LINKS

Co-funded by the European Union

Το πλαίσιο αρμοδιοτήτων ψηφιακής κυριαρχίας

Co-funded by
the European Union

Το έργο αυτό υποστηρίζεται από την Ευρωπαϊκή Επιτροπή μέσω του προγράμματος Erasmus+. Η παρούσα δημοσίευση αντικατοπτρίζει τις απόψεις μόνο του συγγραφέα και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.

Διαβάστε περισσότερα για το έργο

Περιεχόμενα

Εισαγωγή

Το έργο LINKS έχει ως στόχο να υποστηρίξει τους ευρωπαίους εργαζόμενους στον τομέα της νεολαίας να επιτύχουν την κυριαρχία των δεδομένων τους και να ενισχύσουν τις δεξιότητές τους στον τομέα της ψηφιακής ασφάλειας μέσω μιας νέας, καινοτόμου μορφής εκπαιδευτικού περιεχομένου για την υποστήριξη της ανάπτυξης ψηφιακών ικανοτήτων.

Κατά τις αρχικές φάσεις σχεδιασμού αυτού του έργου και της εφαρμογής, η ανάλυση των αναγκών υποστήριξε το γεγονός ότι δεν υπάρχει επί του παρόντος ενιαίο πλαίσιο αρμοδιοτήτων ψηφιακής κυριαρχίας και ασφάλειας για την Ευρώπη.

Το DigComp (Πλαίσιο Ψηφιακών Ικανοτήτων) αναφέρεται σε πολλές από τις γενικότερες και γενικές βασικές δεξιότητες και ικανότητες που σχετίζονται με την ψηφιακή ασφάλεια στο σύνολό της, και το παρόν αποτέλεσμα θα παραπέμπει σε αυτό το υφιστάμενο πλαίσιο ικανοτήτων, αλλά στοχεύει ειδικά στην προληπτική ευαισθητοποίηση των εργαζομένων στον τομέα της νεολαίας σε όλη την Ευρώπη σχετικά με τις απειλές που υπάρχουν σήμερα για την ψηφιακή ασφάλεια.

Το πλαίσιο ικανοτήτων ψηφιακής κυριαρχίας ορίζει τα βασικά συστατικά των ικανοτήτων που χρειάζονται οι εργαζόμενοι στον τομέα της νεολαίας για να ενσωματώσουν αποτελεσματικά τα πρωτόκολλα ψηφιακής κυριαρχίας και ασφάλειας στα τοπικά τους πλαίσια, καθώς και για να παράσχει και να επικυρώσει ένα πλαίσιο αναφοράς της ΕΕ για την ανάπτυξη και την αξιολόγηση
των ικανοτήτων ψηφιακής ασφάλειας. Οι ικανότητες ψηφιακής ασφάλειας συνδέονται σε μεγάλο βαθμό με τις γενικές ψηφιακές ικανότητες και δεν θεωρούνται ικανότητες από μόνες τους.

Το πλαίσιο απευθύνεται στους εργαζόμενους στον τομέα της νεολαίας, αλλά είναι επίσης σχετικό και ενδιαφέρει τους εκπαιδευτικούς και τους εκπαιδευτές ΤΠΕ, καθώς και τους υπεύθυνους χάραξης πολιτικής για την εκπαίδευση και τη δια βίου μάθηση, όσον αφορά την τεχνολογική κατάρτιση και την ανάπτυξη ικανοτήτων των ατόμων.

Αναμένουμε ότι οι ΜΚΟ ψηφιακής εκπαίδευσης και οι εκπαιδευτικοί οργανισμοί σε όλη την Ευρώπη θα υιοθετήσουν το πλαίσιο αυτό ως μέρος των εκπαιδευτικών δραστηριοτήτων αξιολόγησης και διδασκαλίας τους, γεγονός που μακροπρόθεσμα θα αυξήσει την ευαισθητοποίηση και θα ενθαρρύνει την ενσωμάτωση του πλαισίου σε τοπικούς, περιφερειακούς και εθνικούς φορείς ψηφιακής εκπαίδευσης στις ευρωπαϊκές χώρες.

