DIGITAL SECURITY FOR SENIOR CITIZENS

2020-1-PL01-KA204-082121

Πλαίσιο ικανοτήτων ψηφιακής ασφάλειας

Αυτό το έργο χρηματοδοτείται με την υποστήριξη του ταμείου της Ευρωπαϊκής Επιτροπής. Η δημοσίευση αυτή αφορά απόψεις μόνο των συγγραφέων και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση μπορεί να πραγματατοποιηθεί απο τη λήψη των συγκεκριμένων πληροφοριών που συμπεριλαμβάνονται στο έργο

Συντελεστές

Cuiablue Ltd, Ηνωμένο Βασίλειο

CWEP, Πολωνία

FyG Consultores, Ισπανία

eSeniors, Γαλλία

Innovation Hive, Ελλάδα

Περιεχόμενα

Υπόβαθρο

Το πλαίσιο αυτό αναπτύχθηκε ως μέρος του πνευματικού αποτελέσματος 1 του έργου DiSC (Ψηφιακή ασφάλεια για τους πολίτες μεγαλύτερης ηλικίας). Στο πλαίσιο του ευρύτερου πεδίου εφαρμογής του έργου DiSC, αυτό το αποτέλεσμα αποσκοπεί στην υποστήριξη του έργου για την ανάπτυξη της ψηφιακής ικανότητας των ηλικιωμένων πολιτών να αναγνωρίζουν και να προσαρμόζονται προληπτικά στις απειλές και τις απάτες της ψηφιακής ασφάλειας και να θέσει τις βάσεις για την εφαρμογή και την υιοθέτηση στοχευμένων πολιτικών ψηφιακής ασφάλειας σε ευρωπαϊκό επίπεδο. Το παρόν πλαίσιο αποτελεί ένα μικρό βήμα προς τους δύο αυτούς στόχους.

