TeleGrow
Enhancing the Teleworking Digital Skills for the Middle aged employees

Ενότητες Κατάρτισης «How to TeleGrow»: Η Απόλυτη Κατάρτιση τηλεργασίας για τους παρόχους ΕΕΚ

Ενότητα 6 – Βασικές πληροφορίες για τη διαδικτυακή ασφάλεια

27/6/2022

Erasmus+

Το έργο χρηματοδοτείται από: **Πρόσκληση υποβολής προτάσεων 2020, 1ος Γύρος, ΒΔ2 – Συνεργασία για την καινοτομία και την ανταλλαγή καλών πρακτικών / ΒΔ226 – Συμπράξεις για την Ψηφιακή Εκπαιδευτική Ετοιμότητα**

Περιεχόμενα

1. Εισαγωγή στο θέμα

Σε αυτούς τους δύσκολους καιρούς, όλοι οι άνθρωποι προσπαθούν να προσαρμοστούν στη νέα εποχή της εργασίας από το σπίτι χωρίς την υποχρεωτική γνώση της ποσότητας των κινδύνων και των απειλών που υπάρχουν, όχι μόνο για τα άτομα ηλικίας 50+, στα οποία απευθύνεται το έργο TeleGrow αλλά και σε εργαζόμενους όλων των ηλικιών. Μια έκθεση της Ευρωπαϊκής Επιτροπής για το 2020 αναφέρει ότι περίπου το 40% των εργαζομένων στην ΕΕ έχουν αρχίσει να εργάζονται εξ αποστάσεως μετά την πανδημία COVID-19, δηλαδή σχεδόν 8πλάσια αύξηση σε σύγκριση με το έτος πριν από την έναρξη της πανδημίας. Αυτή η ραγδαία αύξηση της τηλεργασίας δυσκολεύει τις επιχειρήσεις να εφαρμόσουν νέα και ισχυρά μέτρα ασφαλείας, γεγονός που ανοίγει ένα παράθυρο για διάφορες κακόβουλες πρακτικές. Με την αύξηση των δραστηριοτήτων ηλεκτρονικού εγκλήματος κατά πάνω από 600% από την έναρξη της πανδημίας, είναι εύκολο να συμπεράνει κανείς ότι τα άτομα ηλικίας 50+ που έχουν ελάχιστη έως καθόλου εμπειρία με την τηλεργασία είναι ιδιαίτερα ευάλωτα στους κινδύνους που μπορεί να επιφέρει. Οι κίνδυνοι αυτοί αφορούν πράγματα όπως κλοπή ταυτότητας, παραβιάσεις δεδομένων, κακόβουλο λογισμικό (malware) και ιούς, τραπεζικές απάτες και πολλές ακόμη απειλές για τις οποίες τα άτομα μεγαλύτερης ηλικίας μπορεί να μην είναι καλά προετοιμασμένα.

Αυτή η ενότητα έχει σχεδιαστεί για να λειτουργήσει ως μια σύντομη εισαγωγή στο θέμα της διαδικτυακής ασφάλειας. Θα περιλαμβάνει περιγραφές των πιο συνηθισμένων κινδύνων της τηλεργασίας και της γενικής χρήσης του Διαδικτύου που μπορεί να αντιμετωπίσουν οι ομάδες-στόχοι του έργου TeleGrow. Αυτό το μέρος της ενότητας θα βοηθήσει στην κατανόηση του τι είναι το spam και το phishing, πώς να τα αναγνωρίζετε και ποιους κινδύνους μπορεί να επιφέρουν. Άλλες κοινές πρακτικές, όπως η πειρατεία, το ransomware ή η κλοπή ταυτότητας, θα εξεταστούν επίσης διεξοδικά και θα εξηγηθούν. Η ενότητα θα εξηγήσει επίσης ποια μέτρα πρέπει να λαμβάνονται για την ασφάλεια της ιδιωτικής σύνδεσης στο Διαδίκτυο και θα εξοικειώσει τον εκπαιδευόμενο με τον Γενικό Κανονισμό για την Προστασία

Δεδομένων. Τέλος, αυτή η ενότητα του έργου TeleGrow θα περιλαμβάνει επίσης ένα σύντομο σύνολο ασκήσεων για τους εκπαιδευόμενους, ώστε να ελέγξουν τις γνώσεις που απέκτησαν κατά τη διάρκεια αυτής της ενότητας.

2. Μαθησιακοί στόχοι

Με την ολοκλήρωση αυτής της ενότητας, ο εκπαιδευόμενος θα είναι σε θέση:

- να γνωρίζει για το spam και το phishing και πώς να τα αναγνωρίζει,
- να κατανοήσει τι είναι το hacking, πώς λειτουργεί το ransomware και πώς να προστατευτεί από την κλοπή ταυτότητας και τις συνέπειες που αυτή συνεπάγεται,
- να γνωρίζει ποια μέτρα πρέπει να λάβει για να ασφαλίσει τη σύνδεσή του στο διαδίκτυο και ποια είναι η διαφορά μεταξύ ενός αδύναμου και ενός ισχυρού κωδικού πρόσβασης,
- να αποκτήσει γνώσεις σχετικά με τον Γενικό Κανονισμό Προστασίας Δεδομένων και τους τρόπους προστασίας των προσωπικών πληροφοριών,
- να δημιουργήσει ένα ασφαλές περιβάλλον εργασίας από το σπίτι με τη χρήση πρακτικής δραστηριότητας στο τέλος της ενότητας.

3. Μαθησιακό περιεχόμενο

Κεφάλαιο 1 – Spam και Phishing

Η λέξη "spam" αναφέρεται σε κάθε ανεπιθύμητο ψηφιακό μήνυμα που λαμβάνουν οι άνθρωποι και το οποίο έχει σταλεί σε μια μεγάλη ομάδα παραληπτών. Αυτή η διαδικασία γίνεται πιο συχνά από πράγματα που ονομάζονται "spambots", τα οποία είναι αυτοματοποιημένα προγράμματα που χρησιμοποιούνται για την αποστολή μηνυμάτων spam σε λογαριασμούς ηλεκτρονικού ταχυδρομείου, ιστότοπους κοινωνικής δικτύωσης ή φόρουμ.

Παρόλο που τα ανεπιθύμητα μηνύματα μπορεί να φαίνονται σαν ένα σχετικά νέο πρόβλημα, η ιστορία του χρονολογείται από το 1978, όταν ο Gary Thuerk θέλησε να προωθήσει το προϊόν του στέλνοντας ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου σε χιλιάδες ανθρώπους, τα οποία υποτίθεται ότι απέφεραν περίπου 12 εκατομμύρια δολάρια σε έσοδα. Σήμερα η χρήση των μηνυμάτων spam παραμένει ως επί το πλείστον η ίδια, καθώς χρησιμοποιείται για τη δημιουργία κέρδους από την προώθηση κάποιου προϊόντος.

Γενικά, τα προϊόντα που διαφημίζονται είναι αμφιβόλου ποιότητας, όπως και τα θέματα που τις περισσότερες φορές περιέχουν τέτοιου είδους μηνύματα, τα οποία είναι:

- φαρμακευτικά
- περιεχόμενο για ενηλίκους
- οικονομικές υπηρεσίες
- διαδικτυακός στοιχηματισμός

- κρυπτονομίσματα

Πηγή: freepik.com

Το 2020, περίπου το 50% του συνόλου των ληφθέντων ηλεκτρονικών μηνυμάτων ήταν ανεπιθύμητα μηνύματα. Τα άτομα που δημιουργούν και στέλνουν μηνύματα spam εκμεταλλεύονται τους άπειρους χρήστες του Διαδικτύου και το άνοιγμα τέτοιων μηνυμάτων μπορεί να έχει πολύ δυσάρεστες συνέπειες, όπως η κοινοποίηση προσωπικών πληροφοριών σε μη εξουσιοδοτημένα άτομα ή αυτές να καταλήγουν στις λίστες αλληλογραφίας διαφόρων πωλητών, γεγονός που θα οδηγήσει σε ακόμη περισσότερα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που θα συσσωρεύονται στο γραμματοκιβώτιο κάποιου.

