
DIGI
WELL

Co-funded by the European Union

Οικοδόμηση ψηφιακής ανθεκτικότητας καθιστώντας την ψηφιακή ευημερία και ασφάλεια προσβάσιμες σε όλους

DigiWELL

2022-2-SK01-KA220-ADU-000096888

Εγχειρίδιο & Μεθοδολογία οικοδόμησης ψηφιακής ανθεκτικότητας

Σεπτέμβριος, 2023

Πίνακας περιεχομένων

Περίληψη

Μετά την πανδημία COVID-19, ορισμένες ανάγκες έχουν γίνει ζωτικής σημασίας λόγω της χρήσης των ψηφιακών τεχνολογιών και του διαδικτύου, που είναι πολύ έντονα στη ζωή μας. Η πιο σημαντική από αυτές είναι να μπορούμε να κάνουμε ασφαλείς συναλλαγές στον ψηφιακό κόσμο χωρίς να υποστούμε ζημιές. Ειδικά οι ενήλικες χρειάζονται μέτρα ψηφιακής ασφάλειας και κάποιες ικανότητες προκειμένου να προστατευτούν από τις απειλές του κυβερνοχώρου. Επίσης, το διαδίκτυο και οι ψηφιακές τεχνολογίες όχι μόνο διευκολύνουν τη ζωή, αλλά δημιουργούν και κάποια αρνητικά ψυχολογικά προβλήματα. Για παράδειγμα, ο διαδικτυακός εκφοβισμός έχει γίνει ένα δύσκολο πρόβλημα για να αντιμετωπιστεί. Κατά συνέπεια, η διασφάλιση της ευημερίας στον ψηφιακό κόσμο έχει γίνει πλέον αναγκαιότητα στις σημερινές συνθήκες. Και πάλι, σε σχέση με αυτό το θέμα, η αυξανόμενη χρήση της ψηφιακής τεχνολογίας και το σημείο στο οποίο έφτασε ο ψηφιακός μετασχηματισμός έχουν φέρει στην ατζέντα των ανθρώπων ορισμένα ζητήματα όπως η ψηφιακή κόπωση.

Στο πλαίσιο αυτό, το έργο DigiWELL στοχεύει στην ενσωμάτωση των αρχών της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων. Οι πρωτοβουλίες του είναι προς την κατεύθυνση της συμβολής στις συνολικές πρακτικές των οργανισμών, δικτύων και πρωτοβουλιών εκπαίδευσης ενηλίκων. Το έργο κατανοεί πόσο κρίσιμο είναι να αντιμετωπιστεί ο τρόπος με τον οποίο η τεχνολογία επηρεάζει την ψυχική υγεία, την παραγωγικότητα και τη γενική ευημερία των ενηλίκων στην ψηφιακή εποχή. Ο κύριος στόχος του DigiWELL είναι να παρέχει στους ενήλικες εκπαιδευόμενους τις πληροφορίες, τις ικανότητες και τους πόρους που είναι απαραίτητοι για την ηθική και ενσυνείδητη πλοήγηση στον ψηφιακό κόσμο. Το έργο DigiWELL περιλαμβάνει επίσης τη δημιουργία και εκτέλεση πρόσθετων πρωτοβουλιών ενδυνάμωσης των ενήλικων εκπαιδευομένων. Στόχος αυτών των δραστηριοτήτων είναι η παροχή ενός υποστηρικτικού περιβάλλοντος όπου οι ενήλικες μπορούν να μοιραστούν τις εμπειρίες, τις δυσκολίες και τους θριάμβους τους στην προώθηση της ψηφιακής ευημερίας. Με αυτό το σκεπτικό, το έργο DigiWELL παρουσιάζει πολλές ευκαιρίες για τα άτομα και τους οργανισμούς ενηλίκων να ευαισθητοποιηθούν και να διαφωτιστούν σχετικά με τη σημασία της ψηφιακής ευημερίας και με τον τρόπο προώθησης της ψηφιακής ευημερίας των ενήλικων ατόμων και των εκπαιδευτών και εκπαιδευτών ενηλίκων. Η ενεργοποίηση της ψηφιακής ευημερίας με μια ολιστική προσέγγιση είναι πολύ πιο εφικτή εάν όλα τα σχετικά μέρη αναλάβουν δράση για την υποστήριξη των αναγκών ψηφιακής ευημερίας των ατόμων. Κατά συνέπεια, οι πληροφορίες, οι συμβουλές και οι καλές πρακτικές που παρουσιάζονται στο παρόν εγχειρίδιο καλούν τους ανθρώπους και τους ενδιαφερόμενους οργανισμούς να αναλάβουν πρωτοβουλίες ώστε περισσότεροι από εμάς να έχουμε καλύτερη ψηφιακή ευημερία και επίσης ισχυρότερη ψηφιακή ζωή.

1. Εισαγωγή

1.1. Στόχος της μεθόδου & Manuel

- Συμβολή στην παροχή δυνατότητας ψηφιακής ευημερίας και ψηφιακής ασφάλειας, προσβάσιμης σε όλους, μέσω της ενθάρρυνσης και της ενημέρωσης των ενηλίκων σχετικά με την ψηφιακή ευημερία και την ψηφιακή ασφάλεια και τις απαραίτητες ικανότητες για αυτές.
- Να εισαγάγει την ψηφιακή ανθεκτικότητα, την ψηφιακή ευημερία και την ψηφιακή ασφάλεια, το πλαίσιο της ορολογίας και τις βέλτιστες πρακτικές της ψηφιακής ευημερίας και της ψηφιακής ασφάλειας σε όλους τους ανθρώπους.
- Διασφάλιση της πολυπολιτισμικότητας, προσαρμογή των αποτελεσμάτων που αναπτύχθηκαν σε σχετικές οργανώσεις στις χώρες εταίρους.

1.2. Πλαίσιο DigComp της ΕΕ

Στο DigComp, η ψηφιακή επάρκεια περιλαμβάνει την "σίγουρη, κριτική και υπεύθυνη χρήση και εμπλοκή με τις ψηφιακές τεχνολογίες για τη μάθηση, την εργασία και τη συμμετοχή στην κοινωνία. Ορίζεται ως ένας συνδυασμός γνώσεων, δεξιοτήτων και στάσεων". (Σύσταση του Συμβουλίου σχετικά με τις βασικές ικανότητες για τη δια βίου μάθηση, 2018).

Το πλαίσιο DigComp προσδιορίζει τα βασικά στοιχεία της ψηφιακής ικανότητας σε 5 τομείς. Οι τομείς συνοψίζονται παρακάτω:

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.

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.

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.

Ασφάλεια: 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.

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.

Μία από τις βασικές αρμοδιότητες στον τομέα της ασφάλειας είναι η προστασία της υγείας και της ευημερίας. Προστασία της υγείας και της ευημερίας σημαίνει: (α) να είναι σε θέση να αποφεύγει κινδύνους για την υγεία και απειλές για τη σωματική και ψυχολογική ευημερία κατά τη χρήση ψηφιακών τεχνολογιών, (β) να είναι σε θέση να προστατεύει τον εαυτό του και τους άλλους από πιθανούς κινδύνους σε ψηφιακά περιβάλλοντα (π.χ. εκφοβισμός στον κυβερνοχώρο) και (γ) να γνωρίζει τις ψηφιακές τεχνολογίες για την κοινωνική ευημερία και την κοινωνική ένταξη.

1.3. Γιατί η M&M είναι μια καλή πηγή για ενήλικες

Όπως αναφέρθηκε παραπάνω, μετά την πανδημία COVID-19, ορισμένες ανάγκες έχουν γίνει ζωτικής σημασίας λόγω της χρήσης των ψηφιακών τεχνολογιών και του διαδικτύου, που είναι πολύ έντονα στη ζωή μας. Η πιο σημαντική από αυτές είναι να μπορούμε να κάνουμε ασφαλείς συναλλαγές στον ψηφιακό κόσμο χωρίς να υποστούμε ζημιές. Ειδικά οι ενήλικες χρειάζονται μέτρα ψηφιακής ασφάλειας και κάποιες ικανότητες προκειμένου να προστατευτούν από τις απειλές του κυβερνοχώρου. Επίσης, το διαδίκτυο και οι ψηφιακές τεχνολογίες όχι μόνο διευκολύνουν τη ζωή, αλλά δημιουργούν και κάποια αρνητικά ψυχολογικά προβλήματα. Για παράδειγμα, ο διαδικτυακός εκφοβισμός έχει γίνει ένα δύσκολο πρόβλημα για να αντιμετωπιστεί. Κατά συνέπεια, η διασφάλιση της ευημερίας στον ψηφιακό κόσμο έχει γίνει πλέον αναγκαιότητα στις σημερινές συνθήκες. Και πάλι, σε σχέση με το θέμα αυτό, η αυξανόμενη χρήση της ψηφιακής τεχνολογίας και το σημείο στο οποίο έφτασε ο ψηφιακός μετασχηματισμός έχουν φέρει στην ατζέντα των ανθρώπων ορισμένα ζητήματα όπως η ψηφιακή κόπωση.

Αυτό το εγχειρίδιο χρησιμοποιεί όσο το δυνατόν περισσότερα παραδείγματα από τον πραγματικό κόσμο και αφήνει τους ενήλικες εκπαιδευόμενους να καταλάβουν μόνοι τους κάποιες έννοιες για να υποστηρίξει την εκπαίδευση ενηλίκων με βάση τον Knowles (1968).

1.4. Γιατί η M&M είναι μια καλή πηγή για τους εκπαιδευτές ενηλίκων

Η κατάρτιση και η εκπαίδευση διαδραματίζουν κρίσιμο ρόλο στην ενίσχυση της ευαισθητοποίησης σχετικά με την ψηφιακή ασφάλεια, ενδυναμώνοντας τα άτομα με τις γνώσεις, τις δεξιότητες και τις βέλτιστες πρακτικές που απαιτούνται για την προστασία των ίδιων και των οργανισμών τους από τις απειλές στον κυβερνοχώρο. Επιπλέον, η κατάρτιση

και η εκπαίδευση για την ψηφιακή ασφάλεια αποτελούν ουσιώδη στοιχεία για την οικοδόμηση μιας ισχυρής κουλτούρας κυβερνοασφάλειας. Με τον σχεδιασμό εκπαιδευτικών προγραμμάτων που είναι προσαρμοσμένα στις συγκεκριμένες ανάγκες και ρόλους εξοπλίζουν τους ενήλικες με τις γνώσεις και τις δεξιότητες που απαιτούνται για τον εντοπισμό και την αποτελεσματική αντιμετώπιση των απειλών στον κυβερνοχώρο.

Η κατάρτιση βοηθά τα άτομα να κατανοήσουν τους διάφορους τύπους απειλών στον κυβερνοχώρο, όπως το phishing, το κακόβουλο λογισμικό, η κοινωνική μηχανική και το ransomware. Αναγνωρίζοντας αυτές τις απειλές, τα άτομα μπορούν να είναι πιο προσεκτικά και επιφυλακτικά κατά τη χρήση ψηφιακών πλατφορμών. Η εκπαίδευση μπορεί να διδάξει στα άτομα πώς να αναγνωρίζουν τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα ή τους ιστότοπους phishing. Μαθαίνουν να εντοπίζουν ύποπτα στοιχεία και να αποφεύγουν να κάνουν κλικ σε κακόβουλους συνδέσμους ή να παρέχουν ευαίσθητες πληροφορίες. Ταυτόχρονα, η εκπαίδευση περιλαμβάνει οδηγίες για την ασφάλεια των κινητών συσκευών, την προστασία τους με κωδικούς πρόσβασης, τη χρήση κρυπτογράφησης και την προσοχή στις λήψεις εφαρμογών, ενώ διασφαλίζει ότι τα άτομα γνωρίζουν τους σχετικούς κανονισμούς για την κυβερνοασφάλεια και τις απαιτήσεις συμμόρφωσης, γεγονός που συμβάλλει στη διατήρηση νομικών και ηθικών πρακτικών. Τέλος, μέσω της εκπαίδευσης, τα άτομα κατανοούν ότι η ασφάλεια στον κυβερνοχώρο αποτελεί κοινή ευθύνη και ότι η ενεργός συμμετοχή όλων είναι απαραίτητη για τη διατήρηση ενός ασφαλούς περιβάλλοντος, ενώ εμπεδώνει καλές συνήθειες κυβερνοασφάλειας, ενθαρρύνοντας τα άτομα να εφαρμόζουν μέτρα ασφαλείας τόσο στην εργασία όσο και στην προσωπική τους ζωή.

Το έργο DigiWELL στοχεύει στην αντιμετώπιση των αναγκών ψηφιακής ασφάλειας και ευημερίας των ενηλίκων που δεν γεννήθηκαν στην εποχή του Διαδικτύου. Θα το επιτύχει αυτό δημιουργώντας και αναπτύσσοντας ευέλικτες ευκαιρίες μάθησης που ανταποκρίνονται στις ειδικές μαθησιακές απαιτήσεις των ενηλίκων. Το έργο θα επικεντρωθεί στην ενίσχυση της ψηφιακής ανθεκτικότητας μέσω μιας μικτής μαθησιακής προσέγγισης. Ειδικά το παρόν εγχειρίδιο συμβάλλει στον παραπάνω στόχο, καθώς δημιουργεί μια κουλτούρα με επίγνωση της ασφάλειας που αμύνεται ενεργά κατά των απειλών στον κυβερνοχώρο και προστατεύει τα ψηφιακά περιουσιακά στοιχεία και τις ευαίσθητες πληροφορίες.

Με άλλα λόγια, ένα εγχειρίδιο με μια ενότητα αφιερωμένη στην ψηφιακή ασφάλεια μπορεί να διαδραματίσει σημαντικό ρόλο στον εφοδιασμό των ενηλίκων με τις απαραίτητες δεξιότητες και γνώσεις για την προστασία τους στην ψηφιακή εποχή, προωθώντας μια ασφαλέστερη και ασφαλέστερη διαδικτυακή εμπειρία τόσο για τα άτομα όσο και για τις κοινότητες. Το DigiWELL είναι μια πολύτιμη πηγή για τους ενήλικες, καθώς εκπαιδεύει τους ενήλικες σχετικά με τους πιθανούς κινδύνους, βοηθώντας τους να κατανοήσουν τη σημασία της ασφάλειας στον κυβερνοχώρο και τον τρόπο με τον οποίο μπορούν να προστατευτούν στο διαδίκτυο. Τέλος, προσφέρει πρακτική καθοδήγηση για την εφαρμογή μέτρων ψηφιακής ασφάλειας και ενδυναμώνει τους ενήλικες να περιηγηθούν στον ψηφιακό κόσμο με αυτοπεποίθηση και χρησιμεύει ως οδηγός αναφοράς, τον οποίο οι ενήλικες μπορούν να

επισκέπτονται εκ νέου κάθε φορά που αντιμετωπίζουν νέες προκλήσεις ψηφιακής ασφάλειας ή χρειάζονται μια ανανέωση σε ορισμένα θέματα.

1.5. Λεξικό του έργου DigiWELL και πώς να το χρησιμοποιήσετε

Στόχος του λεξικού είναι να εισαγάγει τους ενήλικες χρήστες των ψηφιακών τεχνολογιών στους βασικούς όρους και ορισμούς που σχετίζονται με την ψηφιακή ευημερία, την ψηφιακή ασφάλεια και την ψηφιακή ανθεκτικότητα.

Ταξινόμηση των όρων

Όσον αφορά το περιεχόμενο, το λεξικό περιέχει 3 βασικές κατηγορίες όρων,

1. Όροι και ορισμοί από τον τομέα των τεχνολογιών πληροφορικής και επικοινωνιών (ψηφιακές τεχνολογίες σύμφωνα με το σχέδιο).
2. Όροι και ορισμοί από τον τομέα της πληροφορικής, της κυβερνοασφάλειας και της ψηφιακής ασφάλειας (ψηφιακή ασφάλεια σύμφωνα με το έργο).
3. Όροι και ορισμοί που καθορίζονται από τους στόχους του έργου: ψηφιακή ευημερία και ψηφιακή ανθεκτικότητα. Οι όροι αυτοί είναι σχετικά νέοι και αποτελούν μέρος της έρευνας γραφείου των ομάδων έργου. Θα πρέπει να τονιστεί ότι δεν υπάρχει ενιαίος ορισμός αυτών των όρων. Η κατηγορία αυτή περιλαμβάνει επίσης όρους από τον τομέα της ψυχικής και σωματικής υγείας, π.χ. ψηφιακός εθισμός, ψηφιακή κόπωση/εξάντληση, ψηφιακή αποτοξίνωση κ.λπ.

Ανακοίνωση: Στη βάση δεδομένων κειμένου ενός λεξικού, ένας όρος μπορεί να έχει περισσότερους από έναν ορισμούς για πολλούς λόγους: ο αρχικός ορισμός έχει εξελιχθεί με την πάροδο του χρόνου, ο ευρύς ορισμός είναι προσαρμοσμένος σε μια συγκεκριμένη περιοχή, οι ορισμοί των όρων είναι παρόμοιοι αλλά με λεπτές διαφορές κ.λπ.