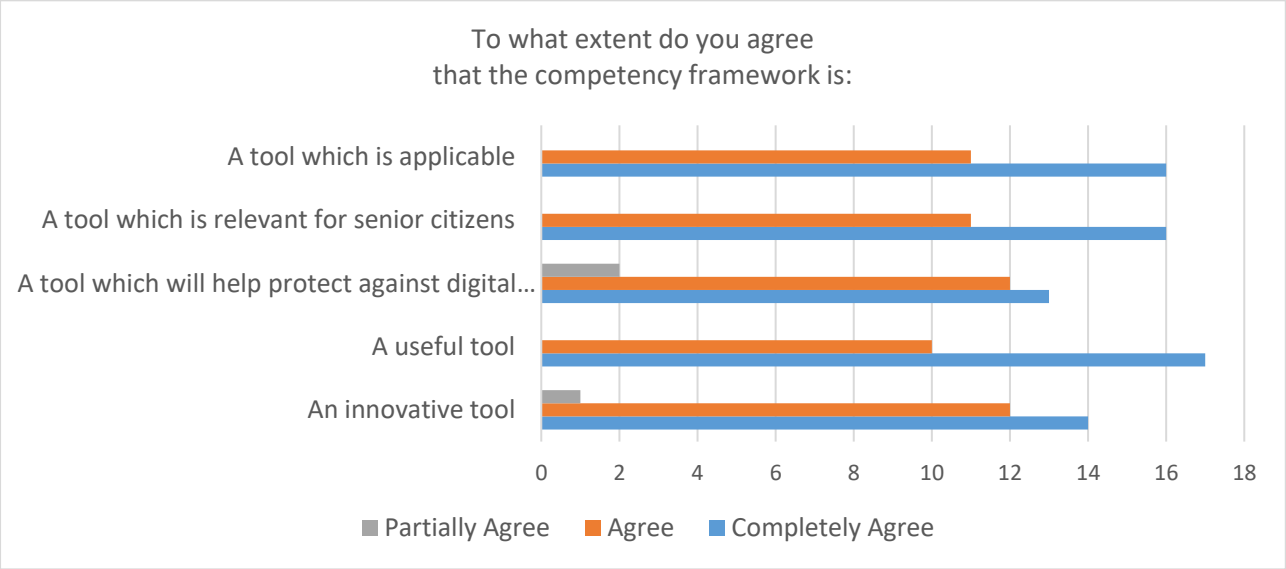
Μεθοδολογία

Η σύμπραξη συζήτησε και συμφώνησε σχετικά με τη μεθοδολογική προσέγγιση για την ανάπτυξη του πλαισίου κατά τη διάρκεια της εναρκτήριας συνάντησης του έργου τον Δεκέμβριο του 2020. Αρχικά, αναπτύχθηκε ένα σύνολο ερωτηματολογίων για τις συνεδριάσεις διαβούλευσης με τους ενδιαφερόμενους φορείς και ένα πρότυπο για την έρευνα γραφείου, το οποίο βελτιώθηκε και τροποποιήθηκε αναλόγως, ώστε οι εταίροι να είναι σε θέση να αρχίσουν να συγκεντρώνουν πληροφορίες σχετικά με την τρέχουσα κατάσταση των πληροφοριών, των συμβουλών, της καθοδήγησης και της πολιτικής για την ψηφιακή ασφάλεια σε εθνικό επίπεδο σε κάθε εκπροσωπούμενη χώρα. Ενώ η κοινοπραξία ανέλαβε την έρευνα γραφείου, αναπτύχθηκε το αρχικό σχέδιο του πλαισίου. Αφού συνοψίστηκαν και αναλύθηκαν τα αποτελέσματα της έρευνας γραφείου και ελήφθησαν υπόψη τα σχόλια που ελήφθησαν από τις συναντήσεις διαβούλευσης με τους ενδιαφερόμενους φορείς, αναπτύχθηκε η δεύτερη επανάληψη του πλαισίου για σχόλια και ανατροφοδότηση από την κοινοπραξία. Αφού ενσωματώθηκαν τα σχόλια και οι παρατηρήσεις, η οριστικοποιημένη έκδοση του πλαισίου μεταφράστηκε και δοκιμάστηκε πιλοτικά με ευρύτερες ομάδες ενδιαφερομένων και τελικούς χρήστες.

Διαβούλευση με τα ενδιαφερόμενα μέρη

Στο πλαίσιο της προσέγγισης του έργου DiSC για τη συνδημιουργία των αποτελεσμάτων του έργου, παρατίθεται παρακάτω περίληψη των σχετικών στοιχείων που συγκεντρώθηκαν από τις πρώτες συναντήσεις διαβούλευσης με τους ενδιαφερόμενους φορείς στις αρχές του 2021 από όλους τους εταίρους του έργου. Οι δηλώσεις σχετικά με το πλαίσιο ικανοτήτων

συνοψίζονται παρακάτω, μετά τις οποίες οι ενδιαφερόμενοι κλήθηκαν να σχολιάσουν την απόφασή τους ή να προσθέσουν τυχόν σκέψεις σχετικά με το πλαίσιο.



Στη συνέχεια ζητήθηκε από τους ενδιαφερόμενους να δώσουν συνέχεια στις ποσοτικές απαντήσεις απαντώντας στην ερώτηση "Έχετε κάποια σχόλια ή συστάσεις που θα μας βοηθούσαν να βελτιώσουμε το Πλαίσιο για τις Ικανότητες Ψηφιακής Ασφάλειας;" και τους δόθηκε ένα ανοιχτό πλαίσιο κειμένου για να δώσουν οποιαδήποτε σχόλια, σκέψεις ή γενικές εντυπώσεις σχετικά με την έννοια που είχαν.

Ειδικές προτάσεις περιλάμβαναν την εξασφάλιση σχετικού λεξιλογίου για την κατανόηση από τους ηλικιωμένους και την εστίαση σε βασικές, εφικτές απαιτήσεις για να εξασφαλιστεί η προσβασιμότητα και η υιοθέτηση. Μια άλλη τέτοια πρόταση ήταν να παρέχονται στους χρήστες τα μέσα και οι πόροι για την ανάπτυξη κάθε ικανότητας, οι οποίοι υποστηρίζουν την ανάγκη για IO2 και IO3.

Η πιο συχνή πρόταση που ελήφθη ήταν ότι το πλαίσιο πρέπει να λαμβάνει υπόψη τις πιο πρόσφατες και ταχύτατες τεχνολογικές εξελίξεις και τα συναφή ζητήματα ασφάλειας στον κυβερνοχώρο- τα κρυπτονομίσματα και οι εκατοντάδες συνεχώς εξελισσόμενες, δημιουργικές προσεγγίσεις που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να επιχειρήσουν να κλέψουν τέτοια νομίσματα είναι ένα καλό παράδειγμα. Μέσα σε αυτό το πλαίσιο, η κοινοπραξία DiSC αντιμετωπίζει τη μεγαλύτερη πρόκληση κατά την εκπόνηση του πλαισίου: πρέπει να είναι αρκετά ολοκληρωμένο ώστε να καλύπτει το ευρύ φάσμα των

διαφορετικών δεξιοτήτων και γνώσεων που απαιτούνται, αλλά και αρκετά ευέλικτο ώστε να προσαρμόζεται στις μελλοντικές καινοτομίες.