Παρόλο που οι αριθμοί μπορεί να φαίνονται συντριπτικοί, οι άνθρωποι σπάνια βλέπουν πλέον μηνύματα spam στα γραμματοκιβώτιά τους. Αυτό οφείλεται στη ραγδαία ανάπτυξη που παρατηρείται στον τομέα του φιλτραρίσματος των ανεπιθύμητων μηνυμάτων. Τα στατιστικά στοιχεία που αποκάλυψε η Google τον Απρίλιο του 2020 έδειξαν ότι κατάφερε να αποκλείσει και να φιλτράρει με επιτυχία το 99,9% των μηνυμάτων spam. Αυτό σημαίνει ότι οι σημερινοί χρήστες του Διαδικτύου, μαζί με τους ανθρώπους ηλικίας 50 ετών και άνω, είναι πολύ πιο ασφαλείς από τη λήψη τέτοιου είδους μηνυμάτων.

Αυτό δε σημαίνει, βέβαια, ότι το φιλτράρισμα λειτουργεί άψογα, καθώς εξακολουθούν να υπάρχουν και να περνούν μηνύματα spam. Για να μπορούν να τα φιλτράρουν από μόνοι τους, οι χρήστες του Διαδικτύου θα πρέπει να γνωρίζουν τι

είδους μήνυμα πρέπει να αποφεύγουν να ανοίγουν. Μερικοί από τους πιο συνηθισμένους τύπους ανεπιθύμητης αλληλογραφίας είναι:

- Πλαστογράφηση ηλεκτρονικού ταχυδρομείου (email)

Αυτού του είδους τα μηνύματα προσπαθούν να μιμηθούν τον αποστολέα πλαστογραφώντας το ίδιο ακριβώς email και εξαπατούν τον παραλήπτη ώστε να νομίζει ότι το μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από ένα άτομο ή έναν ιστότοπο που μπορεί να εμπιστευτεί. Συχνά ζητούν από κάποιον να προβεί σε κάποιου είδους ενέργεια, η οποία μπορεί να είναι είτε αίτημα πληρωμής ενός ανεξόφλητου τιμολογίου, είτε επικύρωση/απεμπλοκή ενός λογαριασμού, είτε επαλήθευση μιας αγοράς, και παρέχουν έναν σύνδεσμο ο οποίος, μόλις πατηθεί, μπορεί να χρησιμοποιηθεί για την κλοπή των προσωπικών στοιχείων του παραλήπτη. Ευτυχώς, πολλοί πάροχοι ηλεκτρονικού ταχυδρομείου προειδοποιούν εκ των προτέρων τον χρήστη για τον κίνδυνο "πλαστογράφησης".

- Απάτες με προκαταβολή αμοιβής

Μερικές φορές αναφέρεται ως "απάτη του Νιγηριανού πρίγκιπα", μια από τις ιδέες πίσω από αυτή είναι ότι ο αποστολέας υπόσχεται ένα μεγάλο χρηματικό ποσό, αλλά μόνο αν ο παραλήπτης παρέχει ένα μικρό δάνειο εκ των προτέρων. Αυτό το δάνειο συνήθως λέγεται ότι απαιτείται για κάποιο νομικό θέμα που θα ξεκλειδώσει το μεγαλύτερο ποσό. Ο άλλος τύπος απάτης με προκαταβολικά τέλη λειτουργεί με παρόμοιο τρόπο, αλλά σε αυτή την περίπτωση, ο αποστολέας παριστάνει τον στενό φίλο ή το μέλος της οικογένειας του παραλήπτη που χρειάζεται χρήματα λόγω κάποιου είδους έκτακτης ανάγκης.

- Διαφημίσεις και κακόβουλο λογισμικό spam

Το διαφημιστικό spam είναι απλώς ένα ανεπιθύμητο μήνυμα που προσφέρει κάποιου είδους προϊόν. Ενώ αυτές οι προσφορές μπορεί μερικές φορές να είναι αληθινές, σε πολλές περιπτώσεις, το προϊόν είτε δεν υπάρχει είτε δε λειτουργεί. Το κακόβουλο λογισμικό spam είναι ένας τύπος μηνύματος που περιέχει διάφορα είδη κακόβουλου περιεχομένου που κρύβεται πίσω από συνδέσμους ή συνημμένα αρχεία που παρέχονται στο μήνυμα. Μόλις το

άτομο κατεβάσει και ανοίξει το αρχείο που επισυνάπτεται ή κατεβαίνει μέσω του συνδέσμου, τα κακόβουλα σενάρια θα εκτελεστούν και θα μολύνουν τον υπολογιστή με διάφορους τύπους επικίνδυνων κακόβουλων λογισμικών.

- Ηλεκτρονικό ψάρεμα (Phishing)

Πηγή: freepik.com

Παρόμοιο με την πλαστογράφηση ηλεκτρονικού ταχυδρομείου αλλά πιο σύνθετο ως έγκλημα στον κυβερνοχώρο είναι το phishing. Αυτή η κακόβουλη πρακτική χρησιμοποιείται στο πλαίσιο της απάτης, της κατασκοπείας ή για τη δημιουργία κυβερνοεπιθέσεων με στόχο διάφορους οργανισμούς. Περιλαμβάνει πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές κλήσεις και ισχυρίζεται ότι προέρχεται από νόμιμη πηγή για να πείσει τα άτομα να αποκαλύψουν τις προσωπικές ή οικονομικές τους πληροφορίες, συχνά χωρίς συγκεκριμένο στόχο. Τα μηνύματα spear phishing αποστέλλονται επίσης από πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνονται αξιόπιστα, αλλά σε αυτή την περίπτωση, ο εγκληματίας του διαδικτύου συλλέγει πληροφορίες για το θύμα από διάφορες πηγές, όπως δημόσιες αναρτήσεις στα μέσα κοινωνικής δικτύωσης, ιστότοπους στους οποίους είναι καταχωρημένο το ηλεκτρονικό ταχυδρομείο του θύματος, προφίλ φίλων του θύματος στα μέσα κοινωνικής δικτύωσης ή πληροφορίες για τους υπαλλήλους στον ιστότοπο της εταιρείας.

Ο χάκερ μπορεί στη συνέχεια να συγκεντρώσει όλες τις πληροφορίες για το συγκεκριμένο άτομο και να προετοιμάσει ένα εξατομικευμένο μήνυμα, στο οποίο ο παραλήπτης μπορεί να πέσει θύμα. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν συχνά κακόβουλους συνδέσμους, αλλά μπορούν επίσης να χρησιμοποιηθούν για να δημιουργηθεί μια σύνδεση μεταξύ του εγκληματία και του θύματος για να κερδίσει ο πρώτος την εμπιστοσύνη του δεύτερου και να κλέψει ευαίσθητες πληροφορίες του. Μερικές φορές, οι επιθέσεις spear phishing στοχεύουν σε τυχόν ανώτερα στελέχη μιας εταιρείας για να τα εξαπατήσουν ώστε να αποκαλύψουν τις προσωπικές τους πληροφορίες ή πολύτιμα δεδομένα της εταιρείας, τα οποία μπορούν αργότερα να χρησιμοποιηθούν για κακόβουλους σκοπούς. Για να είναι λιγότερο επιρρεπείς στο να πέσουν θύμα απόπειρας phishing, οι χρήστες του Διαδικτύου θα πρέπει να δίνουν ιδιαίτερη προσοχή και να αποφεύγουν να ανοίγουν:

- Ηλεκτρονικά μηνύματα σχετικά με την κατάκτηση ενός μεγάλου βραβείου
- Ψεύτικοι ιστότοποι που μοιάζουν πολύ με τους αυθεντικούς
- Απειλές σχετικά με την απενεργοποίηση λογαριασμού ή την απώλεια πρόσβασης σε αυτόν
- Μηνύματα σχετικά με ψεύτικη μόλυνση από κακόβουλο λογισμικό
- Μηνύματα ηλεκτρονικού ταχυδρομείου με θέμα την COVID-19
- Προσποιητοί συγγενείς που ζητούν χρήματα
- Κακή γραμματική και ορθογραφικά λάθη σε δήθεν επίσημα μηνύματα ηλεκτρονικού ταχυδρομείου.