Αποτελέσματα της έρευνας του έργου και των ομάδων εστίασης

Το πλαίσιο ικανοτήτων ψηφιακής κυριαρχίας βασίζεται στη μεθοδολογία και τα ευρήματα της έρευνας και των ομάδων εστίασης του έργου. Προσπαθεί επίσης να ευθυγραμμιστεί με το πλαίσιο DigComp, το οποίο υποστηρίζει τη μακροπρόθεσμη εκμετάλλευση και βιωσιμότητα ως πρόσθετο πλαίσιο ικανοτήτων για συγκεκριμένες ομάδες-στόχους. Η έρευνα του έργου βοήθησε να μάθουμε για τη χρήση της τεχνολογίας και την προστασία των δεδομένων στις πρακτικές ψηφιακής εργασίας των εργαζομένων σε θέματα νεολαίας. Οι
εργαζόμενοι στον τομέα της νεολαίας χρειάζονται μεγαλύτερη ευαισθητοποίηση σε συνδυασμό με την καλή διαχείριση των ψηφιακών ταυτοτήτων, μπορεί να βοηθήσει στον περιορισμό των συμβάντων που προκαλούνται από "απροσεξία" του χρήστη ή του ίδιου του οργανισμού. Έγραψαν για την ανάγκη δημιουργίας και επικοινωνίας πολιτικών ασφαλείας για την απομακρυσμένη εργασία, για τη ρύθμιση της χρήσης προσωπικών συσκευών, την εξασφάλιση
των καναλιών επικοινωνίας και συνεργασίας και την παροχή άγρυπνης υποστήριξης ΤΠ. Συνέστησαν να διατίθενται μαθήματα για περισσότερα μέλη του προσωπικού και νέους, να χρησιμοποιούνται πιο συναφή παραδείγματα σχετικά με συγκεκριμένες εργασίες, να βελτιωθεί η δικτύωση και η ανταλλαγή καλών και κακών εμπειριών στο διαδίκτυο. Είναι σημαντικό να υπάρχει συνεχής ενημέρωση και ιδιαίτερα με τα νέα έγγραφα της ΕΕ.

Ανάγκη του πλαισίου αρμοδιοτήτων ψηφιακής κυριαρχίας

Υπάρχει αυξανόμενη ανησυχία ότι οι πολίτες, οι επιχειρήσεις και τα κράτη μέλη της Ευρωπαϊκής Ένωσης χάνουν σταδιακά τον έλεγχο των δεδομένων τους, την ικανότητά τους για καινοτομία και την ικανότητά τους να διαμορφώνουν και να επιβάλλουν τη νομοθεσία στο ψηφιακό περιβάλλον.Στο πλαίσιο αυτό, αυξάνεται η υποστήριξη για μια νέα πολιτική προσέγγιση που αποσκοπεί στην ενίσχυση της στρατηγικής αυτονομίας της Ευρώπης στον ψηφιακό τομέα.

Οι εταιρείες τεχνολογίας συλλέγουν τεράστιες ποσότητες προσωπικών δεδομένων και η ανησυχία στην ΕΕ έχει αυξηθεί σχετικά με το πώς οι Ευρωπαίοι πολίτες μπορούν να ανακτήσουν τον έλεγχο των ψηφιακών τους δεδομένων σε ένα διαδικτυακό περιβάλλον στο οποίο κυριαρχούν πλέον κυρίως εταιρείες τεχνολογίας εκτός ΕΕ.

Καθώς η εργασία για τη νεολαία προσαρμόζεται όλο και περισσότερο στον ψηφιακό κόσμο, βλέπουμε ότι και οι εργαζόμενοι στον τομέα της νεολαίας υιοθετούν νέες προσεγγίσεις. Ενώ το ψηφιακό είναι νέο και συναρπαστικό, προσφέροντας αμέτρητες ευκαιρίες, απαιτεί ωστόσο καλύτερη κατανόηση στο πλαίσιο της εργασίας με τους νέους. Απαιτούνται περισσότερες δράσεις για τη χαρτογράφηση των υφιστάμενων ψηφιακών πρακτικών, πλατφορμών, εργαλείων και πλαισίων μάθησης της εργασίας με τους νέους, όταν πρόκειται για ικανότητες ψηφιακής κυριαρχίας.

