ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΤΑΣΕΙΣ-ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Χρήσιμες οδηγίες - Προστασία Δεδομένων στον χώρο εργασίας

1. Γιατί πρέπει να ακολουθείται η αρχή του «καθαρού γραφείου»;

Οι εργαζόμενοι μπορούν να βοηθήσουν στην προστασία των προσωπικών τους πληροφοριών και των εμπιστευτικών πληροφοριών κατά την εργασία ώστε να μην βρεθούν στα χέρια μη εξουσιοδοτημένων ατόμων. Η ιδιωτικότητα και η εμπιστευτικότητα μπορούν να προωθηθούν, ιδίως με την τήρηση της λεγόμενης αρχής του «καθαρού γραφείου».

Για αυτόν τον λόγο πρέπει να ακολουθηθούν 3 κυρίως κανόνες:

- **Τακτοποίηση**: Η τάξη στο γραφείο δεν χρησιμεύει μόνον για να μπορεί να βρίσκει κανείς ότι ψάχνει στον εργασιακό του χώρο. Όποιος κρατά τακτοποιημένο το γραφείο του, δεν κινδυνεύει να θέσει δεδομένα και πληροφορίες στα χέρια μη εξουσιοδοτημένων προσώπων. Όσον αφορά την προστασία των δεδομένων, κάντε στον εαυτό σας την ερώτηση: "Πρέπει αυτό να είναι εδώ;" Αν όχι, τότε να το απομακρύνετε! Καλύτερα στο συρτάρι ή στο ντουλάπι αρχειοθέτησης.

- **Απομάκρυνση**: Οποιοσδήποτε φορέας δεδομένων, όπως Notebooks, smartphones, USB ή έγγραφα, θα πρέπει πάντα να απομακρύνεται, αν δεν χρειάζεται να χρησιμοποιηθεί στο πλαίσιο της τρέχουσας εργασίας.
- **Κλείδωμα**: Όταν είστε μακριά από τον εργασιακό σας χώρο για μεγάλο χρονικό διάστημα, για παράδειγμα επειδή πρόκειται να γευματίσετε, όταν βρίσκεστε σε μια συνάντηση ή μετά το τέλος της καθημερινής εργασίας, δεν πρέπει απλά να τοποθετήσετε το φορητό υπολογιστή σας, το κινητό τηλέφωνο και τον φορέα δεδομένων (όπως ένα USB ή έγγραφα) σε ένα ασφαλές χώρο. Θυμηθείτε επίσης να κλείσετε αυτό το χώρο, είτε πρόκειται για ντουλάπι είτε για συρτάρι, και αφαιρέστε το κλειδί. Εάν αφήσετε το κλειδί πάνω στο ντουλάπι, δεν είναι απαραίτητο να είναι κανείς ειδικευμένος για να αποκτηθεί γνώση εμπιστευτικού περιεχομένου.

2. Ποιες είναι οι βασικές αρχές κατά την εισαγωγή κωδίκων πρόσβασης;

"Όταν επιλέγεται κωδικούς πρόσβασης αποφεύγετε να χρησιμοποιείται τους λεγόμενους «ασήμαντους κωδικούς πρόσβασης». Αυτοί αποτελούνται από κωδικούς που μπορούν εύκολα να συνδεθούν με τον χρήστη όπως όνομα, ημερομηνία γέννησης, τηλέφωνο κλπ. Για να είναι σίγουρος ένας κωδικός πρόσβασης πρέπει να λαμβάνονται υπ' όψη τα εξής:

- Ο ιδανικός κωδικός αποτελείται τουλάχιστον από 10 στοιχεία
- Θα πρέπει να χρησιμοποιούνται μεγάλα και μικρά γράμματα καθώς και σύμβολα (π.χ. @, #, ? κλπ.)
- Δεν θα πρέπει να χρησιμοποιούνται πλήκτρα που ευρίσκονται το ένα δίπλα στο άλλο (π.χ. 12345, αβγδε)
- Ο Κωδικός δεν θα πρέπει να μπορεί να συνδεθεί με τον χρήστη (π.χ. αγαπημένο φαγητό, χαϊδευτικό όνομα, όνομα συζύγου κλπ)

3. Πού πρέπει να φυλάει κανείς τους κωδικούς του;

Ο ιδανικός τόπος φύλαξης των κωδικών είναι η μνήμη. Βεβαίως αυτό δεν είναι εύκολο ειδικά όταν ο κωδικός είναι δύσκολος. Φτιάξετε μία έκφραση από τον κωδικό σας, την οποία θα είναι εύκολο να την θυμάστε (π.χ. «ένα το χελιδόνι και η άνοιξη ακριβή» δίνει τον κωδικό «ΕΤΧ&ΗΑΑ»).

Μην σημειώνετε τους κωδικούς σας, Το τμήμα υπολογιστών της επιχείρησης θα σας δώσει συμβουλές για την επιλογή ασφαλών τρόπων αποθήκευσης των κωδικών για

παράδειγμα με προγράμματα που αποθηκεύουν κρυπτογραφημένους τους κωδικούς πρόσβασης.

4. Επιτρέπεται να δίνει κανείς τους κωδικούς τους στους συναδέλφους του;

Δεν επιτρέπεται να δίνετε τους κωδικούς σας σε κανέναν συνάδελφό σας. Ο λόγος είναι, ότι όποιος συνδεθεί με το όνομά σας και με τον κωδικό πρόσβασής σας, προσποιείται ότι είστε εσείς. Αυτό μπορεί να έχει κακές συνέπειες. Εάν ένας συνάδελφός σας προκαλέσει με την χρήση του υπολογιστή βλάβη, πρέπει να αποδείξετε εσείς, ότι δεν έχετε ενεργήσει. Αν ανησυχείτε ότι κάποιος άλλος έχει πάρει τον κωδικό πρόσβασής σας, θα πρέπει να αλλάξετε αμέσως τον κωδικό πρόσβασής σας και εάν είναι απαραίτητο να ενημερώσετε το τμήμα πληροφορικής της επιχείρησης.