Παρόλο που τα φίλτρα για κακόβουλο περιεχόμενο που παρέχουν οι περισσότεροι πάροχοι ηλεκτρονικού ταχυδρομείου προσφέρουν ισχυρή προστασία από το spam και το phishing, οι χρήστες θα πρέπει να έχουν κατά νου ότι δεν είναι όλα άψογα και ότι υπάρχουν ορισμένα αντίμετρα που μπορούν να λάβουν για να μειώσουν ακόμη περισσότερο τις πιθανότητες να κλαπούν τα προσωπικά τους δεδομένα. Για να το πετύχουν περαιτέρω αυτό, θα πρέπει πάντα να αντιγράφουν και να επικολλούν το περιεχόμενο ενός ύποπτου μηνύματος στη μηχανή αναζήτησης (π.χ. Google), καθώς υπάρχει πιθανότητα να έχει αναφερθεί ως απόπειρα ηλεκτρονικού ψαρέματος στο

παρελθόν. Μια άλλη καλή πρακτική είναι να επικοινωνήσετε με την εταιρεία που υποτίθεται ότι έστειλε το ύποπτο μήνυμα χωρίς να κάνετε κλικ στους συνδέσμους ή τα συνημμένα αρχεία που υπήρχαν μέσα σε αυτό. Μια επίσης καλή ιδέα θα ήταν επίσης να εγκαταστήσετε φίλτρα ανεπιθύμητης αλληλογραφίας και γραμμές εργαλείων κατά του phishing σε έναν υπολογιστή, καθώς αυτά τα εργαλεία μπορούν να προστατεύσουν τον χρήστη από τέτοια μηνύματα από μόνα τους. Σε ένα εργασιακό περιβάλλον, οι εργαζόμενοι θα πρέπει να προσπαθούν να επιβεβαιώνουν προφορικά κάθε αίτημα που τους αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου και να αλλάζουν τακτικά τους κωδικούς πρόσβασής τους.

Κεφάλαιο 2 – Ηλεκτρονική πειρατεία (Hacking), Λυτρισμικό (Ransomware), Κλοπή ταυτότητας (Identity theft)

Λόγω της πρόσφατης αύξησης της τηλεργασίας και της ανάγκης να μένουμε στο σπίτι και να διεκπεραιώνουμε πολλές δουλειές στο διαδίκτυο λόγω της πανδημίας COVID-19, ο κόσμος παρακολουθεί επίσης μια τεράστια αύξηση των εγκλημάτων στον κυβερνοχώρο. Αυτά μπορούν να οριστούν ως κάθε παράνομη δραστηριότητα που γίνεται με τη χρήση υπολογιστή και συχνά συνδέονται με άτομα που ονομάζονται "χάκερ" ή "κυβερνοεγκληματίες", οι οποίοι μπορούν να χωριστούν σε πολλές διαφορετικές κατηγορίες ανάλογα με το τι θέλουν να επιτύχουν και πόσο εξειδικευμένοι είναι.

Πηγή: freepik.com

Η **ηλεκτρονική πειρατεία (hacking)** είναι η διαδικασία εντοπισμού κενών ασφαλείας σε ένα σύστημα ή δίκτυο υπολογιστών με σκοπό την απόκτηση πρόσβασης σε προσωπικά ή επιχειρηματικά δεδομένα. Η χρήση ενός αλγορίθμου αποκρυπτογράφησης κωδικού πρόσβασης για την απόκτηση πρόσβασης σε ένα σύστημα υπολογιστή αποτελεί παράδειγμα hacking υπολογιστών. Αν και συχνά θεωρείται κακόβουλη πρακτική, μερικές φορές είναι νόμιμη και χρησιμοποιείται με

καλές προθέσεις, κυρίως για τη βελτίωση της διαδικτυακής ασφάλειας και την εξασφάλιση πολύτιμων δεδομένων στο εσωτερικό ενός συγκεκριμένου οργανισμού. Μια τέτοια πρακτική ονομάζεται "ηθική ηλεκτρονική πειρατεία" ("ethical hacking"). Το συνηθισμένο hacking καλύπτει ένα ευρύ φάσμα κακόβουλων πρακτικών, ξεκινώντας από την επιβράδυνση των υπολογιστών άλλων ατόμων, μέσω της κλοπής πληροφοριών πιστωτικών καρτών, και καταλήγοντας σε εκφοβισμό μεγάλης κλίμακας και απαιτήσεις λύτρων. Όπως αναφέρθηκε στο Κεφάλαιο 1, οι χάκερ μπορούν να αποκτήσουν πρόσβαση στις συσκευές άλλων ανθρώπων μέσω προσπαθειών phishing και κακόβουλου λογισμικού που περιέχεται σε ύποπτα μηνύματα spam, αλλά αυτές δεν είναι οι μόνες μέθοδοι που χρησιμοποιούν. Μια κοινή τεχνική hacking στην οποία πολλοί άνθρωποι μπορεί να είναι επιρρεπείς είναι η δημιουργία ενός ψεύτικου σημείου πρόσβασης Wi-Fi σε δημόσιο χώρο, το οποίο μόλις συνδεθεί, θα ανακατευθύνει το θύμα σ' έναν ιστότοπο που μπορεί να κλέψει τις προσωπικές του πληροφορίες. Για να αποφευχθεί αυτό το ενδεχόμενο, οι άνθρωποι θα πρέπει να αποφεύγουν τη χρήση δημόσιων δικτύων Wi-Fi και να είναι πάντα προσεκτικοί όταν χρησιμοποιούν τις συσκευές τους σε χώρους όπως εστιατόρια, αεροδρόμια, εμπορικά κέντρα ή πάρκα.

Μια άλλη μορφή κακόβουλου λογισμικού που μπορεί να είναι πολύ επικίνδυνη για τα άτομα ηλικίας 50 ετών και άνω που μόλις αρχίζουν την τηλεργασία είναι το λυτρισμικό (ransomware). Έχει αποδειχθεί πολύ επικίνδυνο, καθώς όχι μόνο αποτελεί ένα από τα πιο ανησυχητικά προβλήματα ασφάλειας στο Διαδίκτυο σήμερα, αλλά είναι και πολύ διαδεδομένο. Αυτό το κακόβουλο λογισμικό κρυπτογραφεί αρχεία και έγγραφα σε οτιδήποτε, από έναν μεμονωμένο υπολογιστή έως ένα ολόκληρο δίκτυο, συμπεριλαμβανομένων των διακομιστών. Μετά την επίθεση ransomware, το θύμα αφήνεται με οδηγίες για την καταβολή λύτρων για το ξεκλείδωμα των αρχείων, διαφορετικά, τα πολύτιμα δεδομένα θα δημοσιοποιηθούν ή θα πωληθούν σε άλλους εγκληματίες του κυβερνοχώρου, εξ ου και η ονομασία "λυτρισμικό".

Αυτό και άλλα κακόβουλα προγράμματα εξαπλώνονται συνήθως μέσω συνημμένων σε μηνύματα spam phishing, γι' αυτό και είναι κρίσιμο να αντιμετωπίζετε κάθε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου με εξαιρετική προσοχή. Οι επιθέσεις ransomware είναι εξαιρετικά επικίνδυνες, διότι, εάν είναι επιτυχείς, μπορούν να εκθέσουν πολύτιμες, ιδιωτικές πληροφορίες χιλιάδων εργαζομένων, εάν στοχεύουν σε μια συγκεκριμένη εταιρεία.