Έρευνα γραφείου

Η δεύτερη φάση που ανέλαβε η κοινοπραξία επικεντρώθηκε στη συγκέντρωση σχετικών πληροφοριών, συμβουλών, οδηγιών και εγγράφων εθνικής πολιτικής που θα βοηθούσαν να διαμορφωθεί το πλαίσιο εντός του οποίου εντάσσεται το πλαίσιο αρμοδιοτήτων ψηφιακής ασφάλειας τόσο σε εθνικό επίπεδο σε κάθε χώρα εταίρο όσο και σε ευρωπαϊκό επίπεδο. Συνολικά, η κοινοπραξία ανέλυσε 10 σχετικά έγγραφα, δύο από την Πολωνία, το Ηνωμένο Βασίλειο, την Ελλάδα, τη Γαλλία και την Ισπανία, τα οποία συνοψίζονται παρακάτω. Όλες οι έρευνες γραφείου βρίσκονται ως παράρτημα στο τέλος του παρόντος εγγράφου.

Εθνική στρατηγική της Ελλάδας για την ασφάλεια στον κυβερνοχώρο 2020 - 2025: αποτελείται από ένα εθνικό σχέδιο για την περίοδο 2020-2025 που περιλαμβάνει τους στρατηγικούς στόχους, τις προτεραιότητες, την πολιτική και τα ρυθμιστικά μέτρα για την εξασφάλιση υψηλού επιπέδου ασφάλειας των ψηφιακών συστημάτων επικοινωνίας και πληροφοριών σε εθνικό επίπεδο. Η εκστρατεία της Ελληνικής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος για την ασφάλεια στον κυβερνοχώρο σχετικά με το κακόβουλο λογισμικό για κινητά τηλέφωνα παρουσιάζει σχετικές πληροφορίες και ιδέες σχετικά με τις μορφές των ψηφιακών απειλών και τον τρόπο με τον οποίο οι χάκερ θα μπορούσαν να παραβιάσουν τα προσωπικά δεδομένα των πολιτών.

Στη Γαλλία, τα δύο έγγραφα που εξετάστηκαν ήταν ο δικτυακός τόπος Cyber Malveillance, που δημοσιεύθηκε το 2021 από τη γαλλική κυβέρνηση, και ένα συνοπτικό έγγραφο της CNIL (Εθνική Επιτροπή Πληροφορικής και Ελευθεριών) με τίτλο "10 συμβουλές από την CNIL για να παραμείνετε καθαροί στον Ιστό". Και τα δύο έγγραφα δημοσιεύονται με σκοπό την ευαισθητοποίηση και την ανάπτυξη της ικανότητας αντιμετώπισης των απειλών στον κυβερνοχώρο μεταξύ όλων των πολιτών. Τα δύο έγγραφα διαφέρουν ως προς τον σχεδιασμό και το επίπεδο και το βάθος των πληροφοριών που μεταδίδουν και, ως εκ τούτου, ευθυγραμμίζονται καλά με το έργο DiSC όσον αφορά το τι επιδιώκουμε να επιτύχουμε και πώς η κοινοπραξία του έργου DiSC θα εμπλακεί και θα παρουσιάσει τις πληροφορίες στους τελικούς χρήστες.

Στην Πολωνία, η έρευνα επικεντρώθηκε σε έναν επίσημο οδηγό κυβερνοασφάλειας για τους πολίτες, ο οποίος αναπτύχθηκε και δημοσιεύθηκε από την πολωνική κυβέρνηση με τίτλο "Πώς να προστατευτείτε από τις κυβερνοεπιθέσεις". Το έγγραφο παρέχει ένα βασικό πλαίσιο για το τι θα μπορούσε να θεωρηθεί ως βασική γνώση σχετικά με τη χρήση του διαδικτύου και ιδίως των μέσων κοινωνικής δικτύωσης και, ως εκ τούτου, θα μπορούσε να ληφθεί υπόψη κατά την ανάπτυξη του πλαισίου και, ενδεχομένως, να προσαρμοστεί και να συμπεριληφθεί. Το δεύτερο είναι ένας οδηγός που αναπτύχθηκε μέσω ενός άλλου έργου της ΕΕ. Το έγγραφο παρέχει καθοδήγηση σχετικά με τις βασικές γνώσεις και την ευαισθητοποίηση που θα μπορούσαν να έχουν όλοι οι πολίτες σε βασικό επίπεδο, ώστε να ληφθούν υπόψη κατά την ανάπτυξη του πλαισίου και να προσαρμοστούν και να συμπεριληφθούν. Οι πληροφορίες και στα δύο περιέχουν σχετικό περιεχόμενο που έχει αξία για την εφαρμογή του DiSC και μπορεί να συσχετιστεί με πολλά διαφορετικά ατομικά και οικογενειακά πλαίσια.