Όροι και ορισμοί

Ψηφιακή ανθεκτικότητα: 1. Ψηφιακή ανθεκτικότητα σημαίνει να έχεις την επίγνωση, τις δεξιότητες, την ευελιξία και την αυτοπεποίθηση να χρησιμοποιείς τις νέες τεχνολογίες και να προσαρμόζεσαι στις μεταβαλλόμενες απαιτήσεις ψηφιακών δεξιοτήτων. Η ψηφιακή ανθεκτικότητα βελτιώνει την ικανότητα επίλυσης προβλημάτων και αναβάθμισης των δεξιοτήτων, καθώς και την ικανότητα πλοήγησης στους ψηφιακούς μετασχηματισμούς. 2. Ψηφιακή ανθεκτικότητα είναι η ικανότητα των νέων να αναπτύσσουν κριτική νοοτροπία κατά την πρόσβαση σε ψηφιακές πληροφορίες, ώστε να μειώνουν την ευπάθειά τους σε δυνητικά επιβλαβείς πληροφορίες. 3. Ως ψηφιακή ανθεκτικότητα νοείται "η διαδικασία καλής

προσαρμογής στις ψηφιακές πηγές άγχους και η ανάπτυξη δεξιοτήτων για τη διαχείριση των επιπτώσεων των συνεχώς μεταβαλλόμενων ψηφιακών περιβαλλόντων και εφαρμογών".

Ψηφιακή ασφάλεια: Ψηφιακή ασφάλεια: Η ψηφιακή ασφάλεια είναι η προστασία της ψηφιακής ταυτότητας, καθώς αντιπροσωπεύει μια φυσική ταυτότητα στο δίκτυο ή στις υπηρεσίες διαδικτύου. Η ψηφιακή ασφάλεια είναι ένα σύνολο βέλτιστων πρακτικών και εργαλείων που χρησιμοποιούνται για την προστασία των προσωπικών δεδομένων και της διαδικτυακής ταυτότητας στον διαδικτυακό κόσμο. Παραδείγματα εργαλείων είναι: διαδικτυακές υπηρεσίες, λογισμικό προστασίας από ιούς, κάρτες SIM για smartphones, βιομετρικές και ασφαλείς προσωπικές συσκευές, διαχειριστές κωδικών πρόσβασης, γονικός έλεγχος κ.λπ.

Ψηφιακή ευημερία: 1. Η ψηφιακή ευημερία περιγράφει την ικανότητα ενός ατόμου να διαχειρίζεται αποτελεσματικά τις αρνητικές επιπτώσεις της τεχνολογίας στην επαγγελματική και προσωπική του ζωή. Στόχος της ψηφιακής ευημερίας είναι η προώθηση της υγιούς χρήσης των τεχνολογικών συσκευών και των ψηφιακών υπηρεσιών. 2. Μια κατάσταση προσωπικής ευημερίας που βιώνεται μέσω της υγιούς χρήσης της ψηφιακής τεχνολογίας. 3. Η ψηφιακή ευημερία καλύπτει τους τρόπους με τους οποίους η τεχνολογία της πληροφορικής - συμπεριλαμβανομένων των επικοινωνιών και των αισθητήρων - μπορεί να βοηθήσει τους ανθρώπους να ζήσουν μια μακρά και υγιή ζωή.

Ψηφιακή επάρκεια: Αυτοπεποίθηση, κριτική και υπεύθυνη χρήση και εμπλοκή με τις ψηφιακές τεχνολογίες για τη μάθηση, την εργασία και τη συμμετοχή στην κοινωνία. Ορίζεται ως συνδυασμός γνώσεων, δεξιοτήτων και στάσεων.

Ψηφιακός εθισμός: Ο ψηφιακός εθισμός είναι ένας επιβλαβής εθισμός στα ψηφιακά μέσα, τις συσκευές και το διαδίκτυο που χαρακτηρίζεται από την υπερβολική χρήση τους με τρόπο που έχει αρνητικό αντίκτυπο στη ζωή του χρήστη.

Ψηφιακές δεξιότητες: Ψηφιακές δεξιότητες είναι ένα φάσμα ικανοτήτων χρήσης ψηφιακών συσκευών, εφαρμογών επικοινωνίας και δικτύων για την πρόσβαση και τη διαχείριση πληροφοριών. Επιτρέπουν στους ανθρώπους να δημιουργούν και να μοιράζονται ψηφιακό περιεχόμενο, να επικοινωνούν και να συνεργάζονται και να επιλύουν προβλήματα για αποτελεσματική και δημιουργική αυτοεκπλήρωση στη ζωή, τη μάθηση, την εργασία και τις κοινωνικές δραστηριότητες.

Απειλή στον κυβερνοχώρο: Οποιαδήποτε περίσταση ή γεγονός που μπορεί να επηρεάσει αρνητικά οργανισμούς/ατομικά πρόσωπα μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης πληροφοριών ή/και άρνησης παροχής υπηρεσιών. Στόχος είναι η κλοπή/καταστροφή δεδομένων ή η διατάραξη της ψηφιακής ευημερίας.

Διαδικτυακός εκφοβισμός: Ένας όρος για διάφορες μορφές εκφοβισμού στον ηλεκτρονικό χώρο, κατά τις οποίες ένα ή περισσότερα άτομα χρησιμοποιούν την ψηφιακή τεχνολογία για να βλάψουν σκόπιμα και επανειλημμένα ένα άλλο άτομο (π.χ. στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου ή στιγμιαία μηνύματα, δημοσιεύοντας σχόλια σε κοινωνικά δίκτυα ή δημόσια φόρουμ).

Κυβερνοασφάλεια: Στόχος της είναι η προστασία του κυβερνοχώρου (δηλ. δίκτυα, ενδοδίκτυα, διακομιστές, πληροφορίες, συστήματα και υποδομές πληροφορικής και υπολογιστών) από μη εξουσιοδοτημένη πρόσβαση, κυβερνοεπιθέσεις ή ζημιές. Η κυβερνοασφάλεια επικεντρώνεται στην προστασία των πληροφοριών σε ηλεκτρονική/ψηφιακή μορφή που βρίσκονται σε υπολογιστές, αποθηκευτικούς χώρους και δίκτυα (στον κυβερνοχώρο).

Ψηφιακό απόρρητο: Η ψηφιακή ιδιωτικότητα είναι η ικανότητα ενός ατόμου να ελέγχει και να προστατεύει την πρόσβαση και τη χρήση των προσωπικών του πληροφοριών κατά την πρόσβαση στο διαδίκτυο. Το ψηφιακό απόρρητο βοηθά τα άτομα να παραμένουν ανώνυμα στο διαδίκτυο, προστατεύοντας προσωπικά αναγνωρίσιμες πληροφορίες όπως ονόματα, διευθύνσεις, αριθμούς κοινωνικής ταυτότητας, στοιχεία πιστωτικών καρτών κ.λπ.

Ψηφιακή ασφάλεια vs. Ασφάλεια στον κυβερνοχώρο vs. Ασφάλεια πληροφοριών: Ασφάλεια πληροφοριών: προστατεύει τις πληροφορίες (σε οποιαδήποτε μορφή και μορφή) και τα συστήματα πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και χρήση για την εξασφάλιση και τη διατήρηση της ιδιωτικότητας των σημαντικών δεδομένων. Ασφάλεια στον κυβερνοχώρο: προστατεύει ολόκληρα δίκτυα και συστήματα επικοινωνίας, συστήματα υπολογιστών και άλλα ψηφιακά στοιχεία και τα ψηφιακά δεδομένα που είναι αποθηκευμένα σε αυτά. Ψηφιακή ασφάλεια: προστατεύει τη διαδικτυακή παρουσία (ταυτότητα και σχετικές ευαίσθητες πληροφορίες, περιουσιακά στοιχεία.

Βέλτιστη πρακτική: Μια αποδεδειγμένη μέθοδος ή διαδικασία που προσφέρει την πιο αποτελεσματική λύση σε έναν συγκεκριμένο τομέα, που αποδεδειγμένα οδηγεί σε βέλτιστα αποτελέσματα και έχει καθιερωθεί (προταθεί) ως κατάλληλο πρότυπο για ευρεία υιοθέτηση. Στην ψηφιακή ασφάλεια, πρόκειται για καθορισμένες διαδικασίες που διασφαλίζουν την

προστασία ενός ατόμου/οργανισμού στον ψηφιακό χώρο (π.χ. συνιστώμενες τεχνικές, προγράμματα, οδηγίες, εγχειρίδια).

2. Ψηφιακή ευημερία

2.1. Τι είναι η ευημερία;

Ο όρος "**ευημερία**" περιγράφει την κατάσταση του να είσαι ευχαριστημένος, χαρούμενος και υγιής. Περιλαμβάνει τη σωματική, νοητική και συναισθηματική ευεξία ενός ατόμου, μεταξύ άλλων τομέων της ύπαρξής του. Πέρα από το να είναι κανείς απλώς απαλλαγμένος από ασθένειες ή δυσφορία, η ευημερία εστιάζει στη συνολική ευτυχία και την ποιότητα ζωής.

Η σωματική ευεξία είναι η κατάσταση του σώματος ενός ατόμου, λαμβάνοντας υπόψη πράγματα όπως η φυσική κατάσταση, η διατροφή και η απουσία ασθενειών ή νοσημάτων. Περιλαμβάνει τη διατήρηση ενός υγιεινού τρόπου ζωής μέσω της συνεπούς άσκησης, της θρεπτικής διατροφής, του επαρκούς ύπνου και της διαχείρισης του άγχους.

Η γνωστική και συναισθηματική υγεία ενός ατόμου σχετίζεται με την ***ψυχική του ευεξία***. Συνεπάγεται την ύπαρξη καλών προοπτικών, τη βίωση ικανοποίησης και την ικανότητα να διαχειρίζεται το άγχος και τις δυσκολίες της ζωής. Δραστηριότητες όπως η εξάσκηση της ενσυνειδητότητας, η ενασχόληση με ένα χόμπι, η αναζήτηση υποστήριξης από αγαπημένα πρόσωπα και η λήψη επαγγελματικής βοήθειας όταν είναι απαραίτητο μπορούν να συμβάλουν στη θρέψη της ψυχικής ευεξίας του ατόμου.

Η καλή κατανόηση και η ικανότητα ελέγχου των συναισθημάτων αναφέρεται ως ***συναισθηματική ευημερία***. Περιλαμβάνει την καλλιέργεια της ανθεκτικότητας, τη διατήρηση καλών σχέσεων και τη θετική αίσθηση του εαυτού μας. Η αυτογνωσία, ο συναισθηματικός έλεγχος, η αποτελεσματική επικοινωνία και η ανάπτυξη υποστηρικτικών σχέσεων συμβάλλουν στη συναισθηματική ευημερία.

Η ποιότητα των δεσμών ενός ατόμου και η αίσθηση του ανήκειν στην κοινότητα είναι όλα μέρη της ***κοινωνικής ευημερίας***. Συνεπάγεται την καλλιέργεια διαρκών δεσμών με στενά αγαπημένα πρόσωπα, στενούς φίλους και ένα ευρύτερο κοινωνικό δίκτυο. Η συμμετοχή σε κοινωνικές δραστηριότητες, η προσφορά στην κοινότητα και η διατήρηση του αισθήματος σύνδεσης και του ανήκειν μπορούν να βελτιώσουν την κοινωνική ευημερία.

Συνολικά, **η ευημερία** είναι μια ολοκληρωμένη ιδέα που εξετάζει τον τρόπο με τον οποίο οι διάφορες πτυχές της ζωής ενός ατόμου είναι αλληλένδετες. Περιλαμβάνει την ενεργή αναζήτηση μιας ισορροπημένης και ικανοποιητικής ύπαρξης, τη φροντίδα της σωματικής και ψυχικής υγείας, την καλλιέργεια υγιών σχέσεων και την εξεύρεση νοήματος στη ζωή.

2.2. Ευημερία και ψηφιοποίηση

Επιτρέποντας την επικοινωνία, ενισχύοντας την αποδοτικότητα και βελτιώνοντας την πρόσβαση σε πληροφορίες, η τεχνολογία και η ψηφιοποίηση έχουν τη δυνατότητα να βελτιώσουν την ευημερία. Για τη διαχείριση της ψηφιακής χρήσης, τη διασφάλιση της ιδιωτικής ζωής και της ασφάλειας και την επίτευξη μιας καλής ισορροπίας μεταξύ της τεχνολογίας και άλλων πτυχών της ζωής, είναι ζωτικής σημασίας να γνωρίζετε τα πιθανά μειονεκτήματα και να λαμβάνετε τις απαραίτητες προφυλάξεις.

Η τεχνολογία και η ψηφιοποίηση έχουν βελτιώσει σημαντικά την πρόσβαση σε πληροφορίες και υπηρεσίες, γεγονός που έχει θετικό αντίκτυπο στην ευημερία. Οι άνθρωποι έχουν πλέον εύκολη πρόσβαση σε ψηφιακά εργαλεία για προσωπική ανάπτυξη, πληροφορίες για την υγειονομική περίθαλψη, διαδικτυακές ομάδες υποστήριξης και εκπαιδευτικούς πόρους. Μέσω της απρόσκοπτης επικοινωνίας και της σύνδεσης από απόσταση, η τεχνολογία προωθεί τις κοινωνικές σχέσεις και μειώνει τα αισθήματα μοναξιάς. Οι άνθρωποι μπορούν να διατηρούν επαφή με τους φίλους, την οικογένεια και τις κοινότητες χάρη στις ψηφιακές πλατφόρμες, τα μέσα κοινωνικής δικτύωσης και τις εφαρμογές ανταλλαγής μηνυμάτων, οι οποίες βελτιώνουν την κοινωνική ευημερία. Πολλές πτυχές της ζωής έχουν γίνει πιο αποτελεσματικές και βολικές χάρη στην ψηφιοποίηση. Μέσω της χρήσης ψηφιακών εργαλείων και υπηρεσιών, εργασίες που κάποτε απαιτούσαν πολύ χρόνο και προσπάθεια μπορούν τώρα να ολοκληρωθούν γρήγορα και αβίαστα. Αυτό μπορεί να βοηθήσει στη γενική ευημερία, καθώς απελευθερώνεται χρόνος και μειώνεται το άγχος. Επιπλέον, οι ψηφιακές ικανότητες γίνονται όλο και πιο κρίσιμες στην αγορά εργασίας καθώς η τεχνολογία αναπτύσσεται. Η απασχολησιμότητα και η κοινωνικοοικονομική ευημερία ενός ατόμου μπορούν να βελτιωθούν με την απόκτηση και τη χρήση αυτών των ταλέντων. Το ψηφιακό χάσμα, το οποίο εμφανίζεται όταν ορισμένα άτομα ή ομάδες δεν έχουν πρόσβαση στην τεχνολογία ή στον ψηφιακό γραμματισμό, μπορεί, ωστόσο, να επιδεινώσει τις ήδη υπάρχουσες ανισότητες.

Ενώ η ακατάλληλη ή υπερβολική χρήση της τεχνολογίας μπορεί να έχει επιβλαβείς επιπτώσεις στην ψυχική υγεία, μπορεί επίσης να έχει και καλές επιπτώσεις. Το άγχος, η απελπισία και η χαμηλή αυτοεκτίμηση μπορεί να επηρεαστούν από τον υπερβολικό χρόνο στην οθόνη, τη σύγκριση με τα μέσα κοινωνικής δικτύωσης και τη διαδικτυακή κατάχρηση. Για να διαφυλάξετε την ψυχική υγεία, είναι ζωτικής σημασίας να διατηρήσετε μια υγιή ισορροπία και να εξασκηθείτε στην προσεκτική χρήση της τεχνολογίας. Επίσης, το ψηφιακό περιβάλλον έχει κάποια ζητήματα ιδιωτικότητας και ασφάλειας. Οι απειλές στον κυβερνοχώρο, οι παραβιάσεις δεδομένων και η διαδικτυακή απάτη μπορούν να θέσουν σε κίνδυνο την οικονομική ασφάλεια και τις προσωπικές πληροφορίες των ανθρώπων. Η διατήρηση της συνολικής ευημερίας στην ψηφιακή εποχή απαιτεί την προστασία της ψηφιακής ασφάλειας και της ιδιωτικής ζωής.