Πηγή: freepik.com

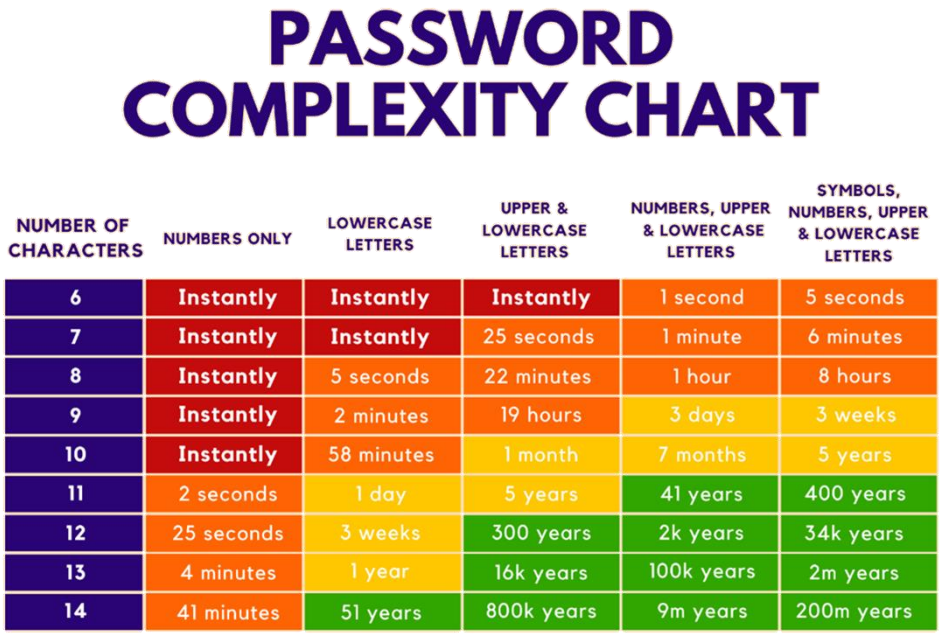
Μία από τις ταχύτερα αναπτυσσόμενες μορφές εγκλήματος στον κυβερνοχώρο είναι η κλοπή ταυτότητας (identity theft). Ο εγκληματίας κλέβει προσωπικά δεδομένα, όπως διαπιστευτήρια, στοιχεία τραπεζικού λογαριασμού, ημερομηνίες γέννησης κ.λπ. προκειμένου να υποδυθεί το θύμα και να χρησιμοποιήσει τις πληροφορίες αυτές για να αποκομίσει χρηματικό κέρδος και να προκαλέσει περαιτέρω ζημιά στους ανθρώπους. Οι μέθοδοι που χρησιμοποιούν οι χάκερ για να το κάνουν αυτό είναι παρόμοιες με άλλα εγκλήματα στον κυβερνοχώρο. Μπορούν να αποκτήσουν αυτά τα πολύτιμα δεδομένα μέσω προσπαθειών "ηλεκτρονικού ψαρέματος" (phishing) ή παραβιάζοντας υπολογιστές χρησιμοποιώντας διάφορα κακόβουλα προγράμματα και ψεύτικα ή κακώς ασφαλισμένα δημόσια σημεία πρόσβασης Wi-Fi. Αργότερα, μπορούν να χρησιμοποιήσουν τα δεδομένα για να λάβουν δάνεια, να αγοράσουν διάφορα πράγματα ή ακόμη και να διαπράξουν εγκλήματα στο όνομα του θύματος.

Είναι καλό να ελέγχετε τακτικά τις πιστωτικές αναφορές και να αναζητάτε τυχόν ανακρίβειες ή τραπεζικές μεταφορές που μπορεί να φαίνονται ύποπτες. Το ποσό των χρημάτων που λείπει δεν είναι απαραίτητο να είναι μεγάλο, επειδή ο κλέφτης μπορεί να κλέβει από χιλιάδες ανθρώπους ταυτόχρονα. Τα θύματα κλοπής ταυτότητας θα πρέπει, το συντομότερο δυνατό, να καταγγείλουν το έγκλημα αυτό στις αρχές, να παγώσουν τους τραπεζικούς τους λογαριασμούς και να ανοίξουν νέους. Εάν είναι δυνατόν, τα θύματα θα πρέπει να επικοινωνήσουν με τράπεζες, εισπρακτικές εταιρείες και άλλα μέρη που γνωρίζουν ότι ο κλέφτης χρησιμοποίησε τα προσωπικά τους στοιχεία. Είναι επίσης σημαντικό να έρθουν σε επαφή με συγγενείς, εργοδότες και συναδέλφους από την εταιρεία που εργάζονται σήμερα, επειδή ο κλέφτης μπορεί να έχει στην κατοχή του και τις δικές τους πληροφορίες.

Οι τεχνικές που χρησιμοποιούν οι χάκερ για να κλέψουν ή να προκαλέσουν χάος στη ζωή των ανθρώπων γίνονται όλο και πιο εξελιγμένες. Έχοντας αυτό κατά νου, οι άνθρωποι πρέπει να γνωρίζουν πώς να προστατεύονται για να ελαχιστοποιήσουν τις πιθανότητες να είναι ένα από τα θύματα των εγκλημάτων στον κυβερνοχώρο. Υπάρχει ένα συγκεκριμένο προστατευτικό αντίμετρο το οποίο, μόλις εφαρμοστεί, μειώνει τον κίνδυνο αντιμετώπισης των εγκληματιών του διαδικτύου.

Δημιουργήστε έναν ισχυρό κωδικό πρόσβασης. Αυτό είναι ζωτικής σημασίας για την ασφάλεια των πολύτιμων δεδομένων. Ένας καλός κωδικός πρόσβασης δεν είναι προφανής, αλλά είναι εύκολο να τον θυμάστε. Δε θα πρέπει να είναι μικρότερος από 12 χαρακτήρες, διότι με τη σημερινή τεχνολογία χρειάζονται δευτερόλεπτα για να σπάσουν οι σύντομοι κωδικοί πρόσβασης. Ένας ισχυρός κωδικός πρόσβασης θα πρέπει να περιλαμβάνει μοναδικά σύμβολα, όπως αριθμούς και πεζά ή κεφαλαία γράμματα, καθώς αυτό θα του προσθέσει ένα επιπλέον επίπεδο ασφάλειας. Είναι σημαντικό να είναι ισχυρός και να είναι δύσκολο να ξεχαστεί. Μια κοινή τεχνική για τη δημιουργία ισχυρών κωδικών πρόσβασης είναι η δημιουργία ενός ακρωνύμιου από ένα αγαπημένο απόσπασμα ή μια φράση που είναι αξιομνημόνευτη και η προσθήκη μερικών ειδικών συμβόλων σε αυτό. Μια άλλη καλή πρακτική είναι η χρήση διαχειριστών κωδικών πρόσβασης. Τα προγράμματα αυτά δημιουργούν και αποθηκεύουν τους κωδικούς πρόσβασης ενός χρήστη σε έναν ασφαλή

κρυπτογραφημένο λογαριασμό. Κάτι ακόμα σημαντικό είναι να κρατάτε τους κωδικούς πρόσβασης ιδιωτικούς και να μην τους στέλνετε ποτέ σε κανέναν μέσω ηλεκτρονικού ταχυδρομείου ή γραπτού μηνύματος. Με τα δεδομένα που συγκεντρώθηκαν, παρουσιάζεται το παρακάτω διάγραμμα που δείχνει πόσο εύκολο είναι για έναν χάκερ να σπάσει έναν κωδικό πρόσβασης που μπορεί να φαίνεται πολύπλοκος για τον χρήστη του.



NUMBER OF CHARACTERS	NUMBERS ONLY	LOWERCASE LETTERS	UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS	SYMBOLS, NUMBERS, UPPER & LOWERCASE LETTERS
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years

Τα δεδομένα συλλέχθηκαν από: https://www.security.org/how-secure-is-my-password/

Από τα δεδομένα που συγκεντρώθηκαν, είναι εύκολο να επιβεβαιωθεί αυτό που αναφέρθηκε προηγουμένως. Ο κωδικός πρόσβασης μήκους 12 χαρακτήρων θα πρέπει να είναι το ελάχιστο για τη βέλτιστη ασφάλεια και δεν χρειάζεται καν να είναι πραγματικά πολύπλοκος. Για να είναι απαραβίαστος για τουλάχιστον 300 χρόνια, αρκεί ένας κωδικός πρόσβασης με πεζά και κεφαλαία γράμματα. Θα πρέπει να σημειωθεί ότι **αντιπροτείνεται αυστηρά το να βάλετε το δικό σας όνομα ως κωδικό πρόσβασης**, καθώς μπορεί να σπάσει εύκολα, ανεξάρτητα από το μήκος του.

Κεφάλαιο 3 – Ασφαλής σύνδεση στο Διαδίκτυο

Είναι γνωστό ότι το διαδίκτυο είναι μια αξιόπιστη αλλά επικίνδυνη πηγή πληροφοριών και ψυχαγωγίας. Λόγω του πλήθους των κακόβουλων προγραμμάτων, των κατασκόπων και των χάκερ που περιμένουν μια καλή ευκαιρία για να επιτεθούν, είναι ζωτικής σημασίας να γνωρίζετε πώς να αμύνεστε εναντίον τους, επειδή μερικές φορές ένας καλός κωδικός πρόσβασης δεν είναι αρκετός. Υπάρχουν πολλοί τρόποι που μπορούν να ενισχύσουν την ασφάλεια μιας σύνδεσης στο διαδίκτυο και πολλοί από αυτούς δεν απαιτούν προηγμένες τεχνολογικές γνώσεις.