Η ισπανική έρευνα οδήγησε τους εταίρους στην Εθνική Στρατηγική για την Κυβερνοασφάλεια 2019 που δημοσιεύθηκε από το Εθνικό Συμβούλιο Ασφάλειας της ισπανικής κυβέρνησης, η οποία θέτει οδηγίες στο πλαίσιο των γενικών γραμμών δράσης για την αντιμετώπιση της πρόκλησης που αντιπροσωπεύει η ευπάθεια στον κυβερνοχώρο για τη χώρα. Η δεύτερη δημοσίευση στο πλαίσιο της έρευνας είναι η "Ζήσε ένα ασφαλές Διαδίκτυο: It's never too late to enjoy a safer internet" από την Organización de Consumidores y Usuarios (OCU). Περιέχει μια σειρά πρακτικών οδηγών για διάφορα μέλη της κοινωνίας, συμπεριλαμβανομένων των παιδιών, των γονέων, των ενηλίκων και των ηλικιωμένων. Για τους ηλικιωμένους ο οδηγός προσφέρει συστάσεις για να μάθουν να απολαμβάνουν όλα τα πλεονεκτήματα του Διαδικτύου, χωρίς να επηρεάζονται από την ηλικία τους.

Η βρετανική έρευνα επικεντρώθηκε στον εθνικό δικτυακό τόπο συμβουλών και καθοδήγησης του Εθνικού Κέντρου Κυβερνοασφάλειας του Ηνωμένου Βασιλείου. Οι παρεχόμενες πληροφορίες εντάσσονται στο πλαίσιο του ευρύτερου στόχου της προστασίας του Ηνωμένου Βασιλείου και, ως εκ τούτου, απευθύνονται σε όλους τους πολίτες, γεγονός που αντικατοπτρίζεται στο περιεχόμενο. Το δεύτερο έγγραφο είναι η Εθνική Στρατηγική Κυβερνοασφάλειας 2016-2021 της κυβέρνησης του Ηνωμένου Βασιλείου, η οποία παρέχει μια ολοκληρωμένη επισκόπηση των στρατηγικών απειλών για την κυβέρνηση, τις

επιχειρήσεις και το κοινό και, επομένως, ενώ έχει συνάφεια με το έργο DiSC, καλύπτει μόνο οριακά τους τομείς με τους οποίους ασχολείται το παρόν έργο. Ο περιεκτικός κατάλογος των τύπων απειλών είναι εξαιρετικά σχετικός με το πλαίσιο και το έργο στο σύνολό του.

Συνοψίζοντας, η έρευνα γραφείου πληροφόρησε για την ανάπτυξη του πλαισίου, παρουσιάζοντας τα ζητήματα, τις απειλές και την ορολογία που χρησιμοποιούνται σε κάθε εθνικό πλαίσιο. Η παρουσίαση και η ανάλυση των διαφόρων μορφών παροχής πληροφοριών που χρησιμοποιούνται για διαφορετικές ομάδες-στόχους είχε επίσης ισχυρή επίδραση στην κατεύθυνση του πλαισίου ικανοτήτων, καθώς ορισμένη ορολογία και η παρουσίαση των πληροφοριών έχει σημαντική σημασία για τους ηλικιωμένους πολίτες- αυτό αποδεικνύεται σε παρόμοιο υλικό σε εθνικό επίπεδο. Όλες οι χώρες εταίροι παρέχουν κάποιο είδος πληροφοριών στους ηλικιωμένους πολίτες στο εθνικό πλαίσιο, είτε ειδικά είτε στο πλαίσιο μιας ευρύτερης εκστρατείας ευαισθητοποίησης για κοινωνικές ομάδες, και ωστόσο, μόλις ολοκληρωθεί το πλαίσιο θα είναι αυτόνομο όσον αφορά την παροχή ενός συνόλου εφαρμοστέων ικανοτήτων που απαιτούνται για την αύξηση της προσωπικής ικανότητας μετριασμού των απειλών στον κυβερνοχώρο.

Εισαγωγή στο πλαίσιο

Ένα πλαίσιο ικανοτήτων είναι μια αποτελεσματική μέθοδος για την αξιολόγηση, τη διατήρηση και την παρακολούθηση των γνώσεων, των δεξιοτήτων και των χαρακτηριστικών των ομάδων-στόχων σχετικά με την ευαισθητοποίηση, την αντιδραστικότητα και την προδραστικότητα στον κυβερνοχώρο. Το πλαίσιο DiSC σχεδιάστηκε για να βασιστεί στο πλαίσιο ψηφιακής επάρκειας Digcomp, το οποίο δεν καλύπτει ρητά την ασφάλεια από επιθετικές κυβερνοεπιθέσεις, spam και κόλπα απάτης που χρησιμοποιούνται για την κλοπή των δεδομένων και των πληροφοριών των ανθρώπων στο διαδίκτυο.