Η ψηφιακή κυριαρχία είναι μια νέα έννοια στην ψηφιακή εποχή, η οποία συνήθως νοείται ως "η ικανότητα των ατόμων να κατέχουν τα προσωπικά τους δεδομένα και να ελέγχουν τη χρήση τους".

Η πανδημία COVID-19 είχε τεράστιες επιπτώσεις στην καθημερινή ζωή των περισσότερων ατόμων. Ως απάντηση, η τεχνολογία προσαρμόστηκε για να προσπαθήσει να μετριάσει αυτές τις επιπτώσεις, προσφέροντας στα άτομα ψηφιακές εναλλακτικές λύσεις για πολλές από τις καθημερινές δραστηριότητες που δεν μπορούν πλέον να ολοκληρωθούν κανονικά. Η εικονική κοινωνικοποίηση και οι διαδικτυακές εκδηλώσεις έχουν γίνει κοινός τόπος και έχουν συμβάλει σε μεγάλο βαθμό στο να μην είναι οι άνθρωποι εντελώς απομονωμένοι ενώ βρίσκονται σε κατάσταση αποκλεισμού.

Η διαδικτυακή εκπαίδευση έχει επίσης γίνει η νέα κανονικότητα σε πολλά μέρη, καθώς τα σχολεία και τα πανεπιστήμια στρέφονται σε διαδικτυακές τάξεις για να διατηρήσουν την εκπαίδευση των φοιτητών σε καλό δρόμο. Επιπλέον, καθώς τα άτομα έχουν πιο ευέλικτα ωράρια ή περισσότερο ελεύθερο χρόνο κατά τη διάρκεια του κλειδώματος, έχει αυξηθεί σημαντικά ο αριθμός των ατόμων που κάνουν χρήση προσωπικών εργαλείων μάθησης και ανάπτυξης, όπως οι εφαρμογές εκμάθησης γλωσσών. Η υγειονομική περίθαλψη έχει επίσης στραφεί σε ψηφιακές λύσεις, και η διαδικτυακή διάθεση τόσο της ψυχικής όσο και της σωματικής υγειονομικής περίθαλψης έχει γίνει πιο συνηθισμένη και είναι αρκετά επιτυχής στο να συμβάλει στον μετριασμό των αρνητικών επιπτώσεων της μειωμένης πρόσβασης στην υγειονομική περίθαλψη.

Υφιστάμενα σχετικά πλαίσια

Διάφορα πλαίσια ψηφιακών παιδαγωγικών ικανοτήτων έχουν αναπτυχθεί για να υποστηρίξουν την αποτελεσματική και ουσιαστική επαγγελματική ανάπτυξη των ψηφιακών παιδαγωγικών ικανοτήτων των επαγγελματιών εκπαιδευτικών βάσει κριτηρίων.

Τα ευρωπαϊκά πλαίσια που δημοσιεύθηκαν τα τελευταία χρόνια περιγράφουν πώς πρέπει να είναι ένας ψηφιακά ικανός εκπαιδευτικός οργανισμός DigCompOrg και ένα ψηφιακά ικανό διδακτικό προσωπικό DigCompEdu, ενθαρρύνοντας τους οργανισμούς να διασφαλίσουν τις ικανότητες του προσωπικού τους και να αναπτύξουν εθνικές λύσεις για τη διασφάλιση της ψηφιακής επάρκειας.

Το DigCompEdu είναι ένα πλαίσιο ψηφιακών ικανοτήτων και έχει ως ομάδα-στόχο κυρίως καθηγητές και μέλη του προσωπικού πανεπιστημίων.
Το πλαίσιο DigComp προσδιορίζει τα βασικά στοιχεία της ψηφιακής ικανότητας σε πέντε τομείς:

