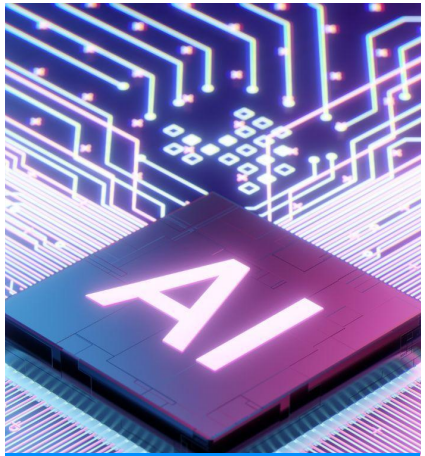
- Οι ηλικιωμένοι **επαναχρησιμοποιούν κωδικούς πρόσβασης** σε κρίσιμους ιστότοπους, διακινδυνεύοντας να παραβιάσουν πολλαπλούς λογαριασμούς.
- **Πλαστοπροσωπία τομέα** με τη δημιουργία πειστικών ψεύτικων ιστότοπων για την κλοπή ευαίσθητων δεδομένων.
- Συνεχείς απαρατήρητες **παραβιάσεις διαπιστευτηρίων** από την παρακολούθηση του σκοτεινού ιστού.
- **Γενική δυσπιστία** ή παρεξήγηση των απειλών στον κυβερνοχώρο που επηρεάζουν τις αντιδράσεις των ηλικιωμένων.
- Εμπόδια που δημιουργούνται από **τεχνολογική πολυπλοκότητα** μείωση της αυτοπεποίθησης και της ανεξαρτησίας.

Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

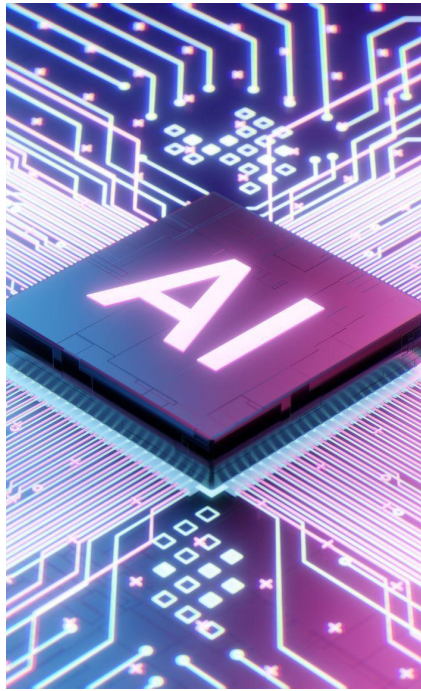
Η τεχνητή νοημοσύνη ενσωματώνεται ολοένα και περισσότερο σε πολλές πτυχές της καθημερινής ζωής, προσφέροντας σημαντικά οφέλη αλλά και εισάγοντας νέους κινδύνους για την κυβερνοασφάλεια.

Η κατανόηση των κύριων τομέων εφαρμογής της Τεχνητής Νοημοσύνης και των συναφών απειλών είναι απαραίτητη για την προστασία ευάλωτων ομάδων, όπως τα άτομα ηλικίας 55 ετών και άνω.



Υποστήριξη

Η παροχή αποτελεσματικής υποστήριξης απαιτεί την ευαισθητοποίηση σχετικά με τους κινδύνους που σχετίζονται με την Τεχνητή Νοημοσύνη.



Co-funded by the
European Union

Βασικοί τομείς χρήσης τεχνητής νοημοσύνης και κυβερνοκίνδυνοι

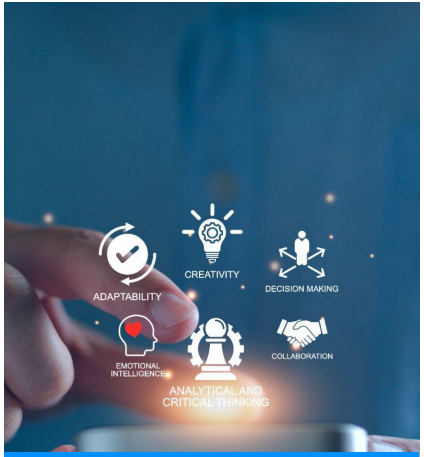
- **Εκπαίδευση** σχετικά με τον κίνδυνο ψευδούς διαδικτυακού περιεχομένου που παράγεται από τεχνητή νοημοσύνη, ιδίως βίντεο που υποστηρίζουν οικογενειακές καταστάσεις έκτακτης ανάγκης.
- **Συμβουλευτική** στους ηλικιωμένους ώστε να επαληθεύουν τα επείγοντα μηνύματα καλώντας απευθείας την οικογένειά τους, τονίζοντας ότι οι πραγματικές έκτακτες ανάγκες συνήθως περιλαμβάνουν τηλεφωνήματα και όχι μηνύματα.
- **Επίγνωση** ότι η Τεχνητή Νοημοσύνη μπορεί να μιμηθεί οποιαδήποτε δεδομένα, συμπεριλαμβανομένων βίντεο και εικόνων, απαιτώντας σκεπτικισμό και εναλλακτική επαλήθευση.
- Κίνδυνοι από **υπερβολική κοινοποίηση προσωπικών πληροφοριών** σε chatbots τεχνητής νοημοσύνης και εργαλεία όπως το ChatGPT, όπου αποθηκεύονται δεδομένα.
- Έμφαση στη **διατήρηση της κριτικής σκέψης** και επαλήθευση πληροφοριών μέσω άλλων καναλιών επικοινωνίας.

Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

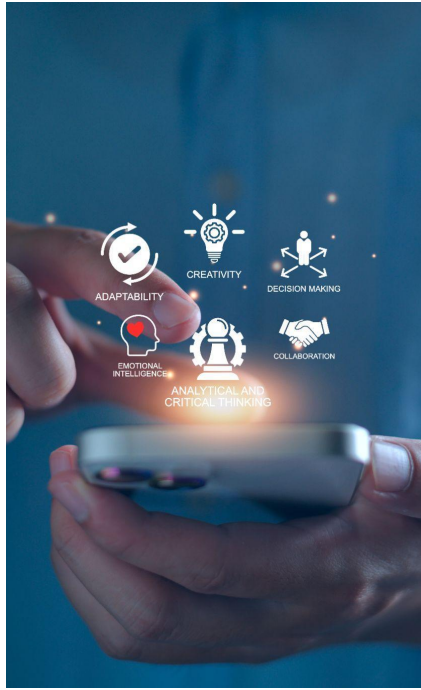
Η ανάπτυξη βασικών ψηφιακών ικανοτήτων είναι ζωτικής σημασίας για να ενδυναμωθούν οι ηλικιωμένοι ώστε να πλοηγούνται στον διαδικτυακό κόσμο με ασφάλεια και αυτοπεποίθηση.

Αυτές οι δεξιότητες τους βοηθούν να αξιοποιούν αποτελεσματικά την τεχνολογία για να βελτιώσουν την καθημερινότητά τους και την ανθεκτικότητά τους έναντι των κυβερνοαπειλών.



Ικανότητες

Δώστε τη δυνατότητα στους ηλικιωμένους να προστατεύουν καλύτερα τον εαυτό τους και να αξιοποιούν με σιγουριά τις σύγχρονες τεχνολογίες.



Co-funded by the
European Union

Κρίσιμες Ικανότητες για Ηλικιωμένους

- Κατανόηση της **σημασίας της επαλήθευσης** πριν απαντήσουν σε επείγοντα αιτήματα μέσω ψηφιακών μέσων.
- Βασικές **ψηφιακές δεξιότητες** συμπεριλαμβανομένης της ασφαλούς διαχείρισης κωδικών πρόσβασης και της επίγνωσης των κινδύνων της Τεχνητής Νοημοσύνης.
- **Ικανότητα υποβολής ερωτήσεων** και να επαληθεύουν απροσδόκητα ή συναισθηματικά φορτισμένα μηνύματα, ειδικά εκείνα που φαίνονται επείγοντα ή αγχωτικά.
- **Σκεπτικισμός** προς την αυθεντικότητα του διαδικτυακού περιεχομένου, ιδίως των μέσων που παράγονται από τεχνητή νοημοσύνη.
- Ενίσχυση της οικοδόμησης εμπιστοσύνης με τα μέλη της οικογένειας για **άμεση επικοινωνία** και βοήθεια.

Co-funded by the European Union

Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τις συνήθεις κυβερνοαπειλές της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.

Απειλές

Παραδείγματα από την πραγματική ζωή υπογραμμίζουν τη σημασία της αναγνώρισης και του μετριασμού των απειλών στον κυβερνοχώρο.

Co-funded by the
European Union

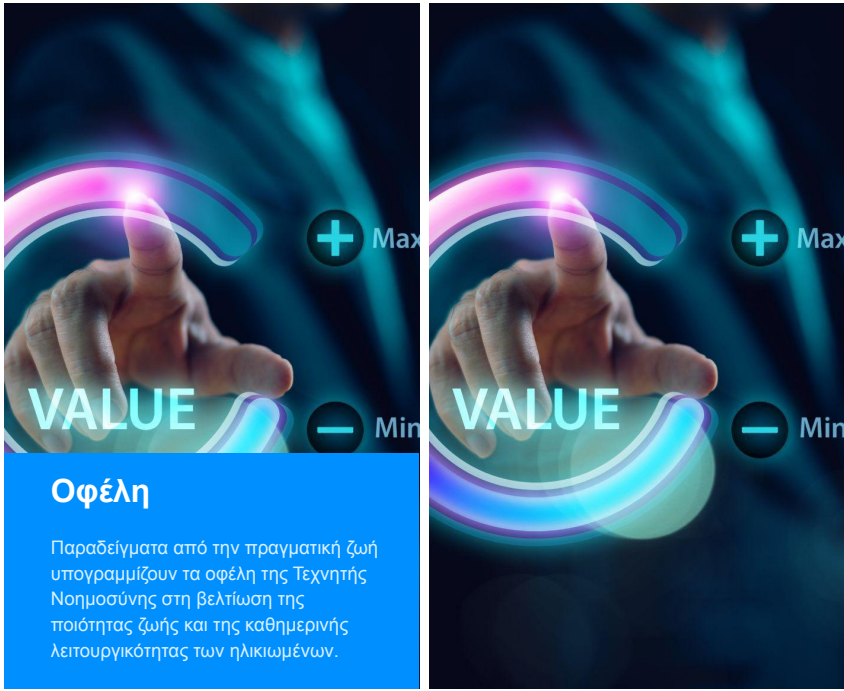
Απειλές στην πραγματική ζωή που εντοπίστηκαν από ειδικούς