Γενικότερα, αυτές οι ικανότητες και δεξιότητες βασίζονται στις ενότητες 4.1 και 4.2 του πλαισίου DigComp 2.1:

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

4.2 Προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής - Προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής σε ψηφιακά περιβάλλοντα. Να κατανοήσουν πώς να χρησιμοποιούν και να μοιράζονται προσωπικά αναγνωρίσιμες πληροφορίες, ενώ είναι σε θέση να προστατεύουν τον εαυτό τους και τους άλλους από ζημιές. Να κατανοήσουν ότι οι ψηφιακές υπηρεσίες χρησιμοποιούν μια "πολιτική απορρήτου" για να ενημερώσουν για τον τρόπο χρήσης των προσωπικών δεδομένων.

Η κοινοπραξία του έργου DiSC έχει αναλύσει την 4.1 προστασία των συσκευών και την 4.2 προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής σε πέντε υποενότητες, οι οποίες χρησιμοποιήθηκαν για την ταξινόμηση των σχετικών ικανοτήτων ψηφιακής ασφάλειας:

1. Επίγνωση των απειλών: επίγνωση των διαφόρων τύπων απειλών για την ψηφιακή ασφάλεια.
2. Κατανόηση των απειλών: γνώση των κινδύνων που συνδέονται με τις απειλές της ψηφιακής ασφάλειας.
3. Σχεδιασμός μετριασμού: προετοιμασία κατά.
4. Ανίχνευση απειλών: εφαρμογή κριτικής και αναλυτικής σκέψης σε πιθανές απειλές ψηφιακής ασφάλειας.
5. Αντιμετώπιση απειλών: επίλυση προβλημάτων για την αντιμετώπιση απειλών και παραβιάσεων.

Η καθιέρωση του πλαισίου ικανοτήτων ψηφιακής ασφάλειας θα επιτρέψει στο έργο DiSC να καθορίσει τις γνώσεις και τις δεξιότητες που απαιτούνται για την αντιμετώπιση πιθανών απειλών στον κυβερνοχώρο, να προσδιορίσει συγκεκριμένες ικανότητες στον κυβερνοχώρο, με τη μορφή συνόλων θεμάτων, και να υποστηρίξει την ανάπτυξη και την πρόταση συγκεκριμένων μαθημάτων και ευκαιριών προσωπικής και επαγγελματικής κατάρτισης για τις ομάδες-στόχους με βάση το πλαίσιο.

Οι τελικοί χρήστες του πλαισίου ικανοτήτων είναι οι πολίτες ηλικίας 55+. Το πλαίσιο αναμένεται επίσης να είναι σχετικό και να ενδιαφέρει τους εκπαιδευτικούς ΤΠΕ, εκπαιδευτές και επαγγελματίες που εργάζονται στον τομέα της ανάπτυξης τεχνολογικών ικανοτήτων των ηλικιωμένων πολιτών.

Το πλαίσιο ικανοτήτων ψηφιακής ασφάλειας αποσκοπεί στον καθορισμό των δεξιοτήτων, των γνώσεων και των στάσεων των βασικών ικανοτήτων που απαιτούνται από τους ηλικιωμένους πολίτες για την αποτελεσματική ενσωμάτωση των πρωτοκόλλων ψηφιακής ασφάλειας στα τοπικά τους πλαίσια, καθώς και στην παροχή ενός πλαισίου αναφοράς της ΕΕ για την ανάπτυξη και την αξιολόγηση των ικανοτήτων ψηφιακής ασφάλειας.

Πεδίο

Για τον καθορισμό του πεδίου εφαρμογής του πλαισίου, οι εταίροι προσδιόρισαν τη συσκευή, την προσέγγιση και τις μεθόδους που λαμβάνονται υπόψη κατά την εφαρμογή του πλαισίου ψηφιακής επάρκειας. Αυτό θα βοηθήσει στη διάκριση μεταξύ άλλων τύπων εγκληματικής δραστηριότητας που δεν καλύπτονται από τις ικανότητες του πλαισίου.

Συσκευές: η συσκευή που χρησιμοποιήθηκε για την επαφή με το θύμα

- Κινητά και Smartphones
- Υπολογιστές και laptops
- Tablets

Προσέγγιση: η τεχνική που χρησιμοποιείται για την εξαπάτηση του θύματος

- Phishing: Η εξαπατητική απόπειρα απόκτησης ευαίσθητων πληροφοριών ή δεδομένων, όπως ονόματα χρηστών, κωδικοί πρόσβασης και στοιχεία πιστωτικών καρτών, μεταμφιέζοντας τον εαυτό σας ως αξιόπιστη οντότητα σε μια ηλεκτρονική επικοινωνία.
- Vishing (Voice Phishing): Voice phishing είναι μια μορφή εγκληματικής τηλεφωνικής απάτης, που χρησιμοποιεί την κοινωνική μηχανική μέσω του τηλεφωνικού συστήματος για να αποκτήσει πρόσβαση σε ιδιωτικές προσωπικές και οικονομικές πληροφορίες με σκοπό την οικονομική ανταμοιβή.
- Smishing (SMS Phishing): Δραστηριότητα που επιτρέπει στους εγκληματίες να κλέψουν τα χρήματα ή την ταυτότητα των θυμάτων ή και τα δύο λόγω της απάντησης σε ένα γραπτό μήνυμα. Το Smishing χρησιμοποιεί το κινητό σας τηλέφωνο (είτε ένα smartphone είτε ένα παραδοσιακό μη συνδεδεμένο με το