1. **Πληροφορική και παιδεία δεδομένων**: Να διατυπώνουν πληροφοριακές ανάγκες, να
εντοπίζουν και να ανακτούν ψηφιακά δεδομένα, πληροφορίες και περιεχόμενο. Να κρίνουν τη συνάφεια της πηγής και του περιεχομένου της. Να αποθηκεύουν, να διαχειρίζονται και να οργανώνουν ψηφιακά δεδομένα, πληροφορίες και περιεχόμενο.
2. **Επικοινωνία και συνεργασία**:Να αλληλεπιδρούν, να επικοινωνούν και να συνεργάζονται μέσω των ψηφιακών τεχνολογιών έχοντας επίγνωση της πολιτισμικής και γενεαλογικής ποικιλομορφίας. Να συμμετέχουν στην κοινωνία μέσω των δημόσιων και ιδιωτικών ψηφιακών υπηρεσιών και της συμμετοχικής ιδιότητας του πολίτη. Να διαχειρίζεται κανείς την ψηφιακή του παρουσία, ταυτότητα και φήμη.
3. **Δημιουργία ψηφιακού περιεχομένου**: Βελτίωση και ενσωμάτωση πληροφοριών και περιεχομένου σε ένα υπάρχον σώμα γνώσεων, κατανοώντας παράλληλα πώς πρέπει να εφαρμόζονται τα πνευματικά δικαιώματα και οι άδειες χρήσης. Να γνωρίζουν πώς να δίνουν κατανοητές οδηγίες για ένα υπολογιστικό σύστημα.
4. **Ασφάλεια**:Προστασία των συσκευών, του περιεχομένου, των προσωπικών
δεδομένων και της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα. Προστασία της σωματικής και ψυχολογικής υγείας και ευαισθητοποίηση στις ψηφιακές τεχνολογίες για την κοινωνική ευημερία και την κοινωνική ένταξη. Να γνωρίζουν τις περιβαλλοντικές επιπτώσεις των ψηφιακών τεχνολογιών και της χρήσης τους.
5. **Επίλυση προβλημάτων**:Εντοπισμός αναγκών και προβλημάτων και επίλυση εννοιολογικών προβλημάτων και προβληματικών καταστάσεων σε ψηφιακά περιβάλλοντα. Χρήση ψηφιακών εργαλείων για την καινοτομία διαδικασιών και προϊόντων. Να συμβαδίζουν με την ψηφιακή εξέλιξη.

Υπάρχει το εννοιολογικό μοντέλο αναφοράς DigComp, όπου 21 ικανότητες αφορούν αυτούς τους τομείς. Πρόσθετες διαστάσεις περιγράφουν τα επίπεδα επάρκειας, τις γνώσεις, τις δεξιότητες και τις στάσεις και τις περιπτώσεις χρήσης.

Το πλαίσιο ικανοτήτων ψηφιακής κυριαρχίας για τους εργαζόμενους στον τομέα της νεολαίας

Με βάση την έρευνα και την ανάλυση των υφιστάμενων πλαισίων, οι εταίροι αυτού του έργου αποφάσισαν να επικεντρωθούν σε τέσσερα θέματα ασφάλειας του DigiComp και να προσθέσουν επίσης ικανότητες που απαιτούνται ειδικά για τους εργαζόμενους σε θέματα νεολαίας. Ακολουθούν οι ικανότητες του πλαισίου DigiComp:

4.1 **Προστασία συσκευών**

Προστασία των συσκευών και του ψηφιακού περιεχομένου και κατανόηση των κινδύνων και των απειλών σε ψηφιακά περιβάλλοντα. Να γνωρίζουν τα μέτρα ασφάλειας και προστασίας και να λαμβάνουν δεόντως υπόψη την αξιοπιστία και την ιδιωτικότητα.

4.2 **Προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής**

Προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα. Να κατανοήσουν πώς να χρησιμοποιούν και να μοιράζονται προσωπικά αναγνωρίσιμες πληροφορίες, ενώ είναι σε θέση να προστατεύουν τον εαυτό τους και τους άλλους από ζημιές.

4.3 **Προστασία της υγείας και της ευημερίας**

Να είναι σε θέση να αποφεύγουν τους κινδύνους για την υγεία και τις απειλές για τη σωματική και ψυχολογική ευεξία κατά τη χρήση των ψηφιακών τεχνολογιών. Να είναι σε θέση να προστατεύουν τον εαυτό τους και τους άλλους από πιθανούς κινδύνους σε ψηφιακά περιβάλλοντα (π.χ.
διαδικτυακός εκφοβισμός). Να γνωρίζουν τις ψηφιακές τεχνολογίες για την κοινωνική ευημερία και την κοινωνική ένταξη.