- Παραδείγματα θυμάτων που έχασαν τις αποταμιεύσεις τους λόγω απάτης deepfake ρομαντικού ρεπορτάζ χρησιμοποιώντας ομοιότητες διασημοτήτων που δημιουργούνται από τεχνητή νοημοσύνη.
- Απάτες μέσω WhatsApp που περιλαμβάνουν ψεύτικα μηνύματα για άρρωστους συγγενείς που χρειάζονται καταθέσεις χρημάτων, οι οποίες μερικές φορές σταματούν με παρέμβαση της οικογένειας.
- Απάτες αγάπης με μέσα κοινωνικής δικτύωσης και εφαρμογές γνωριμιών που οδηγούν ηλικιωμένους να πληρώνουν για ψεύτικη υγειονομική περίθαλψη ή να ταξιδεύουν στο εξωτερικό για ανύπαρκτους συντρόφους.
- Απάτες εργασίας που κλέβουν στοιχεία πιστωτικής κάρτας μέσω φωνητικά κλωνοποιημένων δόλιων προσφορών εργασίας.
- Περιπτώσεις ευάλωτων ατόμων που δημοσίευσαν ακούσια επικίνδυνο περιεχόμενο στο διαδίκτυο χωρίς να κατανοήσουν τις συνέπειες.

Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

Οι ειδικοί μοιράστηκαν παραδείγματα από την πραγματική ζωή που καταδεικνύουν τόσο τους κινδύνους όσο και τα οφέλη των ψηφιακών τεχνολογιών για άτομα ηλικίας 55 ετών και άνω. Αυτές οι περιπτώσεις παρέχουν πολύτιμες πληροφορίες σχετικά με τα οφέλη
της τεχνητής νοημοσύνης στην καθημερινή ζωή των ηλικιωμένων.



Co-funded by the
European Union

Οφέλη στην πραγματική ζωή που έχουν εντοπιστεί από ειδικούς

- Η Τεχνητή Νοημοσύνη βοηθά τους ηλικιωμένους με πρακτικές συμβουλές καθημερινής ζωής, όπως καθαρισμό, επισκευές στο σπίτι και γρήγορη επίλυση προβλημάτων.
- Chatbots τεχνητής νοημοσύνης που παρέχουν συναισθηματική υποστήριξη και συντροφικότητα, προσφέροντας διαθεσιμότητα όλο το 24ωρο για ανακούφιση από το άγχος και γενική συζήτηση.
- Χρήση εργαλείων τεχνητής νοημοσύνης όπως το ChatGPT για την επαλήθευση ύποπτων email ή μηνυμάτων που σχετίζονται με την κυβερνοασφάλεια.
- Η επιτυχία της υιοθέτησης της Τεχνητής Νοημοσύνης ποικίλλει σημαντικά ανάλογα με τις ατομικές τεχνολογικές δεξιότητες των ηλικιωμένων και την εμπιστοσύνη τους στην τεχνολογία.

Co-funded by the European Union

Διαδικτυακές απειλές για άτομα άνω των 55 ετών - γλωσσάρι

Co-funded by the
European Union

Ηλεκτρονικό ψάρεμα (ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου, SMS, σύνδεσμοι, φωνητικές κλήσεις)

Το ηλεκτρονικό ψάρεμα (phishing) είναι ένα είδος κυβερνοεπίθεσης όπου οι εγκληματίες στέλνουν ψεύτικα email, μηνύματα κειμένου, τηλεφωνικές κλήσεις ή συνδέσμους προσποιούμενοι ότι είναι κάποιος που εμπιστεύεστε, όπως μια τράπεζα ή ένας φίλος. Στόχος τους είναι να σας ξεγελάσουν ώστε να δώσετε σημαντικές προσωπικές πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή στοιχεία τραπεζικού λογαριασμού. Αυτά τα ψεύτικα μηνύματα συχνά φαίνονται πολύ αληθινά και προσπαθούν να σας κάνουν να ενεργήσετε γρήγορα δημιουργώντας μια αίσθηση επείγοντος ή φόβου. Οι εισβολείς θέλουν να κλέψουν τα χρήματα ή την ταυτότητά σας ξεγελώντας σας ώστε να κάνετε κλικ σε επικίνδυνους συνδέσμους ή να κοινοποιήσετε ευαίσθητα δεδομένα. Για να παραμείνετε ασφαλείς, ελέγχετε πάντα ξανά ποιος έστειλε το μήνυμα, αποφεύγετε να κάνετε κλικ σε ύποπτους συνδέσμους και μην κοινοποιείτε ποτέ προσωπικές πληροφορίες εκτός εάν είστε απολύτως βέβαιοι ότι είναι ασφαλείς.