Κατ' αρχάς, θα ήταν σκόπιμο να εφαρμόζετε **έλεγχο ταυτότητας δύο παραγόντων (two-factor authentication - 2FA)**, όποτε αυτό είναι δυνατό. Αυτό από μόνο του μπορεί να αποτρέψει τους περισσότερους χάκερ από το να παραβιάσουν το λογαριασμό κάποιου. Λειτουργεί ως δεύτερο επίπεδο επαλήθευσης κατά την είσοδο σε έναν λογαριασμό. Ενώ το ένα είναι συνήθως ένας κωδικός πρόσβασης, το δεύτερο είναι συχνά ένα μοναδικό κλειδί που αποστέλλεται στον αριθμό κινητού τηλεφώνου του χρήστη και το οποίο πρέπει να εισαχθεί μετά την είσοδο με κωδικό πρόσβασης. Θεωρείται μια πραγματικά ισχυρή μέθοδος προστασίας των χρηστών από τον κίνδυνο κλοπής των κωδικών τους, καθώς η μοναδικότητα του κλειδιού καθιστά πολύ πιο δύσκολο για έναν χάκερ να εισχωρήσει σε έναν λογαριασμό.

Μια άλλη καλή πρακτική είναι η χρήση ενός **Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network - VPN)**. Κάθε φορά που κάποιος συνδέεται σε ένα δίκτυο, μια ροή δεδομένων ανταλλάσσεται μεταξύ του χρήστη και των διακομιστών. Το VPN δημιουργεί μια ασφαλή σύνδεση μεταξύ αυτών των δύο μερών, κρυπτογραφώντας τα δεδομένα πριν από την αποστολή ή τη λήψη τους από τους χρήστες. Ένα VPN αποκρύπτει τη διεύθυνση IP και την τοποθεσία του χρήστη, ώστε οι εγκληματίες του διαδικτύου να μην μπορούν πλέον να ανακαλύψουν τις τοποθεσίες των δυνητικών θυμάτων τους, διότι, χάρη στο VPN, θα τους εντοπίσουν στη θέση του διακομιστή αυτού, καθιστώντας πολύ πιο δύσκολο να αποκτήσουν πρόσβαση στα δεδομένα τους. Είναι ένα εξαιρετικό εργαλείο για την ασφάλεια της σύνδεσης κατά τη χρήση

δημόσιων δικτύων Wi-Fi σε μέρη όπως αεροδρόμια ή εστιατόρια που είναι εύκολα παραβιάσιμα.

Πηγή: freepik.com

Για τη δημιουργία αυτού του είδους σύνδεσης είναι απαραίτητο να βρείτε έναν αξιόπιστο πάροχο υπηρεσιών VPN και να εγγραφείτε σε αυτόν. Υπάρχουν μερικοί πάροχοι στην αγορά που προσφέρουν τις υπηρεσίες τους δωρεάν, αλλά συνιστάται η απόκτηση συνδρομής επί πληρωμή, καθώς προσφέρει περισσότερες δυνατότητες για ασφαλέστερη σύνδεση. Μόλις βρεθεί ένας προτιμώμενος πάροχος VPN, ο χρήστης θα κληθεί να κατεβάσει το απαραίτητο λογισμικό. Πρέπει πάντα να γίνεται λήψη απευθείας από τον ιστότοπο του παρόχου, καθώς η λήψη από διαφορετική πηγή μπορεί να έχει ως αποτέλεσμα τη λήψη αρχείων που περιέχουν κακόβουλο λογισμικό. Οι περισσότερες εφαρμογές VPN είναι διαθέσιμες σε μια τεράστια ποικιλία συσκευών και η διαδικασία ρύθμισής τους είναι προσβάσιμη για όλους. Μόλις γίνει λήψη μιας εφαρμογής και δημιουργηθεί ο λογαριασμός, το μόνο που μένει να κάνουμε είναι να την ενεργοποιήσουμε και να ανησυχούμε λιγότερο μήπως κάποιος εισβάλει στη συσκευή μας.

Η αλλαγή του προεπιλεγμένου ονόματος και του κωδικού πρόσβασης του δρομολογητή (router) μπορεί επίσης να βοηθήσει στην προστασία του δικτύου. Κάθε

δρομολογητής συνοδεύεται από ένα γενικό όνομα και έναν κωδικό πρόσβασης, τα οποία απαιτούνται για την πρώτη εγκατάσταση. Αμέσως μετά, μια καλή πρακτική είναι να αλλάξετε το όνομα και τον κωδικό πρόσβασής του σε κάτι μοναδικό, λαμβάνοντας υπόψη τις οδηγίες για τη δημιουργία ενός ισχυρού κωδικού πρόσβασης. Αυτό συμβαίνει, επειδή τα ονόματα των δρομολογητών (SSID - Service Set IDdentifier) τις περισσότερες φορές περιέχουν στο όνομά τους τη μάρκα και το μοντέλο, γεγονός που διευκολύνει τους χάκερ να βρίσκουν αυτούς για τους οποίους γνωρίζουν ότι είναι ευάλωτοι σε παραβιάσεις. Είναι επίσης δυνατό να αποκρύψετε εντελώς το SSID ενός δρομολογητή, έτσι ώστε οι πιθανότητες να ανακαλύψει ένας χάκερ τη σύνδεση να είναι σχεδόν μηδενικές.

Πηγή: freepik.com

Κρατήστε τα πάντα ενημερωμένα. Η ενημέρωση συνήθως φαίνεται σαν μια περιττή ταλαιπωρία και μερικές φορές μπορεί να κάνει μια συσκευή να λειτουργεί χειρότερα από πριν, προσθέτοντας νέες λειτουργίες που δε χρειάζονται ή αφαιρώντας αυτές που ήταν χρήσιμες. Είναι σημαντικό να δίνετε προσοχή σε τυχόν ειδοποιήσεις ενημέρωσης που μπορεί να εμφανιστούν. Κάθε λογισμικό δεν είναι χωρίς ελαττώματα. Τα περισσότερα από αυτά περιέχουν κρυφά τρωτά σημεία που ούτε οι προγραμματιστές δε γνώριζαν στην αρχή. Μόλις βρεθούν, αυτές μπορούν να αξιοποιηθούν από χάκερς. Αυτός είναι και ο λόγος για τον οποίο κάθε λογισμικό χρειάζεται τις νεότερες εκδόσεις του που έχουν διορθώσεις στα ευάλωτα σημεία.

Αυτό είναι πολύ σημαντικό από την άποψη της διαδικτυακής ασφάλειας, καθώς η διατήρηση των πάντων ενημερωμένων μειώνει επίσης τις πιθανότητες μιας επιτυχημένης επίθεσης χάκερ. Οι χρήστες που παρακολουθούν τακτικά την ενημέρωση του λογισμικού τους μειώνουν τις πιθανότητες μιας κυβερνοεπίθεσης που στοχεύει στις συσκευές τους, καθώς είναι πιθανό τα παλαιότερα ευάλωτα σημεία που θα μπορούσαν να χρησιμοποιηθούν από τους χάκερ να έχουν ήδη διορθωθεί. Υπάρχει πιθανότητα η ενημέρωση να διακόψει ορισμένες λειτουργίες του λογισμικού ή ακόμη και να το καταστήσει άχρηστο σε ορισμένες συσκευές, γι' αυτό και, μία φορά μετά την ενημέρωση, είναι καλή πρακτική να ελέγχετε αν η ενημέρωση δε διέκοψε τίποτα. Εκτός αυτού, το λογισμικό που δεν έχει ενημερωθεί μπορεί να χάσει τις νεότερες λειτουργίες που είναι πολύ βολικές. Από την άλλη πλευρά, οι παλαιότερες εκδόσεις του λογισμικού μπορεί απλώς να σταματήσουν να λειτουργούν σε νεότερες συσκευές ή σε αυτές που διατηρούνται ενημερωμένες. Παρόλο που η διαδικασία της ενημέρωσης μπορεί να φαίνεται λίγο χρονοβόρα, είναι πολύ σημαντική, όχι μόνο για λόγους ασφαλείας, αλλά και για να έχετε όλες τις πιο πρόσφατες λειτουργίες μιας συγκεκριμένης συσκευής ή ενός λογισμικού. Μια καλή πρακτική θα ήταν να κάνετε έναν εβδομαδιαίο έλεγχο του λογισμικού που χρησιμοποιείται όσον αφορά την ενημέρωσή του. Αυτός είναι ένας πραγματικά γρήγορος και απλός τρόπος για να διατηρήσετε τα δεδομένα πιο ασφαλή και να ενισχύσετε την απόδοση του λογισμικού αυτού.