4.4 **Προστασία του περιβάλλοντος**

Να έχουν επίγνωση των περιβαλλοντικών επιπτώσεων των ψηφιακών τεχνολογιών και της χρήσης τους.
https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety

Κατά τον ορισμό των βασικών ψηφιακών ικανοτήτων για τους εργαζόμενους στον τομέα της νεολαίας, είναι χρήσιμο να σκεφτούμε τόσο τα καθολικά (ικανότητες DigComp για τους πολίτες) όσο και τα ειδικά (καθημερινές δραστηριότητες στην εργασία των νέων) χαρακτηριστικά της προκύπτουσας πρακτικής μάθησης.

Δεξιότητες για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής

*τεχνικές δεξιότητες ψηφιακών τεχνολογιών,
*την ικανότητα χρήσης των ψηφιακών τεχνολογιών με ουσιαστικό τρόπο για εργασία, σπουδές και άλλες καθημερινές δραστηριότητες,
*την ικανότητα κριτικής αξιολόγησης των ψηφιακών τεχνολογιών,
*να γνωρίζουν τους βασικούς κανόνες σχετικά με την ασφάλεια στο διαδίκτυο,
*για να καταλάβετε πώς λειτουργεί το διαδίκτυο,
*να κατανοήσετε τι είναι το e-marketing και πώς λειτουργεί,
*να κατανοούν την προστασία της ιδιωτικής ζωής και να γνωρίζουν τα δικαιώματα πνευματικής ιδιοκτησίας,
* να γνωρίζει πώς να εφαρμόζει μέτρα ασφαλείας,
* να αναπτύξουν αυτοαποτελεσματικότητα με τη χρήση ψηφιακών τεχνολογιών.

Δεξιότητες για τις συσκευές προστασίας

Προστασία του υπολογιστή και του smartphone με ισχυρό, ενημερωμένο λογισμικό ασφαλείας. Εάν ο υπολογιστής ή το τηλέφωνο έχει μολυνθεί με κακόβουλο λογισμικό, οι άλλες διασφαλίσεις δεν βοηθούν ιδιαίτερα, επειδή οι εγκληματίες μπορεί να έχουν ήδη στην κατοχή τους το κλειδί για όλες τις διαδικτυακές ενέργειες. Επίσης, είναι σημαντικό να βεβαιώνεστε ότι έχουν εγκατασταθεί όλες οι ενημερώσεις του λειτουργικού συστήματος. Οι εργαζόμενοι στον τομέα της νεολαίας θα πρέπει να φροντίζουν όλες τις δικές τους συσκευές. Πρέπει να είναι ενημερωμένοι, με ένα αποτελεσματικό λογισμικό προστασίας από ιούς. Διάφοροι κατασκευαστές κυκλοφορούν ενημερώσεις που όχι μόνο βελτιώνουν τα χαρακτηριστικά, αλλά και διορθώνουν τυχόν κενά ασφαλείας που μπορεί να θέσουν τις συσκευές.

Μαθαίνοντας να εντοπίζετε το spam και τις απάτες

Παρόλο που κάποιες από αυτές είναι εύκολο να αναγνωριστούν, άλλες απόπειρες phishing σε ένα email, σε ιστότοπους κοινωνικής δικτύωσης ή σε ιστοσελίδες μπορεί να φαίνονται πολύ νόμιμες. Ο μόνος τρόπος για να μην πέσετε ποτέ θύμα απάτης phishing είναι να μην κάνετε ποτέ κλικ σε έναν σύνδεσμο που έχει σταλεί. Εάν το μήνυμα ηλεκτρονικού ταχυδρομείου λέει ότι είναι από μια τράπεζα και έχει όλα τα σωστά λογότυπα και γνωρίζετε το όνομα, μπορεί να είναι από την πραγματική τράπεζα ή μπορεί και να μην είναι. Αντί να χρησιμοποιήσετε τον σύνδεσμο που παρέχεται, η εύρεση του ιστότοπου και η χρήση μιας μηχανής αναζήτησης μπορεί να βοηθήσει στην πρόληψη της απάτης. Με αυτόν τον τρόπο ο χρήστης θα γνωρίζει αν έχει προσγειωθεί στον νόμιμο ιστότοπο και όχι σε έναν ψεύτικο ιστότοπο που έχει δημιουργηθεί.