Co-funded by the
European Union

Deepfake επιθέσεις (ψεύτικος ήχος/βίντεο, πλαστοπροσωπία οικογένειας)

Οι επιθέσεις deepfake περιλαμβάνουν τη δημιουργία ψεύτικων ηχογραφήσεων ή βίντεο χρησιμοποιώντας τεχνητή νοημοσύνη που φαίνονται και ακούγονται πολύ αληθινές. Σε αυτές τις επιθέσεις, οι εγκληματίες μιμούνται τη φωνή ή το πρόσωπο κάποιου γνωστού, συχνά ενός μέλους της οικογένειας, για να ξεγελάσουν τους ανθρώπους ώστε να πιστέψουν ότι μιλάνε με ένα αγαπημένο τους πρόσωπο. Για παράδειγμα, ένας απατεώνας μπορεί να χρησιμοποιήσει τεχνολογία deepfake για να πραγματοποιήσει μια τηλεφωνική κλήση που ακούγεται ακριβώς σαν ένα εγγόνι που ζητάει επειγόντως χρήματα. Αυτές οι ψεύτικες ηχογραφήσεις είναι πολύ πειστικές και μπορούν να ξεγελάσουν ακόμη και προσεκτικούς ανθρώπους. Οι επιθέσεις deepfake είναι επικίνδυνες επειδή εκμεταλλεύονται την εμπιστοσύνη και τα συναισθήματα, καθιστώντας δύσκολη την συνειδητοποίηση της εξαπάτησης μέχρι να είναι πολύ αργά. Για να προστατεύσετε τον εαυτό σας, επαληθεύετε πάντα τα ασυνήθιστα αιτήματα επικοινωνώντας απευθείας με το άτομο μέσω διαφορετικών καναλιών επικοινωνίας πριν προβείτε σε οποιαδήποτε ενέργεια.

Co-funded by the
European Union

Ψεύτικα ηλεκτρονικά καταστήματα και απάτες (πλαστές ιστοσελίδες)

Τα ψεύτικα ηλεκτρονικά καταστήματα και οι απάτες είναι δόλιες ιστοσελίδες που έχουν σχεδιαστεί για να μοιάζουν με νόμιμα καταστήματα, αλλά στην πραγματικότητα δημιουργούνται για να ξεγελάσουν τους ανθρώπους ώστε να αγοράσουν προϊόντα που δεν υπάρχουν ή είναι κακής ποιότητας. Αυτά τα ψεύτικα καταστήματα συχνά αντιγράφουν λογότυπα, περιγραφές προϊόντων και φωτογραφίες από πραγματικές εταιρείες για να φαίνονται πειστικά. Οι απατεώνες χρησιμοποιούν αυτές τις ιστοσελίδες για να κλέψουν χρήματα και προσωπικά στοιχεία από ανυποψίαστους πελάτες. Δελεάζουν τους αγοραστές με υποσχέσεις για πολύ χαμηλές τιμές ή ειδικές προσφορές που φαίνονται πολύ καλές για να είναι αληθινές.

Αυτοί οι ιστότοποι ενδέχεται να έχουν παράξενες διευθύνσεις, ορθογραφικά λάθη ή να μην έχουν τα σωστά στοιχεία επικοινωνίας. Αφού οι πελάτες πληρώσουν, συχνά δεν λαμβάνουν ποτέ την παραγγελία τους ή λαμβάνουν πλαστά προϊόντα. Για να προστατεύσετε τον εαυτό σας, αγοράζετε πάντα από αξιόπιστα καταστήματα, ελέγχετε τις κριτικές των ιστότοπων, αποφεύγετε προσφορές που φαίνονται εξωπραγματικά φθηνές και μην κοινοποιείτε ποτέ στοιχεία πληρωμής σε ύποπτους ιστότοπους. Εάν κάτι σας φαίνεται περίεργο, είναι καλύτερο να το ελέγξετε ξανά πριν κάνετε μια αγορά.

Co-funded by the
European Union

Συναισθηματική χειραγώγηση και κοινωνική μηχανική (τακτικές εκφοβισμού)

Η συναισθηματική χειραγώγηση και η κοινωνική μηχανική περιλαμβάνουν την εξαπάτηση των ανθρώπων παίζοντας με τα συναισθήματά τους για να τους κάνουν να ενεργούν με τρόπους που κανονικά δεν θα ενεργούσαν. Οι κυβερνοεγκληματίες χρησιμοποιούν τακτικές όπως ιστορίες τρόμου, επείγον, ψεύτικη εξουσία ή καλοσύνη για να δημιουργήσουν ένα αίσθημα φόβου, εμπιστοσύνης ή υποχρέωσης. Για παράδειγμα, μπορεί να προσποιούνται ότι είναι τραπεζικός υπάλληλος που σας προειδοποιεί για ένα πρόβλημα με τον λογαριασμό σας, προτρέποντάς σας να ενεργήσετε γρήγορα, ώστε να παρέχετε ευαίσθητες πληροφορίες χωρίς να το σκεφτείτε. Αυτές οι τακτικές εκμεταλλεύονται τις φυσικές ανθρώπινες αντιδράσεις - φόβο, εμπιστοσύνη, περιέργεια ή βοήθεια - καθιστώντας δύσκολη την αντίσταση. Η καλύτερη άμυνα είναι η επίγνωση: αναγνωρίζοντας αυτά τα συναισθηματικά κόλπα και σταματώντας για να επαληθεύσετε ποιος πραγματικά ζητά πληροφορίες πριν απαντήσετε.