2.3. Τι είναι η ψηφιακή ευημερία;

Η ανάπτυξη της ψηφιακής ανθεκτικότητας και η υιοθέτηση διαδικασιών ασφαλείας οδηγούν σε μια κατάσταση βέλτιστης υγείας και γενικής ευημερίας στην ψηφιακή σφαίρα, η οποία αναφέρεται ως ***ψηφιακή ευημερία***. Η ψηφιακή ευημερία προέρχεται από την έννοια της ευημερίας και έχει να κάνει με την ψηφιακή ζωή των ατόμων. Η ικανότητα των ανθρώπων να προσαρμόζονται, να διαχειρίζονται και να ευημερούν στον ψηφιακό κόσμο, ενώ παράλληλα διαχειρίζονται με επιτυχία τόσο την ευημερία όσο και την ασφάλειά τους, αναφέρεται ως ***ψηφιακή ανθεκτικότητα,*** η οποία είναι ένα μείγμα ψηφιακής ευημερίας και ασφάλειας. Ο ακρογωνιαίος λίθος της ψηφιακής ανθεκτικότητας είναι η ψηφιακή ευημερία, η οποία δίνει έμφαση στη διατήρηση μιας θετικής και λογικής σύνδεσης με την τεχνολογία. Περιλαμβάνει τον περιορισμό του χρόνου χρήσης της οθόνης, την απόδοση μεγάλης προτεραιότητας στην ψυχική και συναισθηματική υγεία, τη δημιουργία υποστηρικτικών διαδικτυακών κοινοτήτων και την εκμάθηση ψηφιακού γραμματισμού. Στο πλαίσιο της ευημερίας, η ψηφιακή ανθεκτικότητα βοηθά τους ανθρώπους να αντιμετωπίσουν διαδικτυακές δυσκολίες όπως ο διαδικτυακός εκφοβισμός, η διαδικτυακή παρενόχληση ή η έκθεση σε επικίνδυνο περιεχόμενο, διατηρώντας παράλληλα τη γενική τους ευημερία. Τα άτομα μπορούν να οικοδομήσουν μια ισχυρή ψηφιακή ανθεκτικότητα που τους επιτρέπει να κινούνται στον ψηφιακό κόσμο με σιγουριά και υπευθυνότητα, ενσωματώνοντας την ψηφιακή ευημερία με την ψηφιακή ασφάλεια. Είναι καλύτερα σε θέση να διαχειρίζονται τις προκλήσεις του ψηφιακού κόσμου, να προσαρμόζονται στους μεταβαλλόμενους κινδύνους, να λαμβάνουν συνετές αποφάσεις, να προστατεύουν τις προσωπικές τους πληροφορίες και να διατηρούν την ψυχική, συναισθηματική και σωματική τους υγεία κατά τη χρήση του διαδικτύου. Η ψηφιακή ανθεκτικότητα ενθαρρύνει τελικά μια ασφαλέστερη, υγιέστερη και πιο ικανοποιητική διαδικτυακή εμπειρία για τους ανθρώπους.

2.3.1. Ψυχική υγεία, ευημερία και ψηφιακή ευημερία

Ολόκληρη η ποιότητα της ζωής μας επηρεάζεται από τις βαθιές συνδέσεις μεταξύ της ψυχικής μας υγείας και της συνολικής μας ευεξίας. Η ψυχολογική και συναισθηματική μας ευημερία, συμπεριλαμβανομένων πτυχών όπως οι σκέψεις, τα συναισθήματα και οι συμπεριφορές μας, αναφέρεται ως η ψυχική μας υγεία. Είναι θεμελιώδης για τη συνολική μας υγεία, εξίσου σημαντική με τη σωματική ευεξία. Αντίθετα, η ευημερία είναι μια συνολική κατάσταση ισορροπίας, πληρότητας και ικανοποίησης στη ζωή. Η σχέση μεταξύ των δύο βασίζεται στο πώς η ψυχική υγεία ενός ατόμου έχει σημαντικό αντίκτυπο στη σωματική του υγεία και το αντίστροφο. Η συνολική ευημερία μας αυξάνεται όταν καλλιεργούμε τη θετική ψυχική υγεία ελέγχοντας το άγχος, ξεπερνώντας τα εμπόδια και δημιουργώντας υγιείς σχέσεις, γεγονός που οδηγεί σε μια πιο ικανοποιητική και ουσιαστική ζωή. Από την άλλη πλευρά, η αίσθηση ευεξίας μπορεί να βελτιώσει σημαντικά την ψυχική υγεία, ενθαρρύνοντας την ανθεκτικότητα, τη συναισθηματική σταθερότητα και την υψηλότερη ικανότητα να αντιμετωπίζουμε τις προκλήσεις της ζωής. Μπορούμε να δημιουργήσουμε μια

ευτυχισμένη και ευημερούσα ζωή δίνοντας έμφαση στη σχέση μεταξύ της ψυχικής μας υγείας και της ευημερίας μας.

Λόγω της ραγδαίας βελτίωσης της τεχνολογίας και της διάχυτης ενσωμάτωσής της στην καθημερινή μας ζωή, η ψυχική υγεία αποκτά έναν πολύπλοκο και δυναμικό χαρακτήρα στην ψηφιακή εποχή. Στο πλαίσιο της ψηφιακής εποχής, η ψυχική και συναισθηματική ευημερία ενός ατόμου αναφέρεται ως "ψηφιακή ψυχική υγεία". Περιλαμβάνει τα μέσα κοινωνικής δικτύωσης, τις διαδικτυακές αλληλεπιδράσεις, τις ψυχολογικές επιδράσεις των ψηφιακών τεχνολογιών και τη συνεχή συνδεσιμότητα που καθορίζει τη σύγχρονη ζωή. Αν και η τεχνολογία έχει δημιουργήσει πολλά πλεονεκτήματα και ευκαιρίες, έχει επίσης δημιουργήσει σημαντικές δυσκολίες για την ψυχική υγεία. Παρά τη συνεχή εικονική επαφή, η ψηφιακή εποχή μπορεί να οδηγήσει σε προβλήματα όπως ο εθισμός στο διαδίκτυο, ο διαδικτυακός εκφοβισμός, η υπερφόρτωση με πληροφορίες, η κοινωνική σύγκριση και το αίσθημα απομόνωσης. Ωστόσο, παρέχει επίσης πρωτοποριακές προσεγγίσεις για τη διαχείριση της ψυχικής υγείας, όπως εφαρμογές ψυχικής υγείας, διαδικτυακή θεραπεία και εικονικές ομάδες υποστήριξης. Η διατήρηση μιας υγιούς ισορροπίας μεταξύ της διαδικτυακής και της μη διαδικτυακής ζωής μας, η επίγνωση του πόσα ψηφιακά μέσα καταναλώνουμε και η ενεργή αναζήτηση ψηφιακών εργαλείων που μπορούν να βελτιώσουν την ψυχική μας ευημερία, προφυλάσσοντας παράλληλα από πιθανές παγίδες, είναι απαραίτητες καθώς διανύουμε τις περιπλοκές της ψηφιακής εποχής.

Σήμερα, υπάρχει μια πολύπλοκη σχέση μεταξύ της ψυχικής υγείας και της ψηφιακής ευημερίας. Η ψυχολογική και συναισθηματική ευημερία των ατόμων, η οποία περιλαμβάνει παράγοντες όπως η διάθεση, οι σκέψεις, τα συναισθήματα και η συμπεριφορά, αναφέρεται ως ψυχική υγεία. Από την άλλη πλευρά, η ψηφιακή ευημερία περιγράφει την ισορροπία και την αρμονία που νιώθει κάποιος όταν χρησιμοποιεί την τεχνολογία και συμμετέχει σε ψηφιακές σχέσεις. Η ψηφιακή εποχή έχει πολλά οφέλη, επιτρέποντας τη συνδεσιμότητα, την πρόσβαση σε πληροφορίες και τις ευκαιρίες για προσωπική ανάπτυξη. Ωστόσο, η υπερβολική χρήση της τεχνολογίας, οι συνεχείς ειδοποιήσεις, η πίεση των μέσων κοινωνικής δικτύωσης και η υπερφόρτωση με πληροφορίες μπορεί να έχουν αρνητικές επιπτώσεις στην ψυχική υγεία, καθώς προκαλούν ένταση, ανησυχία και μια αίσθηση διαχωρισμού από την πραγματικότητα. Από την άλλη πλευρά, μπορεί να έχει ευεργετικό αντίκτυπο στην ψυχική υγεία, όταν η ψηφιακή ευημερία έχει προτεραιότητα, θέτοντας όρια, κάνοντας τακτικά διαλείμματα από τις οθόνες και προσέχοντας την ψηφιακή κατανάλωση. Για την προώθηση τόσο της ψυχικής υγείας όσο και της ψηφιακής ευημερίας και τη διασφάλιση μιας αρμονικής συνύπαρξης μεταξύ της εικονικής και της πραγματικής μας ζωής, είναι σημαντικό να επιτυγχάνεται μια υγιής ισορροπία μεταξύ της ψηφιακής ενασχόλησης και των δραστηριοτήτων εκτός σύνδεσης. Μια πιο ουσιαστική και ισορροπημένη ζωή στην ψηφιακή εποχή μπορεί να επιτευχθεί με τη συνειδητή υιοθέτηση της τεχνολογίας και τη χρήση ψηφιακών εργαλείων για την ενίσχυση της ψυχικής υγείας.

2.3.2. Γιατί χρειαζόμαστε την ψηφιακή ευημερία;

Οι βασικοί παράγοντες της ψηφιακής ευημερίας είναι η ποιότητα ζωής, η επικοινωνία, η παραγωγικότητα και η επιτυχία, η ψυχική και σωματική υγεία. Επειδή περιλαμβάνει ολόκληρη την κατάσταση ενός ατόμου που είναι υγιές, ευτυχισμένο και ικανοποιημένο, η ψηφιακή ευημερία είναι σημαντική. Αναφέρεται στη συνολική υγεία των ανθρώπων και των κοινοτήτων, λαμβάνοντας υπόψη τις κοινωνικές, ψυχολογικές και σωματικές πτυχές τους. Η υπερβολική ή ανθυγιεινή χρήση κινητών τηλεφώνων, μέσων κοινωνικής δικτύωσης και βιντεοπαιχνιδιών μπορεί να είναι επιζήμια για την ψυχική υγεία. Το άγχος, η απελπισία, η μοναξιά και η χαμηλή αυτοεκτίμηση μπορούν να επιδεινωθούν από τον υπερβολικό χρόνο στην οθόνη, τις συχνές συγκρίσεις με άλλους στα μέσα κοινωνικής δικτύωσης ή τον εκφοβισμό στον κυβερνοχώρο. Από αυτή την άποψη, η ψηφιακή ευημερία είναι ο τρόπος για να έχουμε τον έλεγχο της ζωής μας. Είναι ζωτικής σημασίας να έχουμε μια υγιή σχέση με την τεχνολογία, προκειμένου να υποστηρίξουμε την καλή ψυχική υγεία και την ψηφιακή ευημερία. Ο καθορισμός ορίων για τη χρήση των gadget, η συμμετοχή σε ψηφιακές αποτοξινώσεις, η συμμετοχή σε δραστηριότητες εκτός σύνδεσης και η παροχή απόλυτης προτεραιότητας στην αυτοφροντίδα και στις πρόσωπο με πρόσωπο αλληλεπιδράσεις μπορεί να αποτελούν μέρος αυτού. Πρέπει να έχουμε επίγνωση του αντίκτυπου που έχει η ψηφιακή τεχνολογία στην ψυχική μας υγεία και να λαμβάνουμε προληπτικά μέτρα για να διασφαλίσουμε τη λογική χρήση της.

Η ψηφιακή ευημερία έχει καταστεί βασική ανθρώπινη ανάγκη στην ψηφιακή εποχή, ιδίως μετά την πανδημία του Covid-19. Η εξάρτησή μας από τις ψηφιακές πλατφόρμες έχει αυξηθεί, καθώς η τεχνολογία συνεχίζει να εισβάλλει σε κάθε μέρος της καθημερινής μας ζωής, από την επικοινωνία και την εκπαίδευση έως την απασχόληση και την ψυχαγωγία. Η επιδημία έχει προκαλέσει την πρόοδο της ψηφιοποίησης με πρωτοφανή ρυθμό, απαιτώντας εργασία από απόσταση, διαδικτυακή εκπαίδευση και περισσότερες εικονικές σχέσεις. Ως αποτέλεσμα, η διατήρηση της ψηφιακής μας ευημερίας είναι ζωτικής σημασίας για να ζούμε μια ικανοποιητική και υγιή ζωή. Μπορούμε να χρησιμοποιούμε την τεχνολογία με ευσυνειδησία και υπευθυνότητα, ώστε να διασφαλίσουμε ότι βελτιώνει τη ζωή μας και όχι ότι αποτελεί απειλή για τη γενική μας ευημερία σε αυτό το ταχέως μεταβαλλόμενο ψηφιακό περιβάλλον, αναγνωρίζοντας την ψηφιακή ευημερία ως θεμελιώδη ανθρώπινη ανάγκη.

2.3.3. Καλή και κακή ψηφιακή ευημερία

Η ψηφιακή ευημερία είναι ένας περιεκτικός όρος που καλύπτει μια ποικιλία πτυχών του ψηφιακού κόσμου. Ασχολείται τόσο με τη σωματική, ψυχολογική και κοινωνική υγεία των ατόμων όσο και με το να αισθάνονται ψηφιακά ενήμεροι, ισορροπημένοι, ασφαλείς, ικανοποιημένοι και υγιείς από την άλλη πλευρά. Όπως φαίνεται, η έννοια που αποδίδεται στον όρο "ψηφιακή ευημερία" είναι κυρίως προς την ευνοϊκή πλευρά της ψηφιοποίησης, η οποία αναφέρεται στην καλή ψηφιακή ευημερία. Το αντίθετο, τα άτομα που βιώνουν έλλειψη ψηφιακής ευημερίας αναφέρεται σε κακή ψηφιακή ευημερία. Λαμβάνοντας υπόψη

αυτό, οι ακόλουθες πτυχές θα μπορούσαν να υποστηριχθούν ότι συγκαταλέγονται μεταξύ των κύριων δεικτών της καλής ψηφιακής ευημερίας:

- Ψηφιακή ασφάλεια: Η διασφάλιση της ψηφιακής ασφάλειας συμβάλλει σημαντικά στην ψηφιακή ευημερία του ατόμου. Καλύπτει την προστασία της διαδικτυακής σας παρουσίας, συμπεριλαμβανομένης της ταυτότητας, των δεδομένων και των περιουσιακών σας στοιχείων.
- Ψηφιακή ασφάλεια: Έχει να κάνει με την ικανότητα των ατόμων να αναγνωρίζουν κριτικά και να διαχειρίζονται τις διάφορες απειλές στο ψηφιακό περιβάλλον.
- Ψηφιακή ισορροπία: Αναφέρεται στο σκόπιμο όφελος από την τεχνολογία και τον ψηφιακό κόσμο. Η ψηφιακή ισορροπία έχει να κάνει με τη χρήση του ψηφιακού κόσμου, των ψηφιακών εργαλείων και του ψηφιακού εξοπλισμού για τομείς της ζωής και όχι για τα πάντα. Η τακτική και συνεπής ισορροπία μεταξύ online και offline και η αποφυγή της μεγάλης εξάρτησης από την τεχνολογία είναι σημάδια καλής ψηφιακής ισορροπίας.
- Ψηφιακή ανεξαρτησία: Είναι η ικανότητα να ελέγχει κανείς το χρόνο που περνάει στο διαδίκτυο και να αποφεύγει να επικεντρώνει τον ψηφιακό κόσμο στην καθημερινή του ζωή. Το να ξοδεύετε πολύ χρόνο στο διαδίκτυο και να προγραμματίζετε λιγότερες κοινωνικές δραστηριότητες λόγω της υπερβολικής χρήσης του διαδικτύου είναι μερικά σημάδια της ψηφιακής εξάρτησης.
- Ψηφιακή ικανοποίηση: Αναφέρεται στην επίτευξη ικανοποίησης και στο αίσθημα ευχαρίστησης κατά τη χρήση ψηφιακών εργαλείων και εξοπλισμού και την αλληλεπίδραση με την τεχνολογία.
- Ψηφιακή ευκαιρία: Αφορά την αξιοποίηση της τεχνολογίας και της ψηφιοποίησης, ώστε να ανοίξουν νέες δυνατότητες που σχετίζονται με τη διάδοση των ψηφιακών τεχνολογιών και να αποκτηθούν νεότερες ικανότητες για τη δημιουργία νέων ευκαιριών.
- Κριτική και υπεύθυνη χρήση της τεχνολογίας: Παράλληλα με τις ευκαιρίες που προσφέρει, η τεχνολογία απαιτεί από τους χρήστες να ενεργούν υπεύθυνα προστατεύοντας τα δικά τους δικαιώματα και σεβόμενοι τα δικαιώματα των άλλων, να ενεργούν με υπευθυνότητα και προσοχή και να σκέφτονται κριτικά απέναντι σε κάθε περιεχόμενο στον ψηφιακό κόσμο.