Χρήση αξιόπιστων δικτυακών τόπων κατά την πραγματοποίηση αγορών

Εάν ένας χρήστης δεν γνωρίζει τη φήμη μιας εταιρείας από την οποία θέλει να αγοράσει, είναι σημαντικό να μελετήσει τον ιστότοπο πριν το πράξει. Ρωτήστε "Πώς αξιολογούνται από άλλους χρήστες;", "Χρησιμοποιούν ασφαλή, κρυπτογραφημένη σύνδεση για προσωπικές και οικονομικές πληροφορίες;".

Παραμονή σε εγρήγορση

Να είστε επιφυλακτικοί με το δημόσιο WiFi και να σκέφτεστε δύο φορές πριν συνδεθείτε σε ένα μη ασφαλές δίκτυο. Υπάρχουν εργαλεία που μπορούν να βοηθήσουν έναν χρήστη να έχει περισσότερη ιδιωτικότητα και να θωρακιστεί κατά τη διάρκεια της δραστηριότητας περιήγησης από άλλους χρήστες και τους ίδιους τους ιστότοπους σε δημόσια δίκτυα WiFi.

Παραμονή με ασφάλεια στο διαδίκτυο

Ο διαδικτυακός κόσμος έχει γίνει ένα τόσο ταχέως μεταβαλλόμενο περιβάλλον που οι σημερινές συμβουλές μπορεί να είναι ξεπερασμένες αύριο. Οι εργαζόμενοι στον τομέα της νεολαίας πρέπει να γνωρίζουν ότι το περιεχόμενο που καταναλώνουν (και μερικές φορές μπορεί να είναι πραγματικά πολύ) πρέπει να φιλτράρεται. Είναι σημαντικό να είμαστε λίγο καχύποπτοι. Είναι σχετικά εύκολο να πλαστογραφήσετε πράγματα στο Διαδίκτυο. Είναι πολύ εύκολο να τοποθετήσετε στο Διαδίκτυο κάτι που δεν είναι εντελώς αληθινό ή απλώς ένα μάτσο ψέματα. Θα πρέπει να δίνουμε ιδιαίτερη προσοχή στο να μην πιστεύουμε σε ό,τι βλέπουμε και διαβάζουμε στο Διαδίκτυο. Ως καλή συμβουλή, θα πρέπει να ψάξουμε βαθύτερα για να διακρίνουμε τι είναι αληθινό και τι όχι, σε περίπτωση που έχουμε έστω και την παραμικρή αμφιβολία για οτιδήποτε. Προσπαθήστε να είστε κριτικοί απέναντι στα πράγματα στο διαδίκτυο και έτσι να ελαχιστοποιήσετε τον κίνδυνο που ενέχει οποιαδήποτε διαδικτυακή δραστηριότητα.

Κοινή χρήση πληροφοριών σε κοινωνικό δίκτυο

"Η κοινή χρήση πληροφοριών περιγράφει την ανταλλαγή δεδομένων μεταξύ διαφόρων οργανισμών, ανθρώπων και τεχνολογιών" (Techopedia). Υπάρχουν διάφοροι τύποι ανταλλαγής
πληροφοριών:

- Πληροφορίες που μοιράζονται άτομα (όπως ένα βίντεο που μοιράζεται στο Facebook ή στοYouTube),
- Πληροφορίες που διαμοιράζονται από οργανισμούς (όπως η ροή RSS ενός διαδικτυακούδελτίου καιρού),
- Πληροφορίες που μοιράζονται μεταξύ υλικολογισμικού/λογισμικού (όπως οι διευθύνσεις IP των διαθέσιμων κόμβων δικτύου ή η διαθεσιμότητα του χώρου στο δίσκο)