Το **λογισμικό προστασίας από ιούς (antivirus)** είναι απαραίτητο και πρέπει να είναι εγκατεστημένο σε κάθε συσκευή. Δεν είναι δύσκολο να πέσει κανείς θύμα μιας επίθεσης phishing, και στις μέρες μας, με την αυξανόμενη δημοτικότητα της εξ αποστάσεως εργασίας, η μόλυνση ενός υπολογιστή με ιό μπορεί να προκαλέσει υποχρεωτική διακοπή της εργασίας για ημέρες ή ακόμη και εβδομάδες. Ένα antivirus είναι ένα είδος λογισμικού που ελέγχει κάθε αρχείο ή δεδομένο που είναι εγκατεστημένο ή πρόκειται να εγκατασταθεί σε έναν υπολογιστή. Φτιάχνεται για να διαπιστώνει αν κάποιο από τα αρχεία σε έναν υπολογιστή μπορεί να αποτελέσει πιθανή απειλή ή να προκαλέσει οποιαδήποτε ζημιά στους χρήστες και τις συσκευές τους.

Το antivirus λειτουργεί με δύο διαφορετικούς τρόπους. Ο ένας από αυτούς είναι **μια μέθοδος που βασίζεται σε υπογραφές** και λειτουργεί ως ένας κατάλογος γνωστών αρχείων που περιέχουν κακόβουλο λογισμικό και δημοσιεύονται από τις εταιρείες antivirus. Μόλις βρεθεί μια αντιστοιχία μεταξύ του αρχείου στη λίστα και στη συσκευή του χρήστη, μπλοκάρεται. Αυτή είναι μια κοινή μέθοδος που λειτουργεί καλά, καθώς ανακαλύπτονται χιλιάδες κακόβουλα προγράμματα κάθε μέρα, οπότε η λίστα είναι πραγματικά πλούσια σε δεδομένα. Το μόνο μειονέκτημα αυτής της μεθόδου είναι ότι μόλις η συσκευή του χρήστη μολυνθεί με έναν ιό που δεν περιλαμβάνεται στη λίστα, τότε ενδέχεται να μην προστατεύεται από αυτόν. Ο άλλος τρόπος με τον οποίο τα antivirus προστατεύουν τις συσκευές **είναι βασισμένος στη συμπεριφορά**. Αυτός είναι πιο πολύπλοκος και δε χρησιμοποιείται τόσο συχνά όσο οι άλλες μέθοδοι και μόνο τα πιο εξελιγμένα antivirus τον χρησιμοποιούν. Όπως υποδηλώνει το όνομα, η μέθοδος αυτή μελετά τη συμπεριφορά ενός συγκεκριμένου αρχείου και κρίνει αν το αρχείο αυτό μπορεί να είναι επικίνδυνο για τη συσκευή, ελέγχοντας επίσης για τυχόν απόπειρες τροποποίησης ή κρυπτογράφησης των δεδομένων στη συσκευή και στη συνέχεια το μπλοκάρει επειδή το επισημαίνει ως ιό.

Πηγή: freepik.com

Τα antivirus δεν προστατεύουν τους χρήστες μόνο με το μπλοκάρισμα των αρχείων που βρίσκονται στις συσκευές τους, αλλά τα περισσότερα από αυτά εμποδίζουν επίσης τους χρήστες να εισέρχονται σε μη εξουσιοδοτημένους ιστότοπους που

μπορούν να προκαλέσουν πιθανές απειλές στις συσκευές τους. Ορισμένα από αυτά τα προγράμματα μπορούν επίσης να καθαρίσουν τα λεγόμενα "ανεπιθύμητα αρχεία" για να ελευθερώσουν κάποιο χώρο στη συσκευή. Αυτή η διαδικασία μπορεί μερικές φορές να ενισχύσει επίσης την ταχύτητα επεξεργασίας ενός υπολογιστή ή ενός smartphone. Το antivirus είναι ένα κρίσιμο συστατικό κάθε συσκευής που είναι επιρρεπής στο να μολυνθεί με κακόβουλα δεδομένα και προσφέρει μια ευρεία γκάμα πλεονεκτημάτων που λειτουργούν σαν μια κλειστή πόρτα που δεν αφήνει τους ιούς να μπουν μέσα και διώχνει τους τυχόν υπάρχοντες.

Με όλες αυτές τις προτάσεις σε ισχύ, είναι εξαιρετικά σπάνιο να πέσει κάποιος θύμα κυβερνοεπίθεσης, και ακόμη και αν κάποιος επιχειρήσει να κλέψει τα δεδομένα από τον υπολογιστή κάποιου, είναι εξαιρετικά απίθανο να τα καταφέρει.

Κεφάλαιο 4 – Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα και Ασφάλεια Προσωπικών Πληροφοριών

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (General Data Protection Regulation - GDPR), ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018, είχε τις ρίζες του στη δεκαετία του 1950. Τότε δημιουργήθηκε η Σύμβαση για τα ανθρώπινα δικαιώματα, θέτοντας τα πρώτα θεμέλια για την προστασία των προσωπικών δεδομένων. Τρεις δεκαετίες αργότερα, με την ανάπτυξη των ηλεκτρονικών υπολογιστών, δημιουργήθηκε η Σύμβαση για την Προστασία Δεδομένων, δηλώνοντας ότι η ιδιωτικότητα αποτελεί, στην πραγματικότητα, ανθρώπινο δικαίωμα. Στις 24 Οκτωβρίου 1995, τέθηκε σε ισχύ η Οδηγία για την Προστασία Δεδομένων, η οποία ρύθμιζε τους νόμους για την προστασία των δεδομένων και τη διαβίβαση προσωπικών δεδομένων εκτός της ΕΕ. 17 χρόνια αργότερα, προτάθηκε μια επικαιροποίηση αυτών των κανονισμών και 4 χρόνια από την εν λόγω πρόταση, ο Γενικός Κανονισμός για την Προστασία Δεδομένων εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο για να καταστεί πλήρως εφαρμόσιμος σε ολόκληρη την Ευρωπαϊκή Ένωση μόλις δύο χρόνια αργότερα, τον Μάιο του 2018.

Πηγή: freepik.com

Ο πυρήνας του GDPR είναι να δώσει στους πολίτες της ΕΕ μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων. Πρόκειται για ένα τεράστιο σύνολο 99 άρθρων που ρυθμίζουν τους κανόνες προστασίας δεδομένων και τον τρόπο πρόσβασης στα δεδομένα. Αντικατέστησε την προηγούμενη οδηγία για την προστασία των δεδομένων του 1995, λόγω του γεγονότος ότι το τεχνολογικό περιβάλλον έμοιαζε σημαντικά διαφορετικό σε σχέση με σήμερα. Στις μέρες μας, σχεδόν κάθε Ευρωπαίος πολίτης διαθέτει τουλάχιστον ένα smartphone και οι επιχειρήσεις που προσφέρουν αγαθά ή υπηρεσίες μέσω του διαδικτύου έχουν γίνει εξίσου δημοφιλείς με τις παραδοσιακές αντίστοιχες επιχειρήσεις. Με τον GDPR, είναι ευκολότερο να ελέγχεται ποιες προσωπικές πληροφορίες μπορούν να αποθηκεύονται, να κοινοποιούνται ή να συλλέγονται από διάφορα μέρη. Οι πληροφορίες αυτές μπορεί να ποικίλλουν από διευθύνσεις IP, μέσω πληροφοριών για το μηνιαίο εισόδημα, μέχρι τις διατροφικές συνήθειες ενός ατόμου.