5. Ποιος είναι ο καλύτερος τρόπος να καταστρέφονται έγγραφα;

Σε περίπτωση που τα έγγραφα περιέχουν προσωπικά δεδομένα ή εμπιστευτικές πληροφορίες, δεν επιτρέπεται να δίνονται μαζί με όλα τα απορρίμματα της επιχείρησης. Σε αυτήν την περίπτωση προτιμότερος είναι ο καταστροφέας εγγράφων.

6. Τι πρέπει κανείς να λάβει υπ’ όψη του κατά την καταστροφή φορέων δεδομένων;

Εάν πρέπει να καταστραφούν φορείς δεδομένων όπως οι σκληροί δίσκοι, τα USB stick, DVD ή κάρτες μνήμης, πρέπει να διασφαλιστεί ότι τα αποθηκευμένα προσωπικά δεδομένα και οι εμπιστευτικές πληροφορίες δεν πέφτουν σε λάθος χέρια. Κατ’ αρχή αυτό μπορεί να αποκλειστεί με τη μηχανική καταστροφή των φορέων δεδομένων. Εάν αυτό δεν είναι δυνατό, ο φορέας δεδομένων πρέπει να διαγραφεί με διαδικασίες που λαμβάνουν υπ’ όψη την προστασία δεδομένων. Το τμήμα πληροφορικής της επιχείρησης θα σας πληροφορήσει σχετικά με τα κατάλληλα μέσα για τη διαγραφή των φορέων δεδομένων.

7. Πώς πρέπει να εφαρμόζεται η «αρχή του ελαχίστου»;

Σε ένα επαγγελματικό ταξίδι δεν χρειάζεστε τον πλήρη εξοπλισμό του γραφείου σας. Επομένως, να έχετε μαζί σας μόνο τους φορείς δεδομένων και τα έγγραφα που χρειάζεστε απολύτως για την εργασία σας. Αυτό που δεν έχετε, δεν μπορεί να κλαπεί ή να χαθεί.

8. Για ποιόν λόγο τα δεδομένα και οι φορείς δεδομένων πρέπει να κρυπτογραφούνται;

Η κρυπτογράφηση των δεδομένων και των φορέων δεδομένων καθιστά πολύ δύσκολη την πρόσβαση σε μη εξουσιοδοτημένα άτομα. Οι επιλογές κρυπτογράφησης είναι πολλές, για παράδειγμα, δημιουργώντας ένα αρχείο κρυπτογραφημένου αρχείου (το λεγόμενο αρχείο ZIP) ή χρησιμοποιώντας λογισμικό κρυπτογράφησης. Το βασικό πλεονέκτημα ευρίσκεται στο ότι , εάν υπάρξει κλοπή, η ζημιά περιορίζεται κυρίως στην υλική αξία του κλεμμένου αντικειμένου. Επειδή χάρη στην κρυπτογράφηση δεν μπορεί να υπάρχει πρόσβαση στα δεδομένα, δεν υπάρχει κίνδυνος για το ιδιωτικό απόρρητο και την εμπιστευτικότητα.

9. Ποια τεχνικά μέτρα ασφαλείας έχουν μεγάλη σημασία;

Ιδιαίτερα όταν ευρίσκεστε εκτός γραφείου είναι σημαντικό, να χρησιμοποιείτε τους υφιστάμενους μηχανισμούς προστασίας. Ποτέ μην απενεργοποιείτε το τείχος προστασίας του φορητού σας υπολογιστή και ποτέ μην απενεργοποιείτε τη λειτουργία σαρωτή ιών. Το τείχος προστασίας και η αυτόματη ανίχνευση ιών είναι ιδιαίτερα σημαντικοί όταν συνδέετε τον υπολογιστή σας στο Internet, για παράδειγμα, για να ανακτήσετε μηνύματα ηλεκτρονικού ταχυδρομείου. Αλλά είναι εξίσου σημαντικές όταν λαμβάνετε δεδομένα και αρχεία από συνεργάτες ή πελάτες που βρίσκονται σε USB ή CD. Τα προσωπικά δεδομένα σε έναν φορέα δεδομένων κινητής τηλεφωνίας πρέπει πάντα να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Η κρυπτογράφηση των δεδομένων ή ολόκληρου του τηλεφώνου είναι επαρκές μέσο. Εάν δεν χρειάζεστε την ασύρματη σύνδεση, θα πρέπει να απενεργοποιήσετε τη σχετική λειτουργία του φορητού σας υπολογιστή ή του smartphone σας.

10. Τι πρέπει να γίνει σε περίπτωση απώλειας υπολογιστή, φορέα δεδομένων ή εγγράφων;

Σε αυτή την περίπτωση πρέπει να ενημερώσετε αμέσως την υπηρεσία Πληροφορικής. Ενημερώστε τον προϊστάμενό σας και το τμήμα πληροφορικής. Εάν επηρεάζονται προσωπικά δεδομένα ή εμπιστευτικές πληροφορίες, αυτοί θα αξιολογήσουν την κατάσταση και θα λάβουν τα κατάλληλα μέτρα. Σημαντικό: Εάν κάτι κλαπεί από εσάς, φροντίστε να υποβάλετε μια καταγγελία στην τοπική αστυνομία και να επιβεβαιώσετε τη μήνυσή σας.