Οι πτυχές αυτές θα μπορούσαν επίσης να θεωρηθούν ως διαστάσεις της ψηφιακής ευημερίας. Εάν κάποιος έχει ή εξασφαλίζει σχετικά υψηλότερο επίπεδο ψηφιακής ασφάλειας, προστασίας, ισορροπίας, ανεξαρτησίας, ικανοποίησης, ευκαιρίας ή/και κριτικής και υπεύθυνης χρήσης της τεχνολογίας κατά τη χρήση ψηφιακών εργαλείων και εξοπλισμού, θα μπορούσε να θεωρηθεί ότι έχει καλή ψηφιακή ευημερία. Αντίθετα, αν κάποιος στερείται κάποια από τα παραπάνω στοιχεία, αυτό σημαίνει ότι έχει κακή ψηφιακή ευημερία. Είναι αξιοσημείωτο να θυμόμαστε ότι η σωματική, ψυχολογική και κοινωνική υγεία ενός ατόμου

παραπέμπει επίσης σε καλή ψηφιακή ευημερία και περαιτέρω πτυχές έχουν δυνητική συμβολή στην ψηφιακή ευημερία και τη συνολική ευημερία των ατόμων.

2.3.4. Προώθηση της ψηφιακής ευημερίας των ατόμων: και για την εκπαίδευση ενηλίκων

Η προώθηση της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων ή η ενδυνάμωση της ευημερίας και της ψηφιακής ευημερίας των ενηλίκων παρέχει πολλές ευκαιρίες. Πρώτα απ' όλα, η ευημερία είναι μια βασική ανθρώπινη ανάγκη. Ειδικά μετά την COVID-19, οι περισσότεροι άνθρωποι περνούν πολύ περισσότερο χρόνο στο διαδίκτυο και είναι περισσότερο εκτεθειμένοι στην τεχνολογία μαζί με τους κινδύνους και τις απειλές της. Αν οι άνθρωποι το επιθυμούν σκόπιμα ή όχι, φέρνουν ολόκληρο τον εαυτό τους στην εργασία, δηλαδή υπάρχει σαφής σύνδεση στην ευημερία των ανθρώπων και στην ατμόσφαιρα του εργασιακού περιβάλλοντος. Έτσι, οι πιθανές δράσεις για την προώθηση της ευημερίας και της ψηφιακής ευημερίας των ατόμων συμβάλλουν τόσο σε αυτούς ως ανθρώπινα όντα όσο και στους οργανισμούς για τους οποίους εργάζονται. Από οργανωτική άποψη, η προώθηση της ψηφιακής ευημερίας των εργαζομένων συμβάλλει, αλλά δεν περιορίζεται, στην απόδοση της ομάδας, τη δέσμευση, την καινοτομία και την ικανοποίηση. Η ψηφιακή ευημερία επιτρέπει στα άτομα να γίνονται πιο συγκεντρωμένα, αφοσιωμένα και παραγωγικά, γεγονός που συμβάλλει σε πιο υγιείς ζωές τόσο εντός όσο και εκτός του εργασιακού περιβάλλοντος. Η υιοθέτηση πρακτικών ψηφιακής ευεξίας από τους εργαζόμενους τους επιτρέπει να είναι λιγότερο εξαντλημένοι και αφηρημένοι. Η προώθηση υποστηρικτικών δράσεων για την ψηφιακή ευημερία ενδυναμώνει την ισορροπία μεταξύ εργασίας και προσωπικής ζωής των ατόμων. Επιπλέον, εξαλείφει τις αρνητικές επιπτώσεις της υπερβολικής έκθεσης στην ψηφιοποίηση, γεγονός που επιτρέπει να βιώνουν λιγότερο άγχος, απελπισία, στρες κ.ο.κ.

Η ιδέα της ευημερίας στο πλαίσιο της εκπαίδευσης ενηλίκων υπερβαίνει τις συμβατικές ιδέες των ακαδημαϊκών επιτευγμάτων και περιλαμβάνει τη συνολική υγεία και ολοκλήρωση των σπουδαστών. Η έννοια της "ψηφιακής ευημερίας" έχει αποκτήσει όλο και μεγαλύτερη σημασία με την έλευση της ψηφιακής εποχής, ιδίως για τους ψηφιακούς νομάδες που βασίζονται σε μεγάλο βαθμό στην τεχνολογία ενώ ζουν έναν κινητό τρόπο ζωής. Στην εκπαίδευση ενηλίκων, ο όρος "ψηφιακή ευημερία" αναφέρεται στην παροχή στους σπουδαστές των ικανοτήτων και των πληροφοριών που χρειάζονται για να χρησιμοποιούν το διαδίκτυο λογικά και ηθικά. Η προώθηση της ψηφιακής ευημερίας είναι ζωτικής σημασίας για τη δημιουργία ενός επιτυχημένου μαθησιακού περιβάλλοντος, δεδομένου ότι οι ψηφιακοί νομάδες αντιμετωπίζουν συχνά ιδιαίτερες δυσκολίες, όπως το να συνδυάζουν την προσωπική και την επαγγελματική τους ζωή και να ξεπερνούν τα συναισθήματα μοναξιάς. Η ενσωμάτωση της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων συνεπάγεται τη διδασκαλία των σπουδαστών πώς να ελέγχουν σωστά τον χρόνο τους στην οθόνη, να δημιουργούν θετικές διαδικτυακές κοινότητες και να διατηρούν επίγνωση της ψηφιακής τους χρήσης. Καλύπτει επίσης θέματα όπως η ασφάλεια στον κυβερνοχώρο, η ψηφιακή κόπωση και η ιδιωτικότητα των δεδομένων. Στον σημερινό ψηφιακά καθοδηγούμενο κόσμο, οι εκπαιδευτικοί μπορούν να εξασφαλίσουν μια θετική και εμπλουτισμένη μαθησιακή

εμπειρία αντιμετωπίζοντας την προφανή ανάγκη για ενδυνάμωση της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων και παρέχοντας στους ψηφιακούς νομάδες και άλλους εκπαιδευόμενους τα εργαλεία για να διατηρήσουν μια υγιή ισορροπία μεταξύ των ψηφιακών αλληλεπιδράσεών τους και της συνολικής ευημερίας.

Χρειάζεται μια προσεκτική και εμπεριστατωμένη στρατηγική για την επιτυχή ενσωμάτωση της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων, διότι πρόκειται για μια πολύπλοκη και συνεχή διαδικασία. Το πρώτο και πιο σημαντικό βήμα είναι να δοθεί στους ενήλικες εκπαιδευόμενους εκπαίδευση, ώστε να γνωρίζουν την αξία της ψηφιακής ευημερίας και πώς αυτή επηρεάζει τη γενική υγεία και παραγωγικότητά τους. Αποκτούν τις απαραίτητες πρακτικές δεξιότητες για να περιηγηθούν στον ψηφιακό κόσμο με λογική και ασφάλεια χάρη σε αυτή την εκπαίδευση. Το δεύτερο στάδιο είναι η τροποποίηση του εκπαιδευτικού υλικού έτσι ώστε το πρόγραμμα σπουδών να αντικατοπτρίζει τις έννοιες της ψηφιακής ευημερίας. Αυτό συνεπάγεται την ενσωμάτωση ιδεών όπως ο έλεγχος των ψηφιακών περισπασμών, η διαδικτυακή ιδιωτικότητα, η ψηφιακή εθιμοτυπία και ο ψηφιακός γραμματισμός. Οι ενήλικοι εκπαιδευόμενοι μπορούν να κατανοήσουν καλύτερα τα πλεονεκτήματα και τα μειονεκτήματα της τεχνολογίας και να μάθουν πώς να τη χρησιμοποιούν αποτελεσματικά με την ενσωμάτωση αυτών των χαρακτηριστικών στα μαθήματα. Δημιουργείται ένα υποστηρικτικό περιβάλλον όπου οι εκπαιδευόμενοι μπορούν να μοιράζονται εμπειρίες, να ανταλλάσσουν τεχνικές και να επιβεβαιώνουν τη δέσμευσή τους για ψηφιακή ευημερία με το σχεδιασμό πρόσθετων εκδηλώσεων ενδυνάμωσης, όπως σεμινάρια και συζητήσεις. Για να είναι σχετική και αποτελεσματική η προώθηση της ευημερίας στην ψηφιακή εποχή, η εκπαίδευση ενηλίκων πρέπει να εξελίσσεται συνεχώς, ώστε να συμβαδίζει με το ταχέως μεταβαλλόμενο ψηφιακό τοπίο.

3. Ψηφιακή ασφάλεια

3.1 Ψηφιακή ασφάλεια και κυβερνοασφάλεια

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), η **ψηφιακή ασφάλεια** είναι απαραίτητη για την εμπιστοσύνη στην ψηφιακή εποχή. Ο ΟΟΣΑ διευκολύνει τη διεθνή συνεργασία και αναπτύσσει αναλύσεις πολιτικής και συστάσεις στον τομέα της ψηφιακής ασφάλειας από τις αρχές της δεκαετίας του 1990. Οι εργασίες στον τομέα αυτό αποσκοπούν στην ανάπτυξη και προώθηση πολιτικών που ενισχύουν την εμπιστοσύνη χωρίς να αναστέλλουν το δυναμικό των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) για την υποστήριξη της καινοτομίας, της ανταγωνιστικότητας και της ανάπτυξης. Η ψηφιακή ασφάλεια αναφέρεται στις οικονομικές και κοινωνικές πτυχές της ασφάλειας στον κυβερνοχώρο, σε αντίθεση με τις αμιγώς τεχνικές πτυχές και εκείνες που σχετίζονται με την επιβολή του ποινικού δικαίου ή την εθνική και διεθνή ασφάλεια. Ο όρος "ψηφιακή" συνάδει με εκφράσεις όπως ψηφιακή οικονομία, ψηφιακός μετασχηματισμός και ψηφιακές τεχνολογίες. Αποτελεί τη βάση για εποικοδομητικό διεθνή διάλογο μεταξύ των

ενδιαφερομένων μερών που επιδιώκουν να ενισχύσουν την εμπιστοσύνη και να μεγιστοποιήσουν τις ευκαιρίες από τις ΤΠΕ[1] .

Η ψηφιακή ασφάλεια και η **ασφάλεια στον κυβερνοχώρο** σχετίζονται αλλά δεν είναι το ίδιο. Και οι δύο αφορούν την προστασία των ψηφιακών περιουσιακών στοιχείων και πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση ή ζημία, αλλά διαφέρουν ως προς το πεδίο εφαρμογής και την εστίαση.

Η ψηφιακή ασφάλεια αναφέρεται στην πρακτική της προστασίας των ψηφιακών δεδομένων, πληροφοριών και περιουσιακών στοιχείων από μη εξουσιοδοτημένη πρόσβαση, κλοπή ή ζημία. Περιλαμβάνει ένα ευρύτερο φάσμα μέτρων ασφαλείας που προστατεύουν δεδομένα και πληροφορίες σε διάφορες ψηφιακές πλατφόρμες και συσκευές, συμπεριλαμβανομένων υπολογιστών, smartphones, tablet και άλλων ψηφιακών τεχνολογιών.

Τα μέτρα ψηφιακής ασφάλειας μπορεί να περιλαμβάνουν:

- Προστασία με κωδικό πρόσβασης: Δημιουργία ισχυρών και μοναδικών κωδικών πρόσβασης για διαδικτυακούς λογαριασμούς και συσκευές.
- Κρυπτογράφηση δεδομένων: Κωδικοποίηση δεδομένων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή παραβίασης δεδομένων.
- Ασφαλείς επικοινωνίες: Χρήση πρωτοκόλλων κρυπτογράφησης για ασφαλή μετάδοση δεδομένων.
- Έλεγχοι πρόσβασης: Εφαρμογή δικαιωμάτων και περιορισμών για τον περιορισμό της πρόσβασης σε ευαίσθητα δεδομένα.
- Ασφάλεια συσκευής: Χρήση χαρακτηριστικών όπως κλειδώματα οθόνης και απομακρυσμένη διαγραφή για χαμένες ή κλεμμένες συσκευές.

Η κυβερνοασφάλεια αποτελεί υποσύνολο της ψηφιακής ασφάλειας και επικεντρώνεται ειδικά στην προστασία των ψηφιακών περιουσιακών στοιχείων από απειλές και επιθέσεις στον κυβερνοχώρο. Περιλαμβάνει την άμυνα κατά της μη εξουσιοδοτημένης πρόσβασης, ζημίας ή διατάραξης των ψηφιακών συστημάτων, δικτύων και υποδομών.

Τα μέτρα κυβερνοασφάλειας μπορεί να περιλαμβάνουν:

- Προστασία τείχους προστασίας: Τείχος προστασίας: Δημιουργία φραγμών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο.
- Συστήματα ανίχνευσης εισβολών: Παρακολούθηση δικτύων για ύποπτες δραστηριότητες και πιθανές απειλές.

[1] https://www.oecd.org/digital/digital-security/

- Προστασία από κακόβουλο λογισμικό: Χρήση λογισμικού προστασίας από ιούς για τον εντοπισμό και την αφαίρεση κακόβουλου λογισμικού.
- Σχεδιασμός αντιμετώπισης περιστατικών: Ανάπτυξη πρωτοκόλλων για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοασφάλειας.
- Πληροφορία για απειλές στον κυβερνοχώρο: Συγκέντρωση και ανάλυση πληροφοριών για την πρόβλεψη και πρόληψη απειλών στον κυβερνοχώρο.

Η ψηφιακή ασφάλεια καλύπτει ένα ευρύτερο φάσμα πρακτικών που προστατεύουν τα δεδομένα και τις πληροφορίες στο ψηφιακό πεδίο, ενώ η κυβερνοασφάλεια είναι ένας εξειδικευμένος τομέας που επικεντρώνεται στην άμυνα έναντι κυβερνοαπειλών και επιθέσεων σε ψηφιακά συστήματα και δίκτυα. Και οι δύο αποτελούν κρίσιμα στοιχεία για τη διασφάλιση της συνολικής ασφάλειας και προστασίας των ψηφιακών περιουσιακών στοιχείων και πληροφοριών.

3.2. Απειλές κυβερνοασφάλειας που αντιμετωπίζουν οι ενήλικες

Οι ενήλικες αντιμετωπίζουν ένα ευρύ φάσμα απειλών για την κυβερνοασφάλεια στον σημερινό ψηφιακό κόσμο. Ακολουθούν ορισμένες κοινές απειλές κυβερνοασφάλειας που αντιμετωπίζουν συχνά οι ενήλικες:

- ***Επιθέσεις phishing:*** Είναι μια τεχνική που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να εξαπατήσουν τα άτομα ώστε να δώσουν ευαίσθητες πληροφορίες, όπως στοιχεία σύνδεσης, αριθμούς πιστωτικών καρτών ή προσωπικά δεδομένα. Τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα ή οι ιστότοποι phishing μπορεί να φαίνονται ότι προέρχονται από αξιόπιστες πηγές, αλλά έχουν ως στόχο να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν τις πληροφορίες τους.
- ***Κακόβουλο λογισμικό:*** Το κακόβουλο λογισμικό είναι κακόβουλο λογισμικό που έχει σχεδιαστεί για να διεισδύσει, να βλάψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα υπολογιστών. Τα είδη κακόβουλου λογισμικού περιλαμβάνουν ιούς, ransomware, spyware και Trojans. Το κακόβουλο λογισμικό μπορεί να εξαπλωθεί μέσω κακόβουλων συνημμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, μολυσμένων ιστότοπων ή παραβιασμένου λογισμικού.
- ***Κλοπή ταυτότητας:*** Οι εγκληματίες του κυβερνοχώρου μπορούν να κλέψουν προσωπικές πληροφορίες, όπως αριθμούς κοινωνικής ασφάλισης, ημερομηνίες γέννησης ή οικονομικά δεδομένα, για να διαπράξουν κλοπή ταυτότητας. Οι πληροφορίες αυτές αποκτώνται συχνά μέσω παραβιάσεων δεδομένων ή προσπαθειών ηλεκτρονικού "ψαρέματος" (phishing).
- ***Ηλεκτρονικές απάτες:*** Υπάρχουν πολυάριθμες διαδικτυακές απάτες που στοχεύουν σε ενήλικες, όπως απάτες με λαχεία, απάτες ρομαντικών σχέσεων, ψεύτικες απάτες τεχνικής υποστήριξης και απατηλά επενδυτικά σχέδια. Οι

απατεώνες χρησιμοποιούν διάφορες τακτικές για να χειραγωγήσουν τα άτομα ώστε να στείλουν χρήματα ή να παράσχουν προσωπικές πληροφορίες.