διαδίκτυο κινητό τηλέφωνο) για να χειραγωγήσει αθώους ανθρώπους ώστε να προβούν σε διάφορες ενέργειες που οδηγούν στην εξαπάτηση.

- Απάτη λογισμικού: Μια δραστηριότητα κατά την οποία ο απατεώνας χρησιμοποιεί ψεύτικο ή αντιγραφικό λογισμικό, όπως μια εφαρμογή ή ένα πρόγραμμα, για να αποκτήσει πρόσβαση στα δεδομένα μιας ψηφιακής συσκευής, τα οποία στη συνέχεια χρησιμοποιεί για να κλέψει τα χρήματα ή την ταυτότητα των θυμάτων.
- Social Engineering: Ένας όρος που χρησιμοποιείται για ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων που επιτυγχάνονται μέσω ανθρώπινων αλληλεπιδράσεων. Χρησιμοποιεί ψυχολογική χειραγώγηση για να εξαπατήσει τους χρήστες ώστε να κάνουν λάθη ασφαλείας ή να δώσουν ευαίσθητες πληροφορίες..

Μέθοδος: η επιδιωκόμενη απάτη

- Απάτη μέσω ηλεκτρονικού ταχυδρομείου Phishing
- Απάτη του πλούσιου "πρίγκιπα"
- Απάτη με ευχετήριες κάρτες
- Απάτη με τραπεζικό δάνειο ή πιστωτική κάρτα
- Απάτη λοταρίας
- Απάτη εκβιασμού
- Ρομαντισμός / απάτη online ραντεβού
- Ψεύτικο λογισμικό προστασίας από ιούς
- Απάτη με πλαστοπροσωπία στο Facebook/κλεμμένο προφίλ
- Απάτη “Βγάλτε λεφτά έυκολα και γρήγορα!”
- Απάτη ταξιδιών
- Απάτες κρυπτονομισμάτων
    - Ψεύτικες συναλλαγές Bitcoin
    - Συστήματα Ponzi
    - Καθημερινές απόπειρες απάτης

- Malware

- Απάτη ψεύτικων νέων
- Ψεύτικες ιστοσελίδες αγορών
- Απάτες προσφοράς εργασίας
- SMS Scamming (Smishing)
- Ηλεκτρονική απάτη υπερπληρωμής
- Ηλεκτρονικές απάτες τεχνικής υποστήριξης

Σημείωση: οι ψηφιακές απειλές αλλάζουν και εξελίσσονται διαρκώς, και λόγω της φύσης τους είναι αδύνατο να καταρτιστεί ένας πλήρης κατάλογος. Για να ενημερώνεστε για τις απειλές, το DiSC συνιστά να εγγραφείτε σε έναν οργανισμό ή δίκτυο κυβερνοασφάλειας, όπως για παράδειγμα η Heimdal Security, η οποία δημοσιεύει τακτικές ενημερώσεις σχετικά με θέματα, προσεγγίσεις και μεθόδους κυβερνοασφάλειας, ή τη σελίδα της Europol για τις περιοχές τάσεων του εγκλήματος.

Πλαίσιο

Θεμελιώδεις δεξιότητες	Επίπεδα επάρκειας		
Περιγραφικοί δείκτες	Στοιχειώδη Το άτομο κατανοεί τη βασική έννοια, τις δεξιότητες και τις απαιτήσεις γνώσεων της ψηφιακής ασφάλειας και είναι προετοιμασμένο να επιτύχει το υψηλότερο	Ενδιάμεση Το άτομο επιδεικνύει κριτική σκέψη σχετικά με την ψηφιακή ασφάλεια, μπορεί να διακρίνει τις ψηφιακές απειλές σε όλες τις συσκευές και είναι σε θέση να σχεδιάζει	Προχωρημένη Το άτομο επιδεικνύει αναλυτική σκέψη όσον αφορά την ψηφιακή ασφάλεια και μπορεί να ανταποκρίνεται σε απειλές σε πραγματικό χρόνο,

	επίπεδο ικανοτήτων για το οποίο είναι ικανό.	ανεξάρτητα και να εκτελεί με επιτυχία ενέργειες μετριασμού για την προστασία από αυτές.	αξιολογώντας και επιλέγοντας την πιο αποτελεσματική αντίδραση σε μια κατάσταση υψηλής πίεσης.