Co-funded by the
European Union

Κλοπή ταυτότητας (χρησιμοποιώντας κλεμμένα προσωπικά δεδομένα)

Κλοπή ταυτότητας σημαίνει όταν κάποιος κλέβει τα προσωπικά σας στοιχεία χωρίς την άδειά σας και τα χρησιμοποιεί για να προσποιηθεί ότι είστε εσείς. Μπορεί να χρησιμοποιήσει το όνομά σας, τον αριθμό κοινωνικής ασφάλισης, τα στοιχεία του τραπεζικού σας λογαριασμού ή άλλα δεδομένα για να ανοίξει λογαριασμούς, να λάβει δάνεια ή να κάνει αγορές στο όνομά σας. Αυτό μπορεί να προκαλέσει μεγάλα οικονομικά προβλήματα και να βλάψει τη φήμη σας.

Co-funded by the
European Union

Απάτη «στο εγγόνι» (απατεώνες που προσποιούνται ότι είναι οικογένεια σε κίνδυνο)

Η απάτη «στο εγγόνι», γνωστή και ως «απάτη με τον παππού και τη γιαγιά», είναι μια κοινή μέθοδος που χρησιμοποιείται από εγκληματίες που προσποιούνται ότι είναι μέλος της οικογένειας - συνήθως ένα εγγόνι ή ένα παιδί - που βρίσκεται σε κίνδυνο. Αυτό συμβαίνει συνήθως τηλεφωνικά, όπου ο απατεώνας καλεί ένα ηλικιωμένο άτομο και ισχυρίζεται ότι έχει σοβαρό πρόβλημα, όπως ατύχημα, σύλληψη ή ανάγκη επείγουσας οικονομικής βοήθειας. Ο καλών συχνά ζητά να σταλούν γρήγορα χρήματα και επιμένει να το κρατήσει μυστικό το θύμα, λέγοντας για παράδειγμα: «Μην το πεις στη μαμά, θα ανησυχήσει».

Αυτή η απάτη εκμεταλλεύεται συναισθήματα όπως η αγάπη και το ενδιαφέρον για τα μέλη της οικογένειας, κάνοντάς το άτομο να θέλει να βοηθήσει αμέσως χωρίς να σταματήσει να σκέφτεται. Όλο και περισσότερο, οι απατεώνες χρησιμοποιούν τεχνολογία όπως η τεχνητή νοημοσύνη για να μιμηθούν τη φωνή του πραγματικού εγγονιού, κάνοντας την κλήση να ακούγεται πολύ πειστική.

Co-funded by the
European Union

Ψεύτικα αιτήματα «βοήθειας» μέσω WhatsApp ή Messenger

Τα ψεύτικα αιτήματα «βοήθειας» μέσω WhatsApp ή Messenger είναι απάτες όπου κάποιος προσποιείται ότι είναι φίλος ή μέλος της οικογένειάς του που αντιμετωπίζει επείγοντα προβλήματα, ζητώντας χρήματα ή προσωπικά στοιχεία. Αυτά τα μηνύματα συχνά προέρχονται απροσδόκητα από άγνωστες ή συγκαλυμμένες επαφές. Ο απατεώνας μπορεί να πει ότι έχασε το τηλέφωνό του, ότι κλειδώθηκε έξω από τον λογαριασμό του ή ότι χρειάζεται επείγουσα οικονομική βοήθεια. Προσπαθούν να δημιουργήσουν μια αίσθηση επείγοντος και εμπιστοσύνης για να κάνουν τα θύματα να ενεργήσουν γρήγορα χωρίς να ελέγξουν αν είναι αλήθεια.

Co-funded by the
European Union

Ρομαντικές απάτες και απάτες που βασίζονται σε σχέσεις που χτίστηκαν στο διαδίκτυο

Οι απάτες με ρομαντικές σχέσεις είναι ένα είδος απάτης όπου οι εγκληματίες δημιουργούν ψεύτικα διαδικτυακά προφίλ και προσποιούνται ότι ενδιαφέρονται ρομαντικά για κάποιον. Χτίζουν εμπιστοσύνη και συναισθηματική σύνδεση με την πάροδο του χρόνου, κάνοντας το θύμα να πιστεύει ότι βρίσκεται σε μια γνήσια σχέση. Μόλις κερδίσουν την εμπιστοσύνη, οι απατεώνες επινοούν καταστάσεις έκτακτης ανάγκης ή επείγουσες οικονομικές ανάγκες - όπως ιατρικά έξοδα ή έξοδα ταξιδιού - και ζητούν από το θύμα χρήματα ή δώρα.

Αυτοί οι απατεώνες είναι πολύ επιδέξιοι στο να φαίνονται φροντιστικοί και αξιόπιστοι, αποφεύγοντας συχνά τις προσωπικές συναντήσεις ή τις βιντεοκλήσεις δίνοντας δικαιολογίες. Εκμεταλλεύονται τη μοναξιά και την συναισθηματική ευαλωτότητα, γεγονός που καθιστά τα θύματα πιο πιθανό να τους δώσουν χρήματα.

Co-funded by the
European Union

Επενδυτική απάτη (ψεύτικες διαφημίσεις με διασημότητες)

Η επενδυτική απάτη που περιλαμβάνει ψεύτικες διαφημίσεις με διασημότητες είναι ένα είδος απάτης όπου οι εγκληματίες χρησιμοποιούν εικόνες, βίντεο ή ονόματα διάσημων προσώπων για να κάνουν μια επενδυτική ευκαιρία να φαίνεται νόμιμη και αξιόπιστη. Μερικές φορές, αυτές οι διαφημίσεις περιλαμβάνουν deepfake βίντεο που δείχνουν διασημότητες να υποστηρίζουν μια επένδυση ή παρουσιάζονται ως ειδησεογραφικά άρθρα που συνδέουν διασημότητες με οικονομική επιτυχία με ορισμένες πλατφόρμες.