- ***Παραβιάσεις δεδομένων:*** Οι παραβιάσεις δεδομένων συμβαίνουν όταν ευαίσθητες πληροφορίες που κατέχουν εταιρείες ή οργανισμοί εκτίθενται ή κλέβονται. Ως ενήλικας, μπορεί να επηρεαστείτε από παραβιάσεις δεδομένων, εάν οι προσωπικές σας πληροφορίες αποθηκεύονται από τις επηρεαζόμενες οντότητες.
- ***Κοινωνική μηχανική:*** Η κοινωνική μηχανική περιλαμβάνει τη χειραγώγηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ορισμένες ενέργειες. Οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν τεχνικές κοινωνικής μηχανικής για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή λογαριασμούς.
- ***Επιθέσεις με κωδικούς πρόσβασης:*** Οι αδύναμοι κωδικοί πρόσβασης ή η επαναχρησιμοποίηση κωδικών πρόσβασης μπορεί να οδηγήσουν σε επιθέσεις με κωδικούς πρόσβασης, όπως επιθέσεις ωμής βίας ή επιθέσεις λεξικού, όπου οι εγκληματίες του κυβερνοχώρου προσπαθούν να μαντέψουν ή να σπάσουν κωδικούς πρόσβασης για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση.
- ***Κίνδυνοι δημόσιου Wi-Fi:*** Η χρήση δημόσιων δικτύων Wi-Fi μπορεί να εκθέσει τους ενήλικες σε κινδύνους ασφαλείας, καθώς αυτά τα δίκτυα μπορεί να μην διαθέτουν την κατάλληλη κρυπτογράφηση και να είναι ευάλωτα σε υποκλοπές από επιτιθέμενους.
- ***Απειλές εκ των έσω:*** Οι εσωτερικές απειλές αφορούν υπαλλήλους ή άτομα με εξουσιοδοτημένη πρόσβαση σε συστήματα ή δεδομένα που προκαλούν σκόπιμα ή ακούσια ζημιά ή διαρρέουν ευαίσθητες πληροφορίες.
- ***Ευπάθειες IoT:*** Η αυξανόμενη υιοθέτηση συσκευών του Διαδικτύου των Πραγμάτων (IoT) μπορεί να δημιουργήσει κινδύνους για την ασφάλεια στον κυβερνοχώρο, καθώς πολλές από αυτές τις συσκευές μπορεί να έχουν ανεπαρκή μέτρα ασφαλείας και μπορούν να αξιοποιηθούν από εγκληματίες του κυβερνοχώρου.

Για την προστασία από αυτές τις απειλές, οι ενήλικες θα πρέπει να εφαρμόζουν καλή υγιεινή στον κυβερνοχώρο, όπως η χρήση ισχυρών και μοναδικών κωδικών πρόσβασης, η ενεργοποίηση του ελέγχου ταυτότητας πολλαπλών παραγόντων, η ενημέρωση του λογισμικού και των συσκευών, η προσοχή σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και συνδέσμους και η προσοχή στις πληροφορίες που μοιράζονται στο διαδίκτυο. Η τακτική εκπαίδευση ευαισθητοποίησης σε θέματα κυβερνοασφάλειας μπορεί επίσης να βοηθήσει τα άτομα να ενημερώνονται για τις αναδυόμενες απειλές και τις βέλτιστες πρακτικές για να παραμένουν ασφαλείς στο διαδίκτυο. Στην επόμενη ενότητα παρουσιάζονται λεπτομερώς ορισμένες από τις πιο βασικές πρακτικές ψηφιακής ασφάλειας για τους ενήλικες, ώστε να

μειώσουν τον κίνδυνο να πέσουν θύματα απειλών κυβερνοασφάλειας και να προστατεύσουν την ψηφιακή τους ταυτότητα και τα περιουσιακά τους στοιχεία.

3.3. Πρακτικές ψηφιακής ασφάλειας για ενήλικες

Οι πρακτικές ψηφιακής ασφάλειας είναι απαραίτητες για τους ενήλικες ώστε να προστατεύουν τις προσωπικές τους πληροφορίες, τα δεδομένα και τους διαδικτυακούς τους λογαριασμούς από απειλές κυβερνοασφάλειας. Ακολουθούν ορισμένες σημαντικές πρακτικές ψηφιακής ασφάλειας που πρέπει να ακολουθούν οι ενήλικες:

- ***Χρησιμοποιήστε ισχυρούς και μοναδικούς κωδικούς πρόσβασης:*** Οι ενήλικες πρέπει να δημιουργούν ισχυρούς και μοναδικούς κωδικούς πρόσβασης για τους διαδικτυακούς λογαριασμούς τους. Αποφεύγετε να χρησιμοποιείτε εύκολα μαντεύσιμους κωδικούς πρόσβασης όπως "123456" ή "password". Εξετάστε το ενδεχόμενο χρήσης ενός διαχειριστή κωδικών πρόσβασης για τη δημιουργία και την ασφαλή αποθήκευση σύνθετων κωδικών πρόσβασης.
- ***Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA):*** Όποτε είναι δυνατόν, ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων στους διαδικτυακούς σας λογαριασμούς. Ο MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας μια δεύτερη μορφή επαλήθευσης, όπως έναν κωδικό μιας χρήσης που αποστέλλεται στην κινητή συσκευή σας, εκτός από τον κωδικό πρόσβασής σας.
- ***Διατηρήστε το λογισμικό και τις συσκευές ενημερωμένες:*** Ενημερώστε τακτικά το λειτουργικό σας σύστημα, τα προγράμματα περιήγησης στο διαδίκτυο και τις εφαρμογές λογισμικού. Οι ενημερώσεις συχνά περιλαμβάνουν διορθώσεις ασφαλείας που αντιμετωπίζουν γνωστές ευπάθειες.
- ***Να είστε προσεκτικοί με τα μηνύματα ηλεκτρονικού ταχυδρομείου και τους συνδέσμους:*** Να είστε προσεκτικοί όταν ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή όταν κάνετε κλικ σε ύποπτους συνδέσμους. Να είστε ιδιαίτερα προσεκτικοί με μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν ευαίσθητες πληροφορίες ή σας κατευθύνουν να συνδεθείτε σε έναν ψεύτικο ιστότοπο.
- ***Ασφαλίστε το οικιακό σας δίκτυο:*** Αλλάξτε τον προεπιλεγμένο κωδικό πρόσβασης στον οικιακό σας δρομολογητή Wi-Fi και ενεργοποιήστε την κρυπτογράφηση WPA2 ή WPA3 για να προστατεύσετε το ασύρματο δίκτυό σας. Αποφύγετε τη χρήση δημόσιων δικτύων Wi-Fi για ευαίσθητες δραστηριότητες, εκτός αν χρησιμοποιείτε εικονικό ιδιωτικό δίκτυο (VPN).
- ***Δημιουργήστε τακτικά αντίγραφα ασφαλείας δεδομένων:*** Δημιουργείτε τακτικά αντίγραφα ασφαλείας των σημαντικών αρχείων και δεδομένων σας σε έναν εξωτερικό σκληρό δίσκο, σε αποθηκευτικό χώρο στο σύννεφο ή σε μια ασφαλή υπηρεσία δημιουργίας αντιγράφων ασφαλείας. Σε περίπτωση απώλειας

δεδομένων ή επιθέσεων ransomware, η δημιουργία αντιγράφων ασφαλείας διασφαλίζει ότι μπορείτε να ανακτήσετε τα αρχεία σας.

- ***Χρήση ασφαλούς Wi-Fi και HTTPS:*** Όταν έχετε πρόσβαση σε ευαίσθητους ιστότοπους, βεβαιωθείτε ότι χρησιμοποιούν κρυπτογράφηση HTTPS. Αναζητήστε το σύμβολο του λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης για να επαληθεύσετε την ασφάλεια του ιστότοπου.
- ***Προσέξτε τα μέσα κοινωνικής δικτύωσης:*** Να είστε προσεκτικοί σχετικά με τις πληροφορίες που μοιράζεστε στις πλατφόρμες κοινωνικής δικτύωσης. Αποφύγετε τη δημοσίευση προσωπικών στοιχείων όπως η διεύθυνση, ο αριθμός τηλεφώνου ή τα ταξιδιωτικά σας σχέδια, καθώς οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για επιθέσεις κοινωνικής μηχανικής.
- ***Εγκαταστήστε λογισμικό προστασίας από ιούς και λογισμικό ασφαλείας:*** Χρησιμοποιήστε αξιόπιστο λογισμικό προστασίας από ιούς και λογισμικό ασφαλείας στις συσκευές σας για προστασία από κακόβουλο λογισμικό και άλλες απειλές. Διατηρείτε το λογισμικό ενημερωμένο για να εξασφαλίσετε τη βέλτιστη προστασία.
- ***Ενημερωθείτε για την ασφάλεια στον κυβερνοχώρο:*** Παραμείνετε ενημερωμένοι για τις τελευταίες απειλές και τις βέλτιστες πρακτικές στον κυβερνοχώρο, διαβάζοντας αξιόπιστες πηγές, παρακολουθώντας διαδικτυακά σεμινάρια ή συμμετέχοντας σε προγράμματα ευαισθητοποίησης στον κυβερνοχώρο (βλ. τους διαθέσιμους πόρους ψηφιακής ασφάλειας για ενήλικες).

Ενσωματώνοντας αυτές τις πρακτικές ψηφιακής ασφάλειας στις καθημερινές τους συνήθειες, οι ενήλικες μπορούν να μειώσουν σημαντικά τον κίνδυνο να πέσουν θύματα απειλών κυβερνοασφάλειας και να προστατεύσουν την ψηφιακή τους ταυτότητα και τα περιουσιακά τους στοιχεία.

3.4. Διαθέσιμοι πόροι ψηφιακής ασφάλειας για ενήλικες

Το Κέντρο Εκπαίδευσης για την Κυβερνοασφάλεια[2] (CEH) στο California State University San Marcos προσφέρει πόρους και κατευθύνσεις για τις προσπάθειες της πανεπιστημιούπολης και της κοινότητας για την αύξηση της εκπαίδευσης και της ευαισθητοποίησης σε θέματα ψηφιακής ασφάλειας. Το CEH είναι μια συλλογική προσπάθεια του Γραφείου Ασφάλειας Πληροφοριών της πανεπιστημιούπολης, των Κολλεγίων Επιστημών και Μαθηματικών και Διοίκησης Επιχειρήσεων.

Το CEH εργάζεται για να διασφαλίσει ότι τα εκπαιδευτικά προγράμματα ψηφιακής ασφάλειας της πανεπιστημιούπολης αντιμετωπίζουν ευρύτερα θέματα που σχετίζονται με τα τρέχοντα γεγονότα στον τομέα της ψηφιακής ασφάλειας και παρέχει ευκαιρίες για την

[2] https://www.csusm.edu/cybersec-hub/index.html

ενσωμάτωση θεμάτων ψηφιακής ασφάλειας σε μαθήματα που διδάσκονται σε όλο το πανεπιστήμιο. Το CEH προσφέρει επίσης πόρους σε φοιτητές, φοιτητικές οργανώσεις και στο ευρύ κοινό. Προωθεί και διευκολύνει την επικοινωνία και τη συνεργασία με την εκπαίδευση στην ψηφιακή ασφάλεια σε ολόκληρη την κοινότητα. Παρέχουν εκπαιδευτικό υλικό για θέματα όπως η ιδιωτικότητα και τα μέσα κοινωνικής δικτύωσης, η ασφάλεια στον κυβερνοχώρο για τους φοιτητές, η κυβερνοασφάλεια σήμερα και οι έννοιες της κυβερνοασφάλειας.

Εκτός αυτού, το 2008, εισήχθη το εκπαιδευτικό υλικό του ENISA[3] για την ασφάλεια στον κυβερνοχώρο. Έκτοτε έχει επεκταθεί με νέες ενότητες που περιέχουν κρίσιμες πληροφορίες για την επιτυχία στον τομέα της ασφάλειας στον κυβερνοχώρο. Ο ENISA περιέχει εκπαιδευτικό υλικό, όπως εγχειρίδια για καθηγητές, εργαλειοθήκες για μαθητές και εικονικές εικόνες για τη συμπλήρωση των πρακτικών εκπαιδευτικών συναντήσεων.

4. Βέλτιστες πρακτικές για την οικοδόμηση ψηφιακής ασφάλειας για ενήλικες

Η ψηφιακή ασφάλεια αποκτά ολοένα και μεγαλύτερη σημασία στη διασυνδεδεμένη κοινωνία μας και οι ηλικιωμένοι είναι μία από τις πιο ευάλωτες ομάδες στο διαδίκτυο. Καθώς εξελίσσεται η τεχνολογία, εξελίσσονται και οι απειλές στον κυβερνοχώρο. Επομένως, είναι σημαντικό να θεσπιστούν μέτρα και κατευθυντήριες γραμμές για την προστασία των ηλικιωμένων στο ψηφιακό περιβάλλον. Παρακάτω παρατίθενται ορισμένες καλές πρακτικές και επιτυχημένες δράσεις που εφαρμόστηκαν σε διάφορες χώρες και μπορούν να χρησιμεύσουν ως σημείο αναφοράς για άλλους.

Η στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο εκπροσωπείται στις εκθέσεις που είναι όλες διαθέσιμες στον επίσημο ιστότοπο της Ευρωπαϊκής Επιτροπής και παρέχουν πολύτιμες πληροφορίες για τις βέλτιστες πρακτικές για τη βελτίωση της ψηφιακής ασφάλειας στην Ευρώπη.

4.1. Βασικά ζητήματα για την οικοδόμηση της ψηφιακής ασφάλειας

Το τμήμα αυτό μπορεί να φαίνεται ότι αποτελεί επανάληψη του τμήματος 3.3. Πρακτικές ψηφιακής ασφάλειας για ενήλικες, αλλά περιέχει περισσότερα σενάρια και παραδείγματα από τον πραγματικό κόσμο.

Ισχυροί κωδικοί πρόσβασης: Βοηθήστε τους να δημιουργήσουν ισχυρούς και μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό. Οι κωδικοί πρόσβασης πρέπει να είναι μακροσκελείς και να περιέχουν κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες. Οι κωδικοί πρόσβασης πρέπει να είναι μακροσκελείς (τουλάχιστον 8

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

χαρακτήρες), να περιέχουν κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες. Αποφύγετε τη χρήση προβλέψιμων προσωπικών πληροφοριών, όπως ονόματα ή ημερομηνίες γέννησης. Υπενθυμίστε τους να μην μοιράζονται τους κωδικούς πρόσβασής τους με κανέναν και να τους αλλάζουν τακτικά.

Για παράδειγμα, ένας ισχυρός κωδικός πρόσβασης θα μπορούσε να είναι "P@ssw0rd2023!", ο οποίος συνδυάζει κεφαλαία γράμματα, πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες. Αποφύγετε τη χρήση προβλέψιμων προσωπικών πληροφοριών όπως ονόματα ή ημερομηνίες γέννησης, όπως "John1980" ή "MarySmith123".

Εκπαίδευση και ευαισθητοποίηση: *Ενημέρωση* για τους διαδικτυακούς κινδύνους και απειλές, όπως το phishing, το κακόβουλο λογισμικό και η κλοπή ταυτότητας. Βοηθήστε τους να κατανοήσουν πώς να αναγνωρίζουν και να αποφεύγουν αυτές τις καταστάσεις. Είναι σημαντικό να τους ενημερώσετε για τους διαδικτυακούς κινδύνους, όπως το phishing (απόπειρα απόκτησης εμπιστευτικών πληροφοριών με δόλιο τρόπο), το κακόβουλο λογισμικό (malware) και η κλοπή ταυτότητας. Μάθετε να αναγνωρίζετε αυτά τα προειδοποιητικά σημάδια και αποφύγετε να πέσετε σε αυτές τις παγίδες. Εξηγήστε τις πιθανές αρνητικές επιπτώσεις και τον τρόπο προστασίας.

Για παράδειγμα, εξηγήστε ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing μπορεί να εμφανίζονται ως νόμιμα, ζητώντας τους να κάνουν κλικ σε συνδέσμους και να εισάγουν ευαίσθητες πληροφορίες. Δείξτε τους παραδείγματα ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου και πώς να τα αναγνωρίζουν. Παρέχετε πληροφορίες σχετικά με κοινούς τύπους κακόβουλου λογισμικού, όπως ψεύτικο λογισμικό προστασίας από ιούς ή αναδυόμενα παράθυρα, και πώς να τα αποφεύγουν.

Αυθεντικοποίηση δύο παραγόντων (2FA): Βοηθήστε τους να εφαρμόσουν έλεγχο ταυτότητας δύο παραγόντων, όποτε είναι δυνατόν. Αυτό προσθέτει ένα επιπλέον επίπεδο ασφάλειας στους λογαριασμούς σας. Ο έλεγχος ταυτότητας δύο παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Βοηθήστε τους να ενεργοποιήσουν αυτή τη λειτουργία στους λογαριασμούς τους, αν είναι δυνατόν. Ο 2FA απαιτεί μια άλλη μέθοδο ελέγχου ταυτότητας εκτός από έναν τυπικό κωδικό πρόσβασης, όπως έναν κωδικό μηνύματος κειμένου, έναν επαληθευτή ή ένα δακτυλικό αποτύπωμα.

Για παράδειγμα, αφού πληκτρολογήσουν τον κωδικό πρόσβασής τους, θα λάβουν ένα γραπτό μήνυμα με έναν κωδικό επαλήθευσης που πρέπει να εισάγουν για να αποκτήσουν πρόσβαση στο λογαριασμό τους. Αυτό προσθέτει ένα επιπλέον επίπεδο ασφάλειας και δυσκολεύει την πρόσβαση μη εξουσιοδοτημένων χρηστών στους λογαριασμούς τους.