Όλα τα κοινωνικά δίκτυα (ή τα περισσότερα από αυτά) επιτρέπουν στους χρήστες ναδημιουργούν προφίλ όσο λεπτομερή θέλουν. Σε ορισμένες περιπτώσεις, η διαδικασία αυτή βοηθά τους χρήστες να βρουν άλλους χρήστες με κοινά ενδιαφέροντα κ.ο.κ. Σε κοινωνικά δίκτυα όπως το Facebook, είναι δυνατή η αλλαγή των ρυθμίσεων απορρήτου προκειμένου να ελέγχεται ποιες πληροφορίες είναι δημόσιες και ποιες πληροφορίες διατηρούνται μόνο για τους "φίλους". Είναι
σημαντικό να γνωρίζετε, ωστόσο, ότι το ίδιο το κοινωνικό δίκτυο διαθέτει αυτές τις πληροφορίες ανεξάρτητα από τη ρύθμιση απορρήτου.

Συνήθως οι άνθρωποι μοιράζονται την ηλικία, το φύλο, την οικογένεια, άλλα ενδιαφέροντα, το εκπαιδευτικό υπόβαθρο και λεπτομέρειες που σχετίζονται με τη δική τους απασχόληση.Η ανάρτηση φωτογραφιών ή το "status" είναι ένας γρήγορος τρόπος για να δείξουν συναισθήματα, καταστάσεις και να μοιράζονται πληροφορίες. Τα περισσότερα κοινωνικά δίκτυα έχουν σχεδιαστεί για να το επιτυγχάνουν αυτό με τον ταχύτερο δυνατό τρόπο. Είναι πολύ σημαντικό να γνωρίζετε ποια είναι τα πράγματα που μοιράζεται ένας χρήστης. Ο διαμοιρασμός εκθέτει τις πληροφορίες που επιτρέπουν στους διαφημιστές να εντοπίζουν τις προτιμήσεις και τις προτιμήσεις των δυνητικών καταναλωτών.

GDPR

Ο ΓΚΠΔ εφαρμόστηκε σε όλα τα μέλη της ΕΕ και του ΕΟΧ από τις 25 Μαΐου 2018. Αντικατέστησε τη σημερινή νομοθεσία σχετικά με την προστασία της ιδιωτικής ζωής στις χώρες μέλη που υπόκεινται επί του παρόντος στην οδηγία 95/46 της ΕΕ. Ο ΓΚΠΔ είναι λεπτομερέστερος και ακριβέστερος σε ορισμένους τομείς και λαμβάνει υπόψη τις προκλήσεις του ταχέως εξελισσόμενου ψηφιακού κόσμου, δημιουργώντας κινδύνους για την προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων.

Δικαιώματα πνευματικής ιδιοκτησίας

Όλο το περιεχόμενο στο Διαδίκτυο ανήκει σε κάποιον και το πρόσωπο αυτό (ή μια οντότητα) κατέχει τα σχετικά δικαιώματα πνευματικής ιδιοκτησίας. Σε ορισμένες περιπτώσεις, οι ιδιοκτήτες παραιτούνται από τα δικαιώματά τους και επιτρέπουν την ελεύθερη χρήση του περιεχομένου από άλλους. Οι κάτοχοι πνευματικών δικαιωμάτων μπορούν να συμφωνήσουν να χρησιμοποιείται ελεύθερα το περιεχόμενό τους για ιδιωτικούς σκοπούς, αλλά όχι για εμπορικούς.
Τα κύρια αποτελέσματα είναι:

- Αυξημένη αυτοεκτίμηση / αυτογνωσία / αυτοαναστοχασμός.
- Ενδυνάμωση και αυτοπεποίθηση.
- Νέες ευκαιρίες μάθησης.
- Ερέθισμα και κίνητρο για περαιτέρω μάθηση.
- Πρόσβαση σε υψηλότερο επίπεδο σπουδών.
- Απόκτηση αποδεικτικών στοιχείων για την υποβολή αίτησης για απασχόληση στον τομέα της εργασίας με νέους.

Αναφορές

Data protection and online privacy
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm
Techopedia https://www.techopedia.com/definition/24839/information-sharing
Step by step guidelines on setting up your computer and creating a user
https://www.wikihow.com/Use-a-Computer
Privacy rights
https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and -social