Οι απατεώνες ξεγελούν τους ανθρώπους κάνοντάς τους να πιστέψουν ότι μπορούν να αποκομίσουν γρήγορα και μεγάλα κέρδη, συχνά σε κρυπτονομίσματα ή συναλλαγές συναλλάγματος. Παρασύρουν τα θύματα να δημιουργήσουν λογαριασμούς, να καταθέσουν χρήματα και στη συνέχεια ζητούν περισσότερα χρήματα για να πληρώσουν ψεύτικες χρεώσεις ή φόρους. Οι πρόωρες επιστροφές μπορεί να αποδειχθούν ότι κερδίζουν την εμπιστοσύνη, αλλά όταν τα θύματα προσπαθούν να αποσύρουν τα χρήματά τους, μπλοκάρονται και τους ζητούνται μεγάλες πρόσθετες πληρωμές.

Co-funded by the
European Union

Κακόβουλο λογισμικό και ransomware (μολυσμένα αρχεία, συνημμένα)

Το κακόβουλο λογισμικό μπορεί να μολύνει τον υπολογιστή ή το τηλέφωνό σας και να προκαλέσει βλάβη, όπως κλοπή των προσωπικών σας στοιχείων, καταστροφή αρχείων ή κατάληψη του ελέγχου της συσκευής σας. Το ransomware είναι ένας ειδικός τύπος κακόβουλου λογισμικού που κλειδώνει ή κρυπτογραφεί τα αρχεία σας, καθιστώντας τα μη προσβάσιμα μέχρι να πληρώσετε λύτρα —συνήθως σε κρυπτονομίσματα— στον εισβολέα. Το ransomware μπορεί να εισέλθει στη συσκευή σας μέσω μολυσμένων συνημμένων email, κακόβουλων ιστότοπων ή μη ασφαλών λήψεων.

Μόλις μολυνθεί, το ransomware σάς εμποδίζει να χρησιμοποιήσετε τα σημαντικά αρχεία σας και μερικές φορές απαιτεί χρήματα για να αποκαταστήσετε την πρόσβαση. Η πληρωμή των λύτρων δεν εγγυάται ότι τα δεδομένα σας θα αποκαλυφθούν και ενθαρρύνει τους εγκληματίες να συνεχίσουν αυτές τις επιθέσεις.

Co-funded by the
European Union

Μη επαληθευμένες εφαρμογές και μη ασφαλείς λήψεις λογισμικού

Οι μη επαληθευμένες εφαρμογές και οι μη ασφαλείς λήψεις λογισμικού αποτελούν κυβερνοαπειλές όπου άτομα κατεβάζουν και εγκαθιστούν εφαρμογές ή αρχεία από άγνωστες ή αναξιόπιστες πηγές. Αυτές οι εφαρμογές ή οι λήψεις ενδέχεται να περιέχουν κρυφό κακόβουλο λογισμικό, ιούς ή spyware που μπορούν να βλάψουν τη συσκευή σας, να κλέψουν προσωπικά στοιχεία ή να δώσουν σε χάκερ μη εξουσιοδοτημένη πρόσβαση.

Επειδή αυτές οι εφαρμογές δεν ελέγχονται ή δεν εγκρίνονται από αξιόπιστες πλατφόρμες, μπορούν να επηρεάσουν την ασφάλεια της συσκευής σας, να προκαλέσουν σφάλματα ή να σας εκθέσουν σε απάτες. Οι ψεύτικες εφαρμογές μπορεί να μοιάζουν με πραγματικές, αλλά όταν εγκατασταθούν, μπορούν να συλλέξουν τα δεδομένα σας ή να διαδώσουν επιβλαβές λογισμικό.

Co-funded by the
European Union

Κοινοποίηση ευαίσθητων δεδομένων σε αγνώστους (φωτογραφίες, πληροφορίες)

Η κοινοποίηση ευαίσθητων δεδομένων σε αγνώστους, όπως φωτογραφίες ή προσωπικά στοιχεία, αποτελεί μια κυβερνοαπειλή όπου οι άνθρωποι αποκαλύπτουν προσωπικά στοιχεία σε άγνωστα ή μη έμπιστα άτομα στο διαδίκτυο. Αυτό μπορεί να φαίνεται ακίνδυνο, όπως η κοινοποίηση μιας φωτογραφίας, αλλά αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν λανθασμένα για να κλέψουν την ταυτότητά σας, να διαπράξουν απάτη ή να βλάψουν τη φήμη σας.

Οι φωτογραφίες ενδέχεται να αποκαλύψουν το σπίτι, την τοποθεσία ή τις προσωπικές σας συνήθειες χωρίς να το συνειδητοποιείτε. Άγνωστοι μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να σας εξαπατήσουν ή να σας στοχοποιήσουν σε απάτες. Για να παραμείνετε ασφαλείς, κοινοποιήστε προσωπικές πληροφορίες και φωτογραφίες μόνο σε άτομα που εμπιστεύεστε, σκεφτείτε προσεκτικά πριν δημοσιεύσετε στο διαδίκτυο και προσαρμόστε τις ρυθμίσεις απορρήτου για να περιορίσετε ποιος μπορεί να δει τις πληροφορίες σας.