Ασφαλής χρήση κινητών συσκευών: *Βοηθήστε* τους να ρυθμίσουν κλειδαριές οθόνης, αναγνώριση προσώπου ή δακτυλικά αποτυπώματα για την προστασία των κινητών τους

συσκευών. Υπενθυμίστε τους να μην μοιράζονται τις συσκευές τους με άτομα που δεν γνωρίζουν και να είναι προσεκτικοί όταν κατεβάζουν εφαρμογές από αναξιόπιστες πηγές.

Για παράδειγμα, δείξτε τους πώς να ενεργοποιήσουν ένα PIN ή να χρησιμοποιήσουν το δακτυλικό τους αποτύπωμα για να ξεκλειδώσουν το smartphone τους. Υπενθυμίστε τους να μην μοιράζονται τις συσκευές τους με άτομα που δεν γνωρίζουν και να είναι προσεκτικοί όταν κατεβάζουν εφαρμογές από αναξιόπιστες πηγές.

Ενημερώσεις λογισμικού: Βεβαιωθείτε ότι οι συσκευές σας (υπολογιστές, tablet, smartphones) έχουν εγκαταστήσει τις τελευταίες διορθώσεις και ενημερώσεις ασφαλείας. Οι ενημερώσεις συχνά περιλαμβάνουν διορθώσεις για γνωστές ευπάθειες, οπότε η ενημέρωση των συσκευών σας συμβάλλει στην προστασία τους.

Ηλεκτρονικά ψώνια: Υπενθυμίστε τους να κάνουν αγορές μόνο σε αξιόπιστες και ασφαλείς ιστοσελίδες και να χρησιμοποιούν ασφαλείς μεθόδους πληρωμής. Διδάξτε τους να αναζητούν μια κλειδαριά στη γραμμή διευθύνσεων και να χρησιμοποιούν ασφαλείς μεθόδους πληρωμής, όπως πιστωτικές κάρτες με επιπλέον μέτρα ασφαλείας.

Ασφαλής χρήση του ηλεκτρονικού ταχυδρομείου: Προειδοποιήστε τους για το phishing και συμβουλέψτε τους να αποφεύγουν να κάνουν κλικ σε συνδέσμους ή να κατεβάζουν συνημμένα αρχεία από άγνωστους αποστολείς. Προειδοποιήστε τα για το ηλεκτρονικό ψάρεμα, όπου οι απατεώνες προσπαθούν να αποκτήσουν ευαίσθητες πληροφορίες παριστάνοντας τους νόμιμους αποστολείς. Αυτό υπογραμμίζει τη σημασία του να μην κάνουν κλικ σε συνδέσμους ή να μην κατεβάζουν συνημμένα αρχεία από ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή άγνωστους αποστολείς. Σας προτρέπει να επαληθεύετε τη νομιμότητα των μηνυμάτων ηλεκτρονικού ταχυδρομείου με τον αποστολέα πριν στείλετε εμπιστευτικές πληροφορίες.

Social Media: Βοηθήστε τους να προσαρμόσουν τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης για να ελέγχουν ποιος βλέπει τις αναρτήσεις τους και να αποφεύγουν να μοιράζονται ευαίσθητες προσωπικές πληροφορίες. Διδάξτε τους να αποφεύγουν να μοιράζονται ευαίσθητες πληροφορίες, όπως αριθμούς τηλεφώνου, διευθύνσεις ή οικονομικές πληροφορίες δημοσίως στα μέσα κοινωνικής δικτύωσης.

Για παράδειγμα, καθοδηγήστε τους μέσω των ρυθμίσεων απορρήτου στο Facebook για να περιορίσετε το ποιος μπορεί να βλέπει τις αναρτήσεις τους μόνο σε φίλους. Τονίστε τη σημασία της προσοχής στην κοινοποίηση πληροφοριών όπως αριθμοί τηλεφώνου, διευθύνσεις ή οικονομικά στοιχεία σε πλατφόρμες κοινωνικής δικτύωσης.

Ασφαλής περιήγηση: Μάθετε να αναγνωρίζετε αυτές τις ασφαλείς ιστοσελίδες ("https" και "lock") και αποφύγετε να κάνετε κλικ σε ύποπτους συνδέσμους ή να κατεβάζετε άγνωστα αρχεία. Διδάξτε τους να διακρίνουν τους ασφαλείς ιστότοπους ελέγχοντας τη γραμμή διευθύνσεών τους για την ύπαρξη κλειδαριάς και αν έχουν ξεκινήσει. "http" αντί για "https". Εξηγήστε τη σημασία του να αποφεύγετε να κάνετε κλικ σε ύποπτους συνδέσμους ή να κατεβάζετε αρχεία από άγνωστες πηγές, καθώς μπορεί να περιέχουν κακόβουλο λογισμικό ή να σας ανακατευθύνουν σε δόλιους ιστότοπους.

Ασφάλεια Wi-Fi: Βεβαιωθείτε ότι χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης στο οικιακό τους δίκτυο Wi-Fi και αποφεύγουν τη σύνδεση σε δημόσια ή άγνωστα δίκτυα Wi-Fi. Εξηγήστε τη σημασία της χρήσης ισχυρών κωδικών πρόσβασης στο οικιακό δίκτυο Wi-Fi και της αποφυγής σύνδεσης σε δημόσια ή άγνωστα δίκτυα Wi-Fi. Τα μη ασφαλή δίκτυα Wi-Fi μπορούν δυνητικά να δεχθούν επίθεση ή να υποκλαπούν για κατασκοπεία δεδομένων.

Ανενεργοί λογαριασμοί: Βοηθήστε τους να κλείσουν ή να διαγράψουν τους διαδικτυακούς λογαριασμούς που δεν χρησιμοποιούν πλέον για να μειωθεί ο κίνδυνος ασφάλειας. Οι ανενεργοί λογαριασμοί μπορεί να είναι ευάλωτοι σε επιθέσεις, ειδικά αν περιέχουν προσωπικές πληροφορίες.

Προσοχή σε ύποπτες κλήσεις και μηνύματα: Διδάξτε τους να μην αποκαλύπτουν προσωπικές ή οικονομικές πληροφορίες σε απροσδόκητες κλήσεις ή μηνύματα. Διδάξτε τους να είναι προσεκτικοί όταν αποκαλύπτουν προσωπικές ή οικονομικές πληροφορίες σε απροσδόκητες κλήσεις ή γραπτά μηνύματα. Ενθαρρύνετε τον αποστολέα να επαληθεύει την ταυτότητά του πριν μοιραστεί ευαίσθητες πληροφορίες. Για παράδειγμα, δώστε παραδείγματα κοινών απάτης, όπως ψεύτικες κλήσεις τεχνικής υποστήριξης ή ειδοποιήσεις για κέρδη από λαχεία.

Εποπτεία και υποστήριξη: Προσφερθείτε να βοηθήσετε με τακτικούς ελέγχους των διαδικτυακών σας λογαριασμών και βοηθήστε τους αν υποπτεύονται ύποπτες δραστηριότητες ή έχουν προβλήματα ασφαλείας. Ενημερωθείτε για τις τελευταίες διαδικτυακές απειλές και παρέχετε συνεχή καθοδήγηση και υποστήριξη. Για παράδειγμα, δείξτε τους πώς να επανεξετάζουν την πρόσφατη δραστηριότητα του λογαριασμού τους και τις συνδέσεις τους σε διάφορες πλατφόρμες.

Προσωπικές πληροφορίες: Διδάξτε τους να είναι προσεκτικοί όταν μοιράζονται προσωπικές πληροφορίες στο διαδίκτυο και να περιορίζουν τον όγκο των πληροφοριών που δημοσιεύουν. Περιορίστε την ποσότητα των πληροφοριών που δημοσιεύουν, όπως

διευθύνσεις, αριθμούς τηλεφώνου ή σχολικές πληροφορίες. Προωθείται η ιδιωτικότητα και η σημασία της προστασίας της διαδικτυακής σας ταυτότητας.

Δημιουργία αντιγράφων ασφαλείας σημαντικών δεδομένων: Δημιουργείτε τακτικά αντίγραφα ασφαλείας σημαντικών δεδομένων για να αποφύγετε την απώλεια σε περίπτωση παραβίασης της ασφάλειας ή βλάβης της συσκευής.

4.2. Βέλτιστες πρακτικές ανά τον κόσμο

4.2.1. Cyber Europe

Ο ENISA διοργανώνει το Cyber Europe[4] από το 2010, μια σειρά ασκήσεων διαχείρισης περιστατικών και κρίσεων στον κυβερνοχώρο, με συναρπαστικά σενάρια εμπνευσμένα από πραγματικά γεγονότα και ανεπτυγμένα από Ευρωπαίους εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας. Κάθε δύο χρόνια, δημόσιος και ιδιωτικός τομέας από χώρες της ΕΕ και του ΕΟΧ, καθώς και ευρωπαϊκά θεσμικά όργανα, φορείς και οργανισμοί, συνεργάζονται για να ενισχύσουν τις υφιστάμενες τεχνικές και επιχειρησιακές τους ικανότητες.

Η άσκηση Cyber Europe πραγματοποιείται επί δύο ημέρες και προσομοιώνει περιστατικά μεγάλης κλίμακας στον κυβερνοχώρο που κλιμακώνονται σε κυβερνοκρίσεις που επηρεάζουν ολόκληρη την ΕΕ. Οι συμμετέχοντες στην άσκηση αυτή θα είναι σε θέση να αναλύουν προηγμένα τεχνικά περιστατικά κυβερνοασφάλειας, να αντιμετωπίζουν σύνθετες καταστάσεις επιχειρησιακής συνέχειας και διαχείρισης κρίσεων που απαιτούν συντονισμό και συνεργασία από το τοπικό έως το επίπεδο της ΕΕ.

Η σειρά ασκήσεων Cyber Europe αποσκοπεί στη βελτίωση της ετοιμότητας της Ευρώπης για την αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας, επιτρέποντας στους συμμετέχοντες να δοκιμάσουν και να βελτιώσουν την ετοιμότητά τους σε ολόκληρη την ΕΕ, να οικοδομήσουν εμπιστοσύνη στο οικοσύστημα κυβερνοασφάλειας της ΕΕ και να παρέχουν ευκαιρίες κατάρτισης.

Η συμμετοχή στην Cyber Europe παρέχει μια εξαιρετική ευκαιρία για:

- Αύξηση της ευαισθητοποίησης στον κυβερνοχώρο
- Δημιουργία ή/και δοκιμή διαδικασιών διαχείρισης κρίσεων στον κυβερνοχώρο
- Βελτίωση της επικοινωνίας εντός της αλυσίδας απόκρισης στον κυβερνοχώρο
- Δημιουργήστε μια κοινή γλώσσα και βελτιώστε την κατανόηση του ενός για τον άλλον
- Ανάπτυξη ποικίλων ατομικών και συλλογικών ικανοτήτων και δεξιοτήτων ανθεκτικότητας

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

- Ανάλυση σύνθετων τεχνικών περιστατικών κυβερνοασφάλειας- χειρισμός σύνθετων καταστάσεων επιχειρησιακής συνέχειας και διαχείρισης κρίσεων.

4.2.2. Προσαρμογή της διεπαφής και της τεχνολογίας

Η Ιαπωνία υπήρξε πρωτοπόρος στην προσαρμογή της τεχνολογίας και των συσκευών ώστε να είναι πιο προσιτές στους ηλικιωμένους. Για παράδειγμα, ορισμένα ιαπωνικά smartphones και tablets διαθέτουν απλούστερες διεπαφές χρήστη και βελτιωμένες λειτουργίες προσβασιμότητας, καθιστώντας τα πιο εύχρηστα για άτομα με περιορισμένες ψηφιακές δεξιότητες. Άλλες χώρες και κατασκευαστές τεχνολογίας μπορούν να υιοθετήσουν τέτοιες πολιτικές για να διασφαλίσουν ότι οι ηλικιωμένοι μπορούν να χρησιμοποιούν τις ψηφιακές συσκευές με ασφάλεια και αποτελεσματικότητα. Η υιοθέτηση αυτών των πρακτικών από άλλες χώρες και κατασκευαστές τεχνολογίας μπορεί να διασφαλίσει ότι οι ηλικιωμένοι ενήλικες έχουν πρόσβαση σε πιο φιλικές προς τον χρήστη ψηφιακές συσκευές, συμβάλλοντας στη βελτίωση της ασφάλειας και της συμμετοχής τους στο διαδίκτυο.

Στην ευρωπαϊκή επικράτεια πραγματοποιούνται διάφορα μαθήματα με στόχο την ευαισθητοποίηση των ηλικιωμένων στη χρήση αυτών των εργαλείων. Για παράδειγμα, η ένωση ACDA στο Παρίσι προσφέρει μαθήματα χαμηλού κόστους για την εισαγωγή των ηλικιωμένων στον κόσμο της τεχνολογίας. Τα μαθήματα αυτής της ένωσης προσφέρουν την ευκαιρία να μάθουν από τα βασικά τον χειρισμό ενός υπολογιστή. Την ανακάλυψη των μονάδων του υπολογιστή, των εφαρμογών, των μορφών αρχείων. Στη συνέχεια οι συμμετέχοντες μπορούν να αποκτήσουν πιο προχωρημένες δεξιότητες, όπως η διαχείριση και οργάνωση του γραμματοκιβωτίου τους και η εκμάθηση της χρήσης του word για τον τρόπο επεξεργασίας ενός γραπτού εγγράφου[5] .

4.2.3. Γραμμές βοήθειας και εξειδικευμένη υποστήριξη

Η Σιγκαπούρη έχει δημιουργήσει τη δική της γραμμή βοήθειας για ηλικιωμένους που αντιμετωπίζουν θέματα ψηφιακής ασφάλειας. Αυτή η γραμμή βοήθειας προσφέρει συμβουλές και τεχνική βοήθεια για την επίλυση ζητημάτων κυβερνοασφάλειας. Άλλες χώρες μπορούν να εξετάσουν το ενδεχόμενο να εισαγάγουν παρόμοιες υπηρεσίες για να παρέχουν ένα άμεσο και ασφαλές κανάλι επικοινωνίας για τους ηλικιωμένους που χρειάζονται ηλεκτρονική βοήθεια. Οι υπηρεσίες αυτές παρέχουν στους ηλικιωμένους ένα άμεσο και ασφαλές κανάλι επικοινωνίας για να λάβουν βοήθεια σε θέματα κυβερνοασφάλειας, όπως η διαδικτυακή απάτη ή το κακόβουλο λογισμικό. Η εισαγωγή παρόμοιων υπηρεσιών σε άλλες χώρες μπορεί να αποτελέσει ένα σημαντικό δίκτυο υποστήριξης για την προστασία των ηλικιωμένων στον ψηφιακό κόσμο.

[5] http://www.aucoursdesages.fr/cours.php

Για παράδειγμα, στην ευρωπαϊκή επικράτεια η ένωση AGE UK[6] θέτει ως προτεραιότητα την υποστήριξη των ηλικιωμένων που είναι πιο ευάλωτοι στον ψηφιακό αποκλεισμό.

Εκτός από την παροχή υπηρεσιών στον ηλικιωμένο πληθυσμό, τα μαθήματα θα επικεντρωθούν ειδικά στην παροχή βοήθειας σε μια ομάδα υψηλού κινδύνου για πρόσβαση στον ψηφιακό κόσμο. Παρόλο που τα βασικά στοιχεία του προγράμματος θα παραμείνουν σε μεγάλο βαθμό αμετάβλητα κατά την εργασία με αυτές τις ομάδες υψηλού κινδύνου, θα χρειαστούν πιθανώς κάποιες προσαρμογές για να διασφαλιστεί ότι το πρόγραμμα θα παραμείνει προσβάσιμο και αποτελεσματικό για όσους το χρειάζονται περισσότερο.

Οι υπηρεσίες υψηλού κινδύνου του προγράμματος Digital Champion θα στοχεύουν σε ηλικιωμένους που:

- Έχετε άνοια ή/και απώλεια μνήμης
- Έχουν χαμηλό εισόδημα
- Ζήσε μόνος σου
- Έχετε κινητικά προβλήματα
- Είναι κλεισμένοι στο σπίτι.