1. Επίγνωση απειλών

Επίγνωση απειλών	Στοιχειώδη	Ενδιάμεση	Προχωρημένη
	Γνωρίζω τις συνήθεις προσεγγίσεις που χρησιμοποιούν οι απειλές για την ψηφιακή ασφάλεια.	Γνωρίζω λιγότερο συνηθισμένες προσεγγίσεις που χρησιμοποιούνται από απειλές ψηφιακής ασφάλειας.	Ενημερώνομαι για τις νέες προσεγγίσεις ψηφιακής ασφάλειας καθώς εξελίσσονται.
	Γνωρίζω τις συνήθεις μεθόδους που χρησιμοποιούνται από απειλές για την ψηφιακή ασφάλεια.	Γνωρίζω τις λιγότερο συνηθισμένες προσεγγίσεις που χρησιμοποιούνται από απειλές ψηφιακής ασφάλειας.	Ενημερώνομαι για τις νέες μεθόδους ψηφιακής ασφάλειας καθώς εξελίσσονται.
	Γνωρίζω τις βασικές δραστηριότητες κοινωνικής μηχανικής στο πλαίσιο της ψηφιακής ασφάλειας.	Γνωρίζω πιο σύνθετες τεχνικές κοινωνικής μηχανικής.	Γνωρίζω διάφορους συνδυασμούς τεχνικών, προσεγγίσεων και μεθόδων κοινωνικής μηχανικής.

2. Κατανόηση απειλών

Κατανόηση απειλών	Στοιχειώδη	Ενδιάμεση	Προχωρημένη
	Κατανοώ τα βασικά χαρακτηριστικά και τις λειτουργίες των συνηθέστερων απειλών ψηφιακής	Κατανοώ τα βασικά χαρακτηριστικά και τις λειτουργίες των πιο σπάνιων και ασυνήθιστων απειλών	Ανανεώνω ενεργά τις γνώσεις μου σχετικά με τις ψηφιακές απειλές μέσω αξιόπιστων,

απειλές. Αξιολόγηση των ψηφιακών απειλών και του επιπέδου κινδύνου τους. Κατανόηση της μεταβαλλόμενης φύσης των ψηφιακών απειλών. Επίγνωση της σημασίας αξιόπιστων, ενημερωμένων και ακριβών πηγών πληροφοριών για την ασφάλεια.	ασφάλειας.	ψηφιακής ασφάλειας.	ενημερωμένων και ακριβών πηγών πληροφοριών ασφαλείας.
	Κατανοώ το επίπεδο κινδύνου και τις πιθανές συνέπειες που συνδέονται με απλές απειλές ψηφιακής ασφάλειας.	Αντιλαμβάνομαι το επίπεδο κινδύνου και τις πιθανές συνέπειες που συνδέονται με τις πολύπλευρες απειλές ψηφιακής ασφάλειας.	Κατανοώ το επίπεδο κινδύνου και τις πιθανές συνέπειες που συνδέονται με τις σύνθετες απειλές ψηφιακής ασφάλειας.

3. Μετριασμός του κινδύνου

Μετριασμός του κινδύνου	Στοιχειώδης	Ενδιάμεσος	Προχωρημένος
	Μπορώ να προσδιορίσω τα κατάλληλα εργαλεία ψηφιακής προστασίας για τον μετριασμό των απειλών ψηφιακής	Μπορώ να χρησιμοποιήσω τις προηγούμενες εμπειρίες και δεξιότητές μου για να ενημερώσω τις αποφάσεις μου σχετικά	Μπορώ να χρησιμοποιήσω την εμπειρία και τις δεξιότητές μου για να αναλύσω τις πιθανές επιπτώσεις των διαφόρων κινδύνων

προστασία από ψηφιακές απειλές. Γνώση και κατανόηση των διαφόρων εργαλείων και πόρων για την προστασία από απειλές.	ασφάλειας.	με την προστασία από απειλές ψηφιακής ασφάλειας.	και να επιλέξω τις κατάλληλες στρατηγικές προστασίας αναλόγως.
	Μπορώ να ακολουθώ βασικές οδηγίες ψηφιακής ασφάλειας για τον μετριασμό των απειλών ψηφιακής ασφάλειας.	Μπορώ να αποφασίσω σχετικά με τα καταλληλότερα βασικά εργαλεία ψηφιακής ασφάλειας για τον μετριασμό των απειλών ψηφιακής ασφάλειας.	Μπορώ να αναλύω και να αξιολογώ τις απειλές ψηφιακής ασφάλειας και να προσαρμόζω τη στρατηγική προστασίας μου ανάλογα με την απειλή ψηφιακής ασφάλειας.
	Γνωρίζω πώς να ρυθμίζω μια ψηφιακή συσκευή ώστε να διασφαλίζω την προστασία από βασικές απειλές ψηφιακής ασφάλειας.	Γνωρίζω πώς να ελέγχω και να ενημερώνω μια ψηφιακή συσκευή για να εξασφαλίσω την κατάλληλη προστασία από τις πιο συνηθισμένες απειλές ψηφιακής ασφάλειας.	Γνωρίζω πώς να εγκαθιστώ εργαλεία και λογισμικό προστασίας σε ψηφιακές συσκευές για τον μετριασμό των ψηφιακών απειλών.