Co-funded by the
European Union

Διαρροές δεδομένων από τη χρήση παρωχημένων συσκευές ή λογισμικό

Η χρήση παρωχημένων συσκευών ή λογισμικού αποτελεί κυβερνοαπειλή, επειδή οι παλαιότερες εκδόσεις συχνά δεν διαθέτουν τις πιο πρόσφατες ενημερώσεις ασφαλείας. Αυτές οι ελλείπουσες ενημερώσεις δημιουργούν αδυναμίες, που ονομάζονται ευπάθειες, τις οποίες οι χάκερ μπορούν εύκολα να εκμεταλλευτούν για να αποκτήσουν πρόσβαση στα προσωπικά σας στοιχεία ή να ελέγξουν τη συσκευή σας. Αυτό μπορεί να οδηγήσει σε διαρροές δεδομένων, κλοπή ή μόλυνση από κακόβουλο λογισμικό.

Το παρωχημένο λογισμικό επιβραδύνει επίσης τη συσκευή σας και ενδέχεται να σταματήσει να λειτουργεί με νεότερα προγράμματα, δυσχεραίνοντας τις καθημερινές σας δραστηριότητες. Για να προστατευτείτε, είναι σημαντικό να ενημερώνετε τακτικά τη συσκευή και το λογισμικό σας με τις πιο πρόσφατες ενημερώσεις κώδικα και διορθώσεις ασφαλείας. Αυτό καλύπτει τα κενά ασφαλείας, διατηρεί τα δεδομένα σας ασφαλέστερα και διασφαλίζει την ομαλή λειτουργία της συσκευής σας.

Co-funded by the
European Union

Μαζικές εξατομικευμένες επιθέσεις με χρήση τεχνητής νοημοσύνης, στοχεύοντας προφίλ χρηστών

Οι μαζικά εξατομικευμένες επιθέσεις με χρήση τεχνητής νοημοσύνης είναι κυβερνοαπειλές όπου οι εισβολείς χρησιμοποιούν τεχνητή νοημοσύνη για να δημιουργήσουν εξαιρετικά προσαρμοσμένα και πειστικά μηνύματα που απευθύνονται σε άτομα με βάση τα προσωπικά τους δεδομένα. Η τεχνητή νοημοσύνη αναλύει πληροφορίες από μέσα κοινωνικής δικτύωσης, email και δημόσιες πηγές για να δημιουργήσει μηνύματα που φαίνονται πολύ οικεία και αξιόπιστα στον στόχο.

Αυτές οι επιθέσεις μπορούν να περιλαμβάνουν εξατομικευμένα email ή μηνύματα ηλεκτρονικού "ψαρέματος" (phishing) που αναφέρουν το όνομα, την εργασία, τις πρόσφατες δραστηριότητες ή τα ενδιαφέροντά του θύματος. Στόχος είναι να ξεγελαστούν οι άνθρωποι ώστε να κάνουν κλικ σε κακόβουλους συνδέσμους, να αποκαλύψουν κωδικούς πρόσβασης ή να μεταφέρουν χρήματα. Επειδή η Τεχνητή Νοημοσύνη μαθαίνει και προσαρμόζεται συνεχώς, αυτές οι επιθέσεις γίνονται πιο αποτελεσματικές και πιο δύσκολο να εντοπιστούν.

Co-funded by the
European Union

Παραπληροφόρηση για την υγεία ή επικίνδυνες ιατρικές συμβουλές από εργαλεία τεχνητής νοημοσύνης

Η παραπληροφόρηση για την υγεία ή οι επικίνδυνες ιατρικές συμβουλές από εργαλεία τεχνητής νοημοσύνης αποτελούν μια κυβερνοαπειλή όπου η τεχνητή νοημοσύνη παράγει λανθασμένες, παραπλανητικές ή επιβλαβείς πληροφορίες για την υγεία. Οι άνθρωποι μπορεί να εμπιστεύονται τα chatbots τεχνητής νοημοσύνης ή τα διαδικτυακά εργαλεία για ιατρικές συμβουλές, αλλά μερικές φορές αυτά τα συστήματα παράγουν λανθασμένες διαγνώσεις, προτείνουν μη ασφαλείς θεραπείες ή διαδίδουν ψευδείς ισχυρισμούς σχετικά με ασθένειες.

Αυτή η παραπληροφόρηση μπορεί να οδηγήσει τους ανθρώπους να καθυστερήσουν την κατάλληλη ιατρική περίθαλψη, να χρησιμοποιήσουν αναποτελεσματικά φάρμακα ή να προβούν σε επιβλαβείς ενέργειες. Το περιεχόμενο που δημιουργείται από την τεχνητή νοημοσύνη μπορεί να ακούγεται πολύ επαγγελματικό και πειστικό, καθιστώντας δύσκολο να διαπιστωθεί εάν οι συμβουλές είναι αξιόπιστες.

Co-funded by the
European Union

Απάτες που εκμεταλλεύονται τον ψηφιακό αποκλεισμό σε δημόσιες και τραπεζικές υπηρεσίες

Οι απάτες που εκμεταλλεύονται τον ψηφιακό αποκλεισμό στις δημόσιες και τραπεζικές υπηρεσίες αποτελούν απειλές που στοχεύουν άτομα που έχουν περιορισμένη πρόσβαση ή γνώση των ψηφιακών τεχνολογιών. Αυτές οι απάτες εκμεταλλεύονται άτομα που δυσκολεύονται να χρησιμοποιήσουν διαδικτυακές κυβερνητικές ή τραπεζικές υπηρεσίες, μερικές φορές επειδή δεν έχουν συσκευές, πρόσβαση στο διαδίκτυο, ψηφιακές δεξιότητες ή αυτοπεποίθηση.