4.2.4. Εκστρατείες ευαισθητοποίησης και εκπαίδευσης

Χώρες όπως η Αυστραλία και ο Καναδάς έχουν εφαρμόσει εκστρατείες κυβερνοασφάλειας και προγράμματα εκπαίδευσης σε θέματα ψηφιακής ασφάλειας για ηλικιωμένους. Οι εκστρατείες αυτές παρέχουν πληροφορίες σχετικά με τις κοινές απειλές στον κυβερνοχώρο, συμβουλές για το πώς να προστατεύεστε από την ηλεκτρονική απάτη και τη σημασία της ενημέρωσης των συσκευών σας. Οι κυβερνήσεις μπορούν να συνεργαστούν με τοπικές οργανώσεις, κοινοτικά κέντρα και ομάδες εθελοντών για να προσεγγίσουν τον ηλικιωμένο πληθυσμό και να παρέχουν εκπαίδευση σε ψηφιακές δεξιότητες. Αυτές οι εκστρατείες ενημέρωσης και εκπαίδευσης στοχεύουν στην ενδυνάμωση των ηλικιωμένων μέσω της εκπαίδευσης στην ψηφιακή ασφάλεια. Διδάσκονται πώς να αναγνωρίζουν και να αποφεύγουν την ηλεκτρονική απάτη, να προστατεύουν τις προσωπικές τους πληροφορίες και να χρησιμοποιούν εργαλεία ασφαλείας, όπως antivirus και ισχυρούς κωδικούς πρόσβασης. Ενημερώνονται επίσης για τους κινδύνους που συνδέονται με τη χρήση των μέσων κοινωνικής δικτύωσης και τη σημασία των κατάλληλων ρυθμίσεων απορρήτου στο διαδίκτυο. Η ένωση που αναφέρεται παραπάνω ACDA στο Παρίσι προσφέρει επίσης μαθήματα ψηφιακής ασφάλειας.

Μια άλλη ένωση που επικεντρώνεται στην ψηφιακή ευαισθητοποίηση είναι το Orange Foundation, το οποίο ενημερώνει τις ευαίσθητες ομάδες για τις τελευταίες εξελίξεις στην τεχνολογία και τις κατευθύνει σε ασφαλέστερη ψηφιακή χρήση[7] .

[6] https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/
[7] https://fondationorange.com/en/digital-solidarity

Επιπλέον, το ίδρυμα Orange διοργανώνει μια σειρά δωρεάν μαθημάτων ψηφιακής κατάρτισης σε όλη τη Γαλλία για νέους και γυναίκες που συχνά είναι άνεργοι, δεν έχουν προσόντα και μερικές φορές βρίσκονται σε επισφαλείς καταστάσεις. Εκπαιδεύοντας τους ανθρώπους αυτούς σε ψηφιακές δεξιότητες, τους βοηθούν να επανακοινωνικοποιηθούν, να αναζητήσουν εργασία, να υιοθετήσουν τις επαγγελματικές χρήσεις της ψηφιακής τεχνολογίας, να αναπτύξουν μια επιχείρηση ή ακόμη και να κάνουν την ψηφιακή τεχνολογία επάγγελμά τους.

4.2.5. Προγράμματα οικονομικής προστασίας

Χώρες όπως το Ηνωμένο Βασίλειο και οι ΗΠΑ[8] έχουν θεσπίσει πολιτικές για την προστασία των συνταξιούχων από τις διαδικτυακές οικονομικές απάτες. Οι πολιτικές αυτές περιλαμβάνουν όρια ευθύνης για τα θύματα της απάτης και διορθωτικά μέτρα για την ανάκτηση των κλεμμένων κεφαλαίων. Άλλες χώρες μπορούν να διερευνήσουν αυτές τις πρωτοβουλίες και να τις προσαρμόσουν στα δικά τους χρηματοπιστωτικά συστήματα για την προστασία των ηλικιωμένων από πιθανές οικονομικές απώλειες. Η οικονομική προστασία των ηλικιωμένων αποτελεί σημαντικό μέρος της ψηφιακής ασφάλειας. Προγράμματα ειδικά σχεδιασμένα για την πρόληψη και τον μετριασμό της διαδικτυακής οικονομικής απάτης μπορούν να παρέχουν σε αυτόν τον πληθυσμό μεγαλύτερο επίπεδο ασφάλειας. Ο καθορισμός ορίων στην ευθύνη των θυμάτων απάτης και η δημιουργία μηχανισμών ανάκτησης των κλεμμένων χρημάτων είναι βήματα που μπορούν να ληφθούν. Αυτές οι πολιτικές όχι μόνο προστατεύουν την οικονομική ευημερία των ηλικιωμένων, αλλά στέλνουν επίσης ένα σαφές μήνυμα ότι η ευημερία και η οικονομική τους ασφάλεια λαμβάνονται σοβαρά υπόψη.

Στην Ευρώπη Ο καθορισμός ορίων στην ευθύνη των θυμάτων απάτης αποτελεί ζωτική πτυχή της διασφάλισης της οικονομικής ευημερίας των ηλικιωμένων. Όταν τα θύματα απάτης θεωρούνται υπεύθυνα για τις οικονομικές απώλειες που υφίστανται, αυτό μπορεί να οδηγήσει σε σοβαρές συνέπειες, συμπεριλαμβανομένης της οικονομικής καταστροφής και της συναισθηματικής οδύνης. Με την εφαρμογή πολιτικών που θεσπίζουν εύλογα όρια ευθύνης, η κοινωνία αναγνωρίζει τα μοναδικά τρωτά σημεία που αντιμετωπίζουν οι ηλικιωμένοι και επιδιώκει να ελαφρύνει το βάρος που τους αναλογεί. Το μέτρο αυτό παρέχει ένα δίχτυ ασφαλείας, διασφαλίζοντας ότι οι ηλικιωμένοι ενήλικες δεν επιβαρύνονται άδικα με τις επιπτώσεις των δόλιων δραστηριοτήτων. Η θέσπιση ορίων στην ευθύνη των θυμάτων απάτης αποτελεί βασική πτυχή της διασφάλισης της οικονομικής ευημερίας των ηλικιωμένων. Επί ευρωπαϊκού εδάφους, πολλές ενώσεις είναι αφιερωμένες στην προστασία των ηλικιωμένων, οι οποίοι συχνά πέφτουν θύματα ηλεκτρονικής απάτης, δεν είναι ενημερωμένοι και ενδέχεται να υποστούν οικονομικές απώλειες. Μια τέτοια ένωση είναι η

[8] https://www.bankofamerica.com/signature-services/elder-financial-services/

Marketing Management IO (MMIO), ένας πιστοποιημένος οργανισμός στην Ισπανία και τη Γαλλία.[9]

Όταν τα θύματα απάτης λογοδοτούν για τις οικονομικές τους απώλειες, αυτό μπορεί να έχει σοβαρές συνέπειες. Εξ ου και η σημασία της ευαισθητοποίησης. Με την εφαρμογή πολιτικών που θέτουν λογικά όρια ευθύνης, η κοινωνία αναγνωρίζει τα μοναδικά τρωτά σημεία των ηλικιωμένων και επιδιώκει να τους ελαφρύνει το βάρος. Το μέτρο αυτό παρέχει ένα δίχτυ ασφαλείας, διασφαλίζοντας ότι οι ηλικιωμένοι δεν επιβαρύνονται άδικα από τις επιπτώσεις των δόλιων δραστηριοτήτων.

Η Διαχείριση Μάρκετινγκ IO (MMIO) περιλαμβάνει θέματα όπως οι ευκαιρίες του Διαδικτύου, η φυσική αναφορά, η διαδικτυακή προβολή, το μάρκετινγκ περιεχομένου και η αύξηση των πωλήσεων. Οι έννοιες είναι απλοποιημένες και οι δράσεις είναι δωρεάν. Διατίθενται επίσης πόροι μπόνους.

Το μάθημα περιλαμβάνει 5 μαθήματα με βίντεο. Το Facebook προσφέρει μια πλατφόρμα με δωρεάν πρόσβαση σε πάνω από 70 διαδικτυακά μαθήματα. Αυτά τα μαθήματα επικεντρώνονται ειδικά στη χρήση του Facebook για τη βελτίωση της διαδικτυακής σας παρουσίας και των πωλήσεων της επιχείρησής σας, την ασφάλεια και την ευαισθητοποίηση.

4.2.6. Συνεργασία με την τεχνολογική βιομηχανία

Ορισμένες χώρες, όπως οι Ηνωμένες Πολιτείες, έχουν συνεργαστεί με εταιρείες τεχνολογίας για να αντιμετωπίσουν τις προκλήσεις ψηφιακής ασφάλειας που συνδέονται με τη γήρανση του πληθυσμού. Η συνεργασία αυτή μπορεί να περιλαμβάνει την ενίσχυση του λογισμικού ασφαλείας, τη βελτίωση της ανίχνευσης της απάτης και την εφαρμογή χαρακτηριστικών ασφαλείας σε ψηφιακά προϊόντα και υπηρεσίες. Η συνεργασία με την τεχνολογική βιομηχανία μπορεί να αποτελέσει έναν αποτελεσματικό τρόπο για την ενημέρωση σχετικά με τις πιο πρόσφατες απειλές και λύσεις για την ασφάλεια, όπως η εφαρμογή προηγμένων τεχνολογιών ασφαλείας, η βελτίωση της ανίχνευσης της απάτης και η προώθηση πρακτικών ασφαλείας για ψηφιακά προϊόντα και υπηρεσίες που απευθύνονται σε ηλικιωμένους. Η συνεργασία με την τεχνολογική βιομηχανία εξασφαλίζει ταχύτερη και πιο ενημερωμένη ανταπόκριση στις ψηφιακές απειλές.

Άλλες χώρες, όπως η Γαλλία και η Αγγλία, διαθέτουν μαθήματα ψηφιακής ασφάλειας για να βοηθήσουν τους ηλικιωμένους να κατανοήσουν τις αμυντικές τεχνολογίες- τα προσφερόμενα μαθήματα τους επιτρέπουν να χτίσουν μια βάση στην ψηφιοποίηση και να κατανοήσουν πώς να πλοηγούνται με ασφάλεια στο Διαδίκτυο.

Για παράδειγμα, το Konexio[10] προσφέρει κατάρτιση σε ψηφιακές δεξιότητες - από τις πιο βασικές έως τις πιο προηγμένες - για την προώθηση της κοινωνικής και επαγγελματικής

[9] https://www.marketing-management.io/blog/formation-digital-marketing
[10] https://www.konexio.eu/formations.html

ένταξης. Καινοτόμα, βασισμένα σε πρακτικές μελέτες περίπτωσης και με μεγάλη έμφαση στις εγκάρσιες και σχεσιακές δεξιότητες ή στις ήπιες δεξιότητες, τα εκπαιδευτικά μας προγράμματα στοχεύουν να δώσουν τη δυνατότητα σε όλους να ενταχθούν στην ψηφιοποίηση της κοινωνίας. Προσφέρουν διάφορους σχηματισμούς: ψηφιακές δεξιότητες, σχεδιαστής ιστοσελίδων, τεχνικός συστημάτων και δικτύων, ψηφιακοί βοηθοί. Το πρόγραμμα επικεντρώνεται στην εκμάθηση των κοινωνικών δεξιοτήτων και των κοινωνικών κωδίκων του επαγγελματικού κόσμου μέσω εργαστηρίων. Προσφέρει επίσης ευκαιρίες για άμεση σύνδεση με τον επαγγελματικό κόσμο μέσω του δικτύου μας. Προσφέρει τακτική παρακολούθηση και εξατομικευμένη υποστήριξη για να βοηθήσει τους μαθητές μας να σημειώσουν πρόοδο και να επιλύσουν τυχόν δυσκολίες που μπορεί να αντιμετωπίσουν.

4.2.7. Διεθνείς πόροι, εκθέσεις και πρωτοβουλίες

Οι πόροι αυτοί παρέχουν πολύτιμες οδηγίες και βέλτιστες πρακτικές για τη βελτίωση της ψηφιακής ασφάλειας στην εκπαίδευση ενηλίκων στην ΕΕ.

Ένας ανοικτός, ασφαλής και προστατευμένος κυβερνοχώρος: Η παρούσα έκθεση παρέχει μια επισκόπηση της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, η οποία αποσκοπεί στην προώθηση ενός ανοικτού, ασφαλούς και προστατευμένου κυβερνοχώρου στην Ευρώπη. Η έκθεση περιλαμβάνει βέλτιστες πρακτικές για τη βελτίωση της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένης της διαχείρισης κινδύνων, της αντιμετώπισης περιστατικών και των συμπράξεων δημόσιου και ιδιωτικού τομέα.

ENISA Threat Landscape Report: Η έκθεση αυτή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) παρέχει μια επισκόπηση του σημερινού τοπίου απειλών για την κυβερνοασφάλεια στην Ευρώπη, συμπεριλαμβανομένων των συνηθέστερων τύπων κυβερνοεπιθέσεων και των τομέων που διατρέχουν τον μεγαλύτερο κίνδυνο. Η έκθεση περιλαμβάνει βέλτιστες πρακτικές για την πρόληψη και τον μετριασμό των επιθέσεων στον κυβερνοχώρο, συμπεριλαμβανομένης της εκπαίδευσης σε θέματα ευαισθητοποίησης σε θέματα ασφάλειας, της διαχείρισης ευπαθειών και του σχεδιασμού αντιμετώπισης περιστατικών.

Οδηγία NIS και πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο: Η παρούσα έκθεση παρέχει μια επισκόπηση του νομικού πλαισίου της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμπεριλαμβανομένης της οδηγίας για τα συστήματα δικτύων και πληροφοριών (NIS) και της πράξης της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Η έκθεση περιλαμβάνει βέλτιστες πρακτικές για τη συμμόρφωση με τις νομικές απαιτήσεις, όπως η αναφορά περιστατικών και η διαχείριση κινδύνων.

Πλαίσιο πιστοποίησης κυβερνοασφάλειας της ΕΕ: Η έκθεση αυτή παρέχει μια επισκόπηση του πλαισίου πιστοποίησης της κυβερνοασφάλειας της ΕΕ, το οποίο αποσκοπεί στη βελτίωση της ασφάλειας και της αξιοπιστίας των ψηφιακών προϊόντων και υπηρεσιών. Η έκθεση περιλαμβάνει βέλτιστες πρακτικές για την απόκτηση και τη διατήρηση πιστοποιήσεων κυβερνοασφάλειας, συμπεριλαμβανομένης της ασφάλειας από το

σχεδιασμό, τη δοκιμή και την αξιολόγηση, καθώς και τη συνεχή παρακολούθηση και αξιολόγηση.

Κυβερνοασφάλεια για ΜΜΕ: Η έκθεση αυτή παρέχει καθοδήγηση και βέλτιστες πρακτικές για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) σχετικά με τη βελτίωση της κατάστασης της κυβερνοασφάλειάς τους. Η έκθεση περιλαμβάνει συμβουλές σχετικά με τη διαχείριση κινδύνων, την εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας, την ασφαλή ανάπτυξη λογισμικού και τον σχεδιασμό αντιμετώπισης περιστατικών.

Ψηφιακές δεξιότητες στον ενήλικο πληθυσμό: Αυτή η έκθεση της Ευρωπαϊκής Επιτροπής παρέχει μια επισκόπηση των ψηφιακών δεξιοτήτων του ενήλικου πληθυσμού στην ΕΕ. Περιλαμβάνει μια ενότητα για την ψηφιακή ασφάλεια, η οποία υπογραμμίζει την ανάγκη οι ενήλικες να έχουν βασικές γνώσεις και δεξιότητες για να προστατεύονται από απειλές στον κυβερνοχώρο.

Ψηφιακές δεξιότητες για δια βίου μάθηση: Αυτή η έκθεση της Ευρωπαϊκής Επιτροπής παρέχει καθοδήγηση και βέλτιστες πρακτικές για την ανάπτυξη ψηφιακών δεξιοτήτων μεταξύ των ενηλίκων. Περιλαμβάνει μια ενότητα για την ψηφιακή ασφάλεια, η οποία παρέχει συμβουλές σχετικά με τη διαχείριση κινδύνων, την ασφαλή περιήγηση, τη διαχείριση κωδικών πρόσβασης και την προστασία δεδομένων.

Το έργο "Κυβερνοασφάλεια για την ψηφιακή εκπαίδευση": Το έργο αυτό του European Schoolnet παρέχει πόρους και κατάρτιση σχετικά με την κυβερνοασφάλεια για εκπαιδευτικούς και μαθητές στην Ευρώπη. Το έργο περιλαμβάνει μια σειρά υλικών, συμπεριλαμβανομένων διαδικτυακών μαθημάτων, σχεδίων μαθημάτων και εργαλείων αξιολόγησης, τα οποία επικεντρώνονται στη βελτίωση της ψηφιακής ασφάλειας στην εκπαίδευση.

Το πρόγραμμα "Ψηφιακή ασφάλεια για ηλικιωμένους πολίτες": Αυτό το έργο του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) παρέχει πόρους και κατάρτιση σχετικά με την κυβερνοασφάλεια για τους ηλικιωμένους πολίτες. Το έργο περιλαμβάνει μια σειρά υλικών, συμπεριλαμβανομένων διαδικτυακών μαθημάτων, οδηγών και βίντεο, τα οποία επικεντρώνονται στη βελτίωση της ψηφιακής ασφάλειας των ηλικιωμένων.

Συνασπισμός για ψηφιακές δεξιότητες και θέσεις εργασίας: Η πρωτοβουλία αυτή της Ευρωπαϊκής Επιτροπής αποσκοπεί στη βελτίωση των ψηφιακών δεξιοτήτων των Ευρωπαίων, ώστε να μπορέσουν να συμμετάσχουν πλήρως στην ψηφιακή οικονομία. Περιλαμβάνει μια σειρά πόρων και ευκαιριών κατάρτισης, μεταξύ άλλων για την ψηφιακή ασφάλεια.