4. Ανίχνευση απειλών

Ανίχνευση απειλών	Στοιχειώδη	Ενδιάμεση	Προχωρημένη
	Μπορώ να αναγνωρίζω και να εντοπίζω τις πιο συνηθισμένες απειλές ψηφιακής	Μπορώ να αναγνωρίζω και να εντοπίζω τις πιο σπάνιες και ασυνήθιστες απειλές	Παραμένω ενεργά ενήμερος για τις απειλές της ψηφιακής ασφάλειας μέσω αξιόπιστων, επικαιροποιημένων και

κινδύνων. Γνώση ώστε να είναι σε θέση να κατηγοριοποιεί τις ψηφιακές απειλές ανάλογα με το επίπεδο κινδύνου.	ασφάλειας για τα προσωπικά μου δεδομένα και πληροφορίες.	ψηφιακής ασφάλειας για τα προσωπικά μου δεδομένα και πληροφορίες.	ακριβών πηγών πληροφόρησης για την ασφάλεια.
	Μπορώ να αναγνωρίζω σαφείς και προφανείς κινδύνους και απειλές σε ψηφιακά περιβάλλοντα.	Μπορώ να αναγνωρίζω σκοτεινές απειλές ψηφιακής ασφάλειας.	Μπορώ να αναγνωρίζω πολύπλοκους κινδύνους και απειλές σε ψηφιακά περιβάλλοντα.
	Μπορώ να χρησιμοποιήσω τις γνώσεις μου για να αξιολογήσω πιθανές απειλές για την ασφάλεια και να αποφασίσω αν είναι ύποπτες.	Μπορώ να χρησιμοποιήσω την αναλυτική μου προσέγγιση στην ψηφιακή ασφάλεια για να αναδείξω τις ψηφιακές απειλές.	Μπορώ να χρησιμοποιώ τις ικανότητές μου κριτικής σκέψης για να αναλύω, να συγκρίνω και να αξιολογώ την έκταση μιας ψηφιακής απειλής και το σχετικό επίπεδο κινδύνου.

5. Αντιμετώπιση απειλών

Αντιμετώπιση απειλών	Στοιχειώδη	Ενδιάμεση	Προχωρημένη
	Είμαι ευέλικτος και καλά προετοιμασμένος για τις απειλές της ψηφιακής ασφάλειας.	Χρησιμοποιώ την προσαρμοστικότητα για την αντιμετώπιση των απειλών ψηφιακής ασφάλειας.	Προβλέπω ενεργά τις απειλές για την ψηφιακή ασφάλεια και τους κινδύνους τους και εξασκώ την προσαρμοστικότητα για την αντιμετώπισή

Ψυχική δύναμη για την αντιμετώπιση της αβεβαιότητας, του άγχους και των δύσκολων καταστάσεων.			τους.
	Παραμένω θετικός όταν αντιμετωπίζω απειλές ή παραβιάσεις της ψηφιακής ασφάλειας.	Μπορώ να χρησιμοποιήσω τις δικές μου εμπειρίες για να προσεγγίσω πιθανές απειλές και παραβιάσεις με αισιοδοξία και αυτοπεποίθηση.	Μπορώ να εξηγήσω πώς η θετική στάση, οι συμπεριφορές και οι ενέργειες απέναντι στην ψηφιακή ασφάλεια συνέβαλαν στην ψηφιακή μου ασφάλεια.
	Μπορώ να αναλογιστώ προηγούμενες συναντήσεις με ψηφιακές απειλές και να αντλήσω διδάγματα από αυτές.	Μπορώ να αναλογιστώ τις προηγούμενες συναντήσεις και να αλλάξω τη συμπεριφορά και τη στάση μου απέναντι στις ψηφιακές απειλές, ώστε να γίνω πιο ανθεκτικός σε αυτές.	Μπορώ να αναλογιστώ τις προηγούμενες συναντήσεις με ψηφιακές απειλές και να αλλάξω τη συμπεριφορά και τη στάση μου στη ζωή, ώστε να γίνω πιο ανθεκτικό άτομο.