Οι εγκληματίες ξεγελούν αυτά τα άτομα προσφέροντας ψεύτικη βοήθεια με διαδικτυακές διαδικασίες ή στέλνοντας δόλια μηνύματα που μιμούνται επίσημα ιδρύματα, ελπίζοντας ότι τα θύματα θα κοινοποιήσουν ευαίσθητα δεδομένα ή θα στείλουν χρήματα. Επειδή αυτά τα άτομα έχουν λιγότερους πόρους ή υποστήριξη για να αναγνωρίσουν απάτες, είναι πιο ευάλωτα.

Co-funded by the European Union

Έλλειψη πρακτικών πολυπαραγοντικής επαλήθευσης ταυτότητας (απλοποιημένοι κωδικοί πρόσβασης, επαναχρησιμοποίηση)

Η έλλειψη πολυπαραγοντικού ελέγχου ταυτότητας (MFA) σημαίνει ότι χρησιμοποιείτε μόνο έναν κωδικό πρόσβασης —συχνά απλό ή επαναλαμβανόμενο σε πολλούς ιστότοπους— για την προστασία των διαδικτυακών λογαριασμών. Αυτό είναι επικίνδυνο, επειδή αν κάποιος κλέψει ή μαντέψει τον κωδικό πρόσβασής σας, μπορεί εύκολα να αποκτήσει πρόσβαση στους λογαριασμούς σας.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας δύο ή περισσότερες μορφές επαλήθευσης. Για παράδειγμα, αφού πληκτρολογήσετε τον κωδικό πρόσβασής σας, ενδέχεται να εισαγάγετε έναν κωδικό που αποστέλλεται στο τηλέφωνό σας ή να χρησιμοποιήσετε σάρωση δακτυλικών αποτυπωμάτων. Αυτό καθιστά πολύ πιο δύσκολο για τους χάκερ να αποκτήσουν πρόσβαση στον λογαριασμό σας, ακόμα κι αν έχουν τον κωδικό πρόσβασής σας.

Co-funded by the
European Union

Απώλεια πρόσβασης σε κρίσιμες υπηρεσίες λόγω τεχνολογικών αλλαγών (πρόσβαση μόνο μέσω εφαρμογής, περιορισμένες εναλλακτικές λύσεις)

Η απώλεια πρόσβασης σε κρίσιμες υπηρεσίες λόγω τεχνολογικών αλλαγών συμβαίνει όταν σημαντικές δημόσιες ή τραπεζικές υπηρεσίες μεταβαίνουν σε αποκλειστικά ψηφιακές μορφές, όπως εφαρμογές ή διαδικτυακές πύλες, χωρίς εύκολες εναλλακτικές λύσεις για άτομα που δεν είναι άνετα ή δεν είναι εξοπλισμένα για να τις χρησιμοποιήσουν. Αυτό σημαίνει ότι άτομα που δεν διαθέτουν smartphone, υπολογιστές ή ψηφιακές δεξιότητες μπορεί να δυσκολεύονται ή να μην έχουν πρόσβαση σε βασικές υπηρεσίες, όπως ραντεβού υγειονομικής περίθαλψης, συνταξιοδοτικά επιδόματα ή τραπεζικές συναλλαγές.

Αυτή η ψηφιακή μετάβαση μπορεί να αποκλείσει πολλούς, ειδικά ηλικιωμένους ενήλικες ή άτομα με περιορισμένους πόρους, καθιστώντας τους εξαρτημένους από άλλους ή ανίκανους να ολοκληρώσουν σημαντικές εργασίες.

Co-funded by the
European Union

Αυτοματοποιημένη χειραγώγηση των ροών των μέσων κοινωνικής δικτύωσης, παραγωγή παραπληροφόρησης και άγχους

Η αυτοματοποιημένη χειραγώγηση των ροών κοινωνικής δικτύωσης αποτελεί μια κυβερνοαπειλή όπου προγράμματα υπολογιστών, που ονομάζονται bots, και η τεχνητή νοημοσύνη ελέγχουν το περιεχόμενο που βλέπετε στις σελίδες σας στα μέσα κοινωνικής δικτύωσης. Αυτά τα συστήματα αναλύουν τι σας αρέσει, τι κοινοποιείτε ή τι σχολιάζετε και, στη συνέχεια, σας εμφανίζουν περισσότερες παρόμοιες αναρτήσεις για να σας κρατήσουν αφοσιωμένους.

Δυστυχώς, αυτό μπορεί να χρησιμοποιηθεί για τη διάδοση παραπληροφόρησης, ψευδών ειδήσεων ή ακραίου περιεχομένου που προκαλεί άγχος, φόβο ή θυμό. Τα bots μπορούν να ενισχύσουν τεχνητά τη δημοτικότητα τέτοιων αναρτήσεων επισημαίνοντας με like, κοινοποιώντας ή σχολιάζοντας, κάνοντάς τους να φαίνονται ότι πολλοί άνθρωποι συμφωνούν μαζί τους.