Στο πλαίσιο του GDPR, υπάρχουν 7 βασικές αρχές που θα πρέπει να χρησιμοποιούνται ως οδηγός για τον τρόπο διαχείρισης των δεδομένων των χρηστών. Αυτοί οι κανόνες μπορούν να εκληφθούν ως ένα πλαίσιο που έχει σχεδιαστεί για να δείξει τον κύριο σκοπό του κανονισμού. Μεταξύ αυτών των 7 κανόνων είναι:

- Νομιμότητα, δικαιοσύνη και διαφάνεια

Αυτό σημαίνει ότι τα δεδομένα πρέπει να αποθηκεύονται και να υποβάλλονται σε επεξεργασία με νόμιμο τρόπο. Δεν πρέπει να παραπλανούν άλλους χρήστες ως προς τον τρόπο αποθήκευσης και χρήσης τους.

- Περιορισμός του σκοπού

Προτείνεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται και να αποθηκεύονται για σαφείς, αδιαμφισβήτητους και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο που να αντιβαίνει στους σκοπούς αυτούς.

- Ακρίβεια

Αυτό σημαίνει ότι πρέπει να ληφθούν όλα τα εύλογα μέτρα για να διασφαλιστεί ότι όλα τα ανακριβή δεδομένα προσωπικού χαρακτήρα διαγράφονται ή διορθώνονται αμέσως. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και, όταν απαιτείται, να ενημερώνονται.

- Ελαχιστοποίηση δεδομένων

Οι οργανισμοί δεν πρέπει να συλλέγουν περισσότερα δεδομένα από όσα χρειάζονται από τους χρήστες τους. Θα πρέπει να είναι επαρκή και να περιορίζονται στα αναγκαία όσον αφορά τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

- Όριο αποθήκευσης

Σημαίνει ότι τα δεδομένα δεν πρέπει να αποθηκεύονται για διάστημα μεγαλύτερο από το αναγκαίο.

- Ακεραιότητα και εμπιστευτικότητα

Με άλλα λόγια, πρόκειται για την ασφάλεια των αποθηκευμένων δεδομένων. Η επεξεργασία τους θα πρέπει να γίνεται με κατάλληλα τεχνικά ή οργανωτικά μέτρα για την καλύτερη δυνατή ασφάλεια των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από ακούσια απώλεια, καταστροφή ή ζημία.

- Λογοδοσία

Αυτό σημαίνει ότι οι εταιρείες θα πρέπει να αποδεικνύουν ότι ακολουθούν τους κανόνες που αναφέρονται παραπάνω και να διασφαλίζουν ότι λαμβάνουν μέτρα για τον δεοντολογικό χειρισμό των προσωπικών δεδομένων.

Ο GDPR σχεδιάστηκε για την προστασία των χρηστών και των δεδομένων τους. Λαμβάνοντας αυτό υπόψη, προβλέπονται **οκτώ ατομικά δικαιώματα**. Τα σημαντικότερα από αυτά είναι:

- Το δικαίωμα ενημέρωσης σχετικά με τη συλλογή και τη χρήση των προσωπικών δεδομένων.

- Το δικαίωμα πρόσβασης, εξέτασης και λήψης αντιγράφου των προσωπικών δεδομένων που συλλέγονται και υποβάλλονται σε επεξεργασία από ορισμένα μέρη..
- Το δικαίωμα διαγραφής των προσωπικών δεδομένων.

Πηγή: freepik.com

Τα άλλα πέντε δικαιώματα των φυσικών προσώπων είναι: το δικαίωμα διόρθωσης, το δικαίωμα περιορισμού της επεξεργασίας, το δικαίωμα φορητότητας των δεδομένων, το δικαίωμα αντίρρησης και το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων.

Λόγω της αυξανόμενης συνειδητοποίησης της αξίας των προσωπικών πληροφοριών, οι άνθρωποι έχουν αρχίσει να δίνουν μεγαλύτερη προσοχή στο πόσα δεδομένα δίνουν σε εταιρείες και προτιμούν να επιλέγουν τα μέρη που είναι διαφανή σχετικά με τη συλλογή δεδομένων. Λόγω του GDPR, οι εταιρείες πρέπει να είναι περισσότερο ευαισθητοποιημένες σχετικά με το ποια δεδομένα συλλέγουν και πώς τα διασφαλίζουν, λόγω των υψηλών προστίμων που συνδέονται με τη μη συμμόρφωση με τους κανονισμούς του GDPR.

Η γνώση του GDPR μαζί με τις άλλες πρακτικές που αναφέρονται σε αυτόν τον οδηγό μπορεί όχι μόνο να διασφαλίσει το υψηλό επίπεδο ασφάλειας των προσωπικών πληροφοριών του χρήστη, αλλά και να καταστήσει δυσκολότερο για τους

εγκληματίες του διαδικτύου να παραβιάσουν τις βάσεις δεδομένων των εταιρειών. Οι ισχυροί κωδικοί πρόσβασης και οι γνώσεις σχετικά με διάφορες κακόβουλες πρακτικές, όπως το phishing και οι ιοί, εάν γίνουν κατανοητές και εφαρμοστούν σωστά, μπορούν να κάνουν τους ανθρώπους που εργάζονται εξ αποστάσεως να αισθάνονται πολύ πιο ασφαλείς σε αυτούς τους καιρούς που η τηλεργασία έχει γίνει κοινή πρακτική παγκοσμίως.

Κεφάλαιο 5 – Πρακτική δραστηριότητα

Πρακτική 1. Δημιουργία ενός ισχυρού και αξιομνημόνευτου κωδικού πρόσβασης

Ένας ισχυρός κωδικός πρόσβασης είναι μακρύς, περίπλοκος και περιέχει πολλά σύμβολα, αλλά είναι επίσης εύκολο να τον θυμάστε. Έχοντας αυτό κατά νου, ας δημιουργήσουμε έναν τέτοιο κωδικό χρησιμοποιώντας αυτά τα λίγα απλά βήματα:

1. Σκεφτείτε μια πρόταση ή ένα απόσπασμα που σκέφτεστε συχνά. Για παράδειγμα, ένα διάσημο απόσπασμα του Wayne Gretzky:
   "You miss 100 percent of the shots you don't take" («Χάνεις το 100 τοις εκατό των προσπαθειών που δεν κάνεις»).
2. Τώρα, φτιάξτε ένα ακρωνύμιο από αυτό το απόσπασμα:
   Y(ou) **m**(iss) **100 p**(ercent) **o**(f) **t**(he) **s**(hots) **y**(ou) **d**('ont) **t**(ake) = Ym100potsynt
3. Τώρα, προσθέστε ειδικούς χαρακτήρες. Για παράδειγμα, αντικαταστήστε το "1" με το "!", το "p" με το "%", προσθέστε μια υπογράμμιση και αλλάξτε τη γραφή των γραμμάτων, ώστε το τελικό αποτέλεσμα να μοιάζει ως εξής:
   Ym!00%ots_Ydt

Ο κωδικός πρόσβασης φαίνεται περίπλοκος, αλλά αν τον αναλύσουμε, θα δούμε ότι είναι αρκετά απλός και εύκολος στη μνήμη. Μια καλή πρακτική είναι να εξασκηθούμε στη σύνταξή του για κάποιο χρονικό διάστημα, ώστε η μυϊκή μας μνήμη να θυμάται τη σειρά των κουμπιών που πατάμε.

Πηγή: freepik.com

Πρακτική 2. Ελέγξτε το γραμματοκιβώτιό σας για ανεπιθύμητα μηνύματα και πιθανές απόπειρες ηλεκτρονικού "ψαρέματος".

Μάθαμε για τα διάφορα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου που μπορούν να μας σταλούν και πώς να τα αναγνωρίζουμε.

Ανοίξτε το γραμματοκιβώτιό σας και ελέγξτε αν υπάρχουν διαφημίσεις για προϊόντα που δεν έχετε ακούσει ποτέ ή ειδοποιήσεις για την κατάκτηση κάποιου βραβείου. Ελέγξτε επίσης για ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου σχετικά με απλήρωτα τιμολόγια ή αναστολές λογαριασμού. Αναλύστε τα, αλλά σε καμία περίπτωση **ΜΗΝ** ανοίγετε συνδέσμους ή συνημμένα αρχεία που παρέχονται στα μηνύματα. Στη συνέχεια, διαγράψτε αυτά τα μηνύματα και σκεφτείτε πόσα ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου υπήρχαν.