4.3. Βέλτιστες πρακτικές της εκπαίδευσης ενηλίκων για την ψηφιακή ασφάλεια

Πρόγραμμα εκπαίδευσης εκπαιδευτών του ENISA

Όλο το ηλεκτρονικό εκπαιδευτικό υλικό και τα εκπαιδευτικά μαθήματα στην ενότητα "Εκπαιδευτικά μαθήματα για ειδικούς στην ασφάλεια στον κυβερνοχώρο" βασίζονται στη φιλοσοφία "Εκπαιδεύστε τον εκπαιδευτή". Το πρόγραμμα και η φιλοσοφία "Εκπαιδεύστε τον εκπαιδευτή" αποσκοπούν στην επέκταση του δικτύου εκπαιδευτών και στην προώθηση της καλύτερης ανταλλαγής πληροφοριών. Αυτό θα εξυπηρετήσει διάφορους σκοπούς, μεταξύ άλλων:

- Κοινή χρήση εκπαιδευτικού υλικού για την εξοικονόμηση χρόνου και χρημάτων στην εκπαίδευση,
- Δημιουργία περιφερειακών προσπαθειών κατάρτισης,
- Προώθηση της συνεργασίας μεταξύ διαφορετικών παρόχων κατάρτισης,
- Προώθηση ορθών πρακτικών κατάρτισης,
- Μείωση του ανταγωνισμού και των επικαλύψεων.

Το διαδικτυακό εκπαιδευτικό υλικό του ENISA θα περιλαμβάνει ένα εγχειρίδιο εκπαιδευτών, ένα σύνολο εργαλείων για μαθητές και εικονικές μηχανές για λήψη. Αυτό επιτρέπει στους δυνητικούς εκπαιδευτές να προετοιμάσουν το μάθημα, ενώ το Εγχειρίδιο θα τους βοηθήσει στην καθοδήγηση των μαθητών κατά τη διάρκεια του μαθήματος. Θα περιέχει φύλλα αντιγραφής, πιθανά μικρά τεστ για να διαπιστωθεί αν οι μαθητές έχουν κατανοήσει τα σημαντικά μαθήματα των μαθημάτων, καθώς και πρόσθετες πληροφορίες ή ασκήσεις που μπορεί να χρησιμοποιήσει ο εκπαιδευτής για να κάνει το μάθημα πιο ενδιαφέρον ή πιο απαιτητικό.

Η μάθηση από τις επιτυχίες και τις αποτυχίες των άλλων επιτρέπει τόσο στους αρχάριους όσο και στους έμπειρους εκπαιδευτές να σχεδιάζουν και να υλοποιούν καλύτερα τις εκπαιδεύσεις, καθιστώντας τες πιο επιτυχημένες, πιο "διασκεδαστικές" και με καλύτερα και πιο μακροχρόνια αποτελέσματα.

TiK - Τεχνολογία εν συντομία

Το έργο υψηλής τεχνολογίας ακολουθεί μια διαγενεακή προσέγγιση μέσω της κατάρτισης που προσφέρουν νέοι εθελοντές (ηλικίας 16 έως 30 ετών) ως οι λεγόμενοι "εκπαιδευτές ταμπλετών", οι οποίοι εκπαιδεύονται σύμφωνα με ένα ειδικό πρόγραμμα εκπαίδευσης με ταμπλέτες. Τα μαθήματα διακρίνονται από μια πληθώρα μεθόδων και ευέλικτων κατευθυντήριων ερωτήσεων και μια ιδιαίτερη δέσμευση των νέων εκπαιδευτών. Προσφέρουν εθελοντικά μαθήματα χαμηλού κατωφλιού με μικρή μόνο αποζημίωση εξόδων. Η περαιτέρω ανάπτυξη των μαθημάτων εξασφαλίζεται από την ανατροφοδότηση των συμμετεχόντων και των εκπαιδευτών, οι οποίοι επίσης επεξεργάζονται δικό τους ειδικό υλικό και έντυπα χωρίς εμπόδια για τους ηλικιωμένους. Τα μαθήματα είναι εύκολα προσβάσιμα από τους ενδιαφερόμενους και δίνεται μεγάλη προσοχή στην ευρεία γεωγραφική διανομή των "TiKmodules" και των πληροφοριών στην ιστοσελίδα www.digitaleseniorinnen.at. Οι συμμετέχοντες στα μαθήματα είναι άτομα και ιδιαίτερα οικονομικά μειονεκτούσες γυναίκες

με χαμηλό μορφωτικό επίπεδο. Μέχρι το τέλος του 2018 περισσότερα από 2.000 άτομα έμαθαν με τις ενότητες και άλλα 1.000 άτομα συμμετείχαν στο πρόγραμμα μαθημάτων. Ο γηραιότερος συμμετέχων που συμμετέχει απλώς σε ένα μάθημα είναι 97 ετών, παίρνει την εκπαίδευσή του από έναν νεαρό άνδρα σε ένα βρεφονηπιακό ίδρυμα. Το πρόγραμμα βραβεύτηκε αρκετές φορές σε ομοσπονδιακό και επαρχιακό επίπεδο.

5. Εκπαίδευση ενηλίκων: Πώς να οικοδομήσουμε ψηφιακή ανθεκτικότητα

Η ανδραγωγική ως μελέτη της εκπαίδευσης ενηλίκων ξεκίνησε στην Ευρώπη τη δεκαετία του 1950, αλλά μόλις τη δεκαετία του 1970 πρωτοστάτησε ως θεωρία και μοντέλο εκπαίδευσης ενηλίκων από τον Malcolm Knowles, έναν Αμερικανό επαγγελματία και θεωρητικό της εκπαίδευσης ενηλίκων, ο οποίος όρισε την ανδραγωγική ως "την τέχνη και την επιστήμη του να βοηθάς τους ενήλικες να μαθαίνουν" (Fidishun 2000). Ο Fidishun (2000) πρότεινε να χρησιμοποιούνται οι αρχές της ανδραγωγικής στο σχεδιασμό των διαδικτυακών τάξεων, ώστε να διευκολύνεται "η ευελιξία και η δυνατότητα των εκπαιδευομένων να κινούνται στα μαθήματα όποτε, όπου και με το δικό τους ρυθμό".

5.1. Τέσσερις αρχές της Ανδραγωγικής

Λαμβάνοντας υπόψη ότι οι ενήλικες έχουν τον δικό τους, μοναδικό τρόπο μάθησης, υπάρχουν 4 κεντρικές αρχές που εξηγούν πώς να αναπτύξουμε καλύτερα την εκπαίδευση γι' αυτούς.

- Όταν πρόκειται για μάθηση, οι ενήλικες θέλουν ή πρέπει να συμμετέχουν στον τρόπο με τον οποίο σχεδιάζεται, παρέχεται και εκτελείται η εκπαίδευσή τους. Θέλουν να ελέγχουν τι, πότε και πώς μαθαίνουν.
- Οι ενήλικες κερδίζουν περισσότερα όταν μπορούν να αξιοποιήσουν τις εμπειρίες του παρελθόντος στη διαδικασία μάθησης. Μπορούν να αντλήσουν από αυτά που γνώριζαν προηγουμένως για να προσθέσουν μεγαλύτερο πλαίσιο στη μάθησή τους.
- Η απομνημόνευση γεγονότων και πληροφοριών δεν είναι ο σωστός τρόπος μάθησης για τους ενήλικες. Πρέπει να λύνουν προβλήματα και να χρησιμοποιούν συλλογισμούς για να προσλαμβάνουν με τον καλύτερο δυνατό τρόπο τις πληροφορίες που τους παρουσιάζονται.
- Οι ενήλικες θέλουν να μάθουν "Πώς μπορώ να χρησιμοποιήσω αυτές τις πληροφορίες τώρα;". Αυτό που μαθαίνουν πρέπει να είναι εφαρμόσιμο στη ζωή τους και να μπορεί να εφαρμοστεί άμεσα.

5.2. Πώς οι εκπαιδευτές ενηλίκων θα εφαρμόσουν την Ανδραγωγική

Ενεργοποίηση της αυτοκατευθυνόμενης μάθησης

Στο παρελθόν, η μάθηση ήταν συχνά μια υποχρεωτική δραστηριότητα που γινόταν σε μια συγκεκριμένη ώρα. Τώρα, με τεχνολογίες όπως ένα σύστημα διαχείρισης μάθησης, μπορούμε να δημιουργήσουμε ένα πολύ πιο αυτοκατευθυνόμενο, ανεξάρτητο περιβάλλον μάθησης για τους ενήλικες εκπαιδευόμενους. Μπορούμε να τους επιτρέψουμε να εκπαιδεύονται όταν και όπου θέλουν, να τους προσφέρουμε μια επιλογή μαθημάτων στα οποία μπορούν να επιλέξουν να εγγραφούν και να τους δώσουμε τη δυνατότητα να έχουν τους δικούς τους ξεχωριστούς μαθησιακούς στόχους.

Χρήση πραγματικών παραδειγμάτων μάθησης

Όπως αναφέρει η θεωρία, οι ενήλικες επιθυμούν να γνωρίζουν πώς η εκπαίδευση θα έχει άμεση εφαρμογή και όφελος για αυτούς. Έτσι, όταν δημιουργούμε περιεχόμενο μαθημάτων, θα πρέπει να το εμπλουτίζουμε με όσο το δυνατόν περισσότερα παραδείγματα από τον πραγματικό κόσμο.

Όταν εκπαιδεύετε ενήλικες εκπαιδευόμενους στην ψηφιακή ευημερία ή/και την ψηφιακή ασφάλεια, καθοδηγήστε τους βήμα προς βήμα σε μια ροή εργασίας που θα χρησιμοποιήσουν στην πραγματικότητα και δηλώστε ρητά πώς και γιατί θα τη χρησιμοποιήσουν. Δηλώστε πώς θα βοηθήσει η εκπαίδευση και στη συνέχεια χρησιμοποιήστε γνήσια παραδείγματα για την εκπαίδευση.

Αφήνοντας τους ενήλικες εκπαιδευόμενους να το καταλάβουν μόνοι τους

Δεδομένου ότι οι ενήλικες προτιμούν την επίλυση προβλημάτων από την απλή πληροφόρηση, όταν δημιουργείτε περιεχόμενο, καλό είναι να μην δίνετε κατευθείαν όλες τις απαντήσεις. Γιατί να μην γίνετε δημιουργικοί και να δημιουργήσετε μαθήματα που να ενεργοποιούν το μυαλό των μαθητών σας;

Μπορούμε να το κάνουμε αυτό με μερικούς απλούς τρόπους, όπως η προσθήκη αξιολογήσεων και προσομοιώσεων που περιγράφουν συγκεκριμένα προβλήματα που μπορεί να αντιμετωπίσει ένας εκπαιδευόμενος και στη συνέχεια να βάλουμε τους ενήλικες εκπαιδευόμενους να χρησιμοποιήσουν τις δεξιότητές τους για να τα ξεπεράσουν.

6. Συμπέρασμα

Η ψηφιακή ασφάλεια των ηλικιωμένων είναι ένα βασικό ζήτημα που απαιτεί προσοχή και δράση από τις κυβερνήσεις και την κοινωνία στο σύνολό της. Εφαρμόζοντας τις προαναφερθείσες καλές πρακτικές, οι χώρες μπορούν να βελτιώσουν την ψηφιακή προστασία και την ευημερία του γηράσκοντος πληθυσμού τους. Η ευαισθητοποίηση, η εκπαίδευση, η ειδική υποστήριξη, η τεχνολογική προσαρμογή και η συνεργασία του κλάδου

αποτελούν βασικούς πυλώνες για τη διασφάλιση μιας ασφαλούς και θετικής διαδικτυακής εμπειρίας για τους ηλικιωμένους.

Το έργο DigiWELL στοχεύει στην ενσωμάτωση των αρχών της ψηφιακής ευημερίας στην εκπαίδευση ενηλίκων. Οι πρωτοβουλίες του αποσκοπούν στη συμβολή στις συνολικές πρακτικές των οργανισμών, δικτύων και πρωτοβουλιών εκπαίδευσης ενηλίκων. Το έργο αντιλαμβάνεται πόσο ζωτικής σημασίας είναι να αντιμετωπιστεί ο τρόπος με τον οποίο η τεχνολογία επηρεάζει την ψυχική υγεία, την παραγωγικότητα και τη γενική ευημερία των ενηλίκων στην ψηφιακή εποχή. Ο κύριος στόχος του DigiWELL είναι να παρέχει στους ενήλικες εκπαιδευόμενους τις πληροφορίες, τις ικανότητες και τους πόρους που είναι απαραίτητοι για την ηθική και ενσυνείδητη πλοήγηση στον ψηφιακό κόσμο. Το έργο DigiWELL περιλαμβάνει επίσης τη δημιουργία και εκτέλεση πρόσθετων πρωτοβουλιών ενδυνάμωσης των ενήλικων εκπαιδευομένων. Στόχος αυτών των δραστηριοτήτων είναι η παροχή ενός υποστηρικτικού περιβάλλοντος όπου οι ενήλικες μπορούν να μοιραστούν τις εμπειρίες, τις δυσκολίες και τους θριάμβους τους στην προώθηση της ψηφιακής ευημερίας. Με αυτό το σκεπτικό, το έργο DigiWELL παρουσιάζει πολλές ευκαιρίες για τα άτομα και τους οργανισμούς ενηλίκων να ευαισθητοποιηθούν και να διαφωτιστούν σχετικά με τη σημασία της ψηφιακής ευημερίας και με τον τρόπο προώθησης της ψηφιακής ευημερίας των ενήλικων ατόμων και των εκπαιδευτών και εκπαιδευτών ενηλίκων. Η ενεργοποίηση της ψηφιακής ευημερίας με μια ολιστική προσέγγιση είναι πολύ πιο εφικτή εάν όλα τα σχετικά μέρη αναλάβουν δράση για την υποστήριξη των αναγκών ψηφιακής ευημερίας των ατόμων. Κατά συνέπεια, οι πληροφορίες, οι συμβουλές και οι καλές πρακτικές που παρουσιάζονται στο παρόν εγχειρίδιο καλούν τους ανθρώπους και τους ενδιαφερόμενους οργανισμούς να αναλάβουν πρωτοβουλίες ώστε περισσότεροι από εμάς να έχουμε καλύτερη ψηφιακή ευημερία και επίσης ισχυρότερη ψηφιακή ζωή.

7. Αναφορές

Για την προετοιμασία του λεξικού χρησιμοποιήθηκαν ελεύθερα διαθέσιμες διαδικτυακές πηγές: διαδικτυακά λεξικά, επιστημονικά άρθρα και βιβλιογραφία στον τομέα της ασφάλειας των πληροφοριών, των ψηφιακών τεχνολογιών και υπηρεσιών, της ψηφιακής ευημερίας και της ψηφιακής ανθεκτικότητας, καθώς και όροι και ορισμοί από το αντικείμενο της ασφάλειας των πληροφοριών. Όλες οι πηγές παρατίθενται στη βάση δεδομένων κειμένου της έκδοσης εργασίας του λεξικού.

1 BAI. Γλωσσάριο της Επιτροπής Συστημάτων Εθνικής Ασφάλειας (CNSS) (2015). Στο *BAI Information Security Consulting & Training [online]*. Ανακτήθηκε από: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Γλωσσάριο Capterra*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Γλωσσάριο*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Γλωσσάριο όρων για την ασφάλεια στον κυβερνοχώρο*. Παγκόσμια γνώση. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Γλωσσάριο*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Γλωσσάριο*. Το Εργαστήριο Ψηφιακής Ευεξίας. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Ασφάλεια στον κυβερνοχώρο - Κατευθυντήριες γραμμές για την ασφάλεια στο Διαδίκτυο*. Πλατφόρμα διαδικτυακής περιήγησης (OBP) - ISO. https://www.iso.org/obp/ui/iso.

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Πέμπτη έκδοση.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, 16 Ιουλίου). *Γλωσσάριο βασικών όρων για την ασφάλεια των πληροφοριών*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1.

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Γλωσσάριο βασικών όρων ασφάλειας πληροφοριών*. NIST. Ανακτήθηκε από: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Ασφάλεια υπολογιστών: Μανώλης*: *Αρχές και πρακτική. Τρίτη έκδοση.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *Γλωσσάριο TVETipedia*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Διδασκαλία ενηλίκων φοιτητών στη χρήση ηλεκτρονικών πηγών: Αξιοποιώντας τα κλειδιά του Lawler για τη μάθηση ενηλίκων για να γίνει η διδασκαλία πιο αποτελεσματική. *Πληροφορική και βιβλιοθήκες*, *19*(3), 157-157.

15 Ευρωπαϊκή Επιτροπή, Γενική Διεύθυνση Εκπαίδευσης, Νεολαίας, Αθλητισμού και Πολιτισμού, Βασικές ικανότητες για τη διά βίου μάθηση, Υπηρεσία Εκδόσεων, 2019, https://data.europa.eu/doi/10.2766/569540.