Χρήσιμοι σύνδεσμοι:

Πόσο ασφαλής είναι ο κωδικός πρόσβασής σας:

https://www.security.org/how-secure-is-my-password/

Πώς να εγκαταστήσετε μια σύνδεση VPN:

https://www.businessnewsdaily.com/15710-how-to-install-a-vpn-connection.html

4. Βιβλιογραφία

Anderson, S. (2022). *What Is Phishing? Guide with Examples for 2022*. SafetyDetectives. Retrieved May 10, 2022, from https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-...

Awati, R., & Teravainen, T. (2021). *What is email spam and how to fight it?* SearchSecurity. Retrieved May 9, 2022, from https://www.techtarget.com/searchsecurity/definition/spam?msclkid=9aeb4557cf8211ec82e6cfc07708ec54

Barracuda. (2020). *Spear Phishing: Top Threats and Trends* (Vol. 5). Barracuda. Retrieved May 10, 2022, from https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5...

Castagna, R., & Lavery, T. (2021). *General Data Protection Regulation (GDPR)*. WhatIs.Com. Retrieved June 24, 2022, from https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

Cheema, A. N., & Aamir, R. (2021). Trends of cyber crimes. *Proc. 18th International Conference on Statistical Sciences*, *35*, 261–269. https://www.researchgate.net/profile/Muhammad-Suhail-6/publication/353070981_Comparison_of_Ridge...

Chng, S., Han Yu, L., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*. https://doi.org/10.1016/s2451-9588(22)00018-5

Digital Marketing Experts – Editorial Review Board. (2021). *The Importance of Updating*. THAT! Company. Retrieved June 24, 2022, from https://www.thatcompany.com/the-importance-of-updating...

D'Mello, Y. (2018). *How did we get here? A brief history of the GDPR*. AiThority. Retrieved June 24, 2022, from https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/

Edwards, R. (2022). *How Can I Secure My Internet Connection?* SafeWise. Retrieved June 24, 2022, from https://www.safewise.com/online-security-faq/secure-internet-connection/

Elvin, A. E., Sundström, F., & von Heland, W. (2021). *Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations* (Master's dissertation). Department of Informatics, Lund School of Economics and Management, Lund University. Retrieved June 24, 2022, from https://lup.lub.lu.se/student-papers/search/publication/9052971

FIT Information Technology. (2022). *What is antivirus and why is it important?* Retrieved June 24, 2022, from https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/

Fogg, S. (2022). *What is GDPR? The Basics of the EU's General Data Protection Regulation*. Termly. Retrieved June 24, 2022, from https://termly.io/resources/articles/what-is-gdpr/

Fruhlinger, J. (2020). *Ransomware explained: How it works and how to remove it*. CSO Online. Retrieved May 11, 2022, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it...

Gajić, A. (2022). *Spam Statistics*. 99firms. Retrieved May 9, 2022, from https://99firms.com/blog/spam-statistics/?msclkid=18264839cf8b11ec8144c5ced7add618

General Data Protection Regulation (GDPR) – Official Legal Text. (2019). General Data Protection Regulation (GDPR). Retrieved June 24, 2022, from https://gdpr-info.eu/

Gibson, K. (2022). *6 Famous Identity Theft Cases in Recent Years*. Home Security Heroes. Retrieved May 12, 2022, from https://www.homesecurityheroes.com/famous-identity-theft-cases/

Gupta, M. (2021). Identity Theft in Cyberspace in India. *International Journal of Research Publication and Reviews*, *2*(7), 1700–1701. https://www.ijrpr.com/uploads/V2ISSUE7/IJRPR791.pdf

Hiley, C. (2021). *Brief history of cybersecurity and hacking*. CyberNews. Retrieved May 11, 2022, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/?msclkid=ebaaa52cd10911ecbb48b6bc018d0384

Jančis, M. (2022). *How to create a good and strong password*. CyberNews. Retrieved June 16, 2022, from https://cybernews.com/best-password-managers/how-to-create-a-strong-password/

Janssen, D. (2022). *VPN Explained: How Does It Work? Why Would You Use It?* VPNoverview.Com. Retrieved June 1, 2022, from https://vpnoverview.com/vpn-information/what-is-a-vpn/

Johansen, A. G. (2018). *What to Do If Your Identity Is Stolen: 14 Steps*. LifeLock. Retrieved May 12, 2022, from https://www.lifelock.com/learn/identity-theft-resources/do-these-things-immediately-if-your-identity-has-been-stolen

Lopez, A. (2021). *Top 10 Reasons Why an Antivirus Is Important*. Business 2 Community. Retrieved June 24, 2022, from https://www.business2community.com/cybersecurity/top-10-reasons-why-an-antivirus-is-important...

Malwarebytes. (n.d.). *What is spam?* Retrieved May 11, 2022, from https://www.malwarebytes.com/spam...

Martens, B. (2021). *The Ultimate Internet Safety Guide for Seniors (2022)*. SafetyDetectives. Retrieved June 24, 2022, from https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/?msclkid=9e7ed272cf5f11ecbe3d195abee11879

Milasi, S., González-Vázquez, I., & Fernández-Macías, E. (2020). *Telework in the EU before and after the COVID-19: Where we were, where we head to*. Joint Research Centre. Retrieved June 24, 2022, from https://joint-research-centre.ec.europa.eu/system/files/2021-06/...

Minahan, B. (2020). *How to Create a Strong Password in 6 Easy Steps*. aNetworks. Retrieved June 1, 2022, from https://www.anetworks.com/how-to-create-a-strong-password-2021/

Mitra, A. (2017). *What is a spambot and how to stop spambots?* TheSecurityBuddy. Retrieved May 11, 2022, from https://www.thesecuritybuddy.com/anti-spam/what-is-spambot-and-how-to-stop-spambots...

Molinaro, D. (2022). *How Does Two-Factor Authentication (2FA) Work?* Avast. Retrieved June 1, 2022, from https://www.avast.com/c-how-does-two-factor-authentication-work...

Movassagh, N. (2021). *Awareness and perception of phishing variants from Policing, Computing and Criminology students in Canterbury Christ Church University.* (Master's dissertation). Canterbury Christ Church University School of Law. https://repository.canterbury.ac.uk/item/8yq89/awareness-and-perception-of-phishing-variants-from-policing-computing-and-criminology-students...

Peterson, S. (2019). *The Ultimate Guide for Online Security and Privacy in 2020*. The Hack Post. Retrieved June 1, 2022, from https://thehackpost.com/the-ultimate-guide-for-online-security-and-privacy-in-2020.html

Proofpoint. (n.d.). *What is Email Spoofing? Definition & Examples*. Retrieved June 24, 2022, from https://www.proofpoint.com/us/threat-reference/email-spoofing?msclkid=df4910a2d03511ecb958bcffa531b6ab

Spoofing and Phishing. (2022). Federal Bureau of Investigation. Retrieved May 10, 2022, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing?msclkid=8cb3cf19d04d11ecb7c47a9f8893c5e8

Tanwar, R., Choudhury, T., Zamani, M., Gupta, S., & Tajpour, A. (2021). Information Security and Optimization. In *Information Security and Optimization* (pp. 25–26). CRC Press. Retrieved May 10, 2022, from https://books.google.nl/books?id=...

TechFunnel Contributors. (2020). *Most Common Hacking Techniques for Beginners*. Techfunnel. Retrieved May 11, 2022, from https://www.techfunnel.com/information-technology/hacking-techniques/?msclkid=94348692d12111eca373f0ead6ff7fe9

Tschabitscher, H. (2021). *What Is an Example of Spam Email?* Lifewire. Retrieved May 9, 2022, from https://www.lifewire.com/what-and-why-spam-email-1173993#toc-what-are-some-examples-of-spam

Tsonchev, A. (2020). *Six of the biggest security threats facing the remote workforce*. TechRadar. Retrieved June 24, 2022, from https://www.techradar.com/news/six-of-the-biggest-security-threats-facing-the-remote-workforce?msclkid=9e80a80ccf5f11ec92c0ce7275373494

Williams, L. (2022). *What is Hacking? Types of Hackers | Introduction to Cybercrime*. Guru99. Retrieved June 24, 2022, from https://www.guru99.com/what-is-hacking-an-introduction...

Πηγή εικόνας στη σελίδα τίτλου: freepik.com