ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ / ΕΤΑΙΡΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΗΛΕΡΓΑΣΙΑ

Κάθε φορά που είναι αναγκαίο να εργαζόμαστε από το σπίτι ή εξ αποστάσεως, είναι καλό να μη λησμονούμε ορισμένους κανόνες που θα μας βοηθήσουν να διασφαλίσουμε την ακέραιη διατήρηση των προσωπικών δεδομένων και εταιρικών πληροφοριών. Ας έχουμε υπόψη ότι η εξ αποστάσεως εργασία αποτελεί ένα προνόμιο και για αυτό το λόγο, ανεξαρτήτως του χώρου εργασίας μας, θα πρέπει όλοι να ακολουθούμε τις διαδικασίες και πολιτικές της WIN MEDICA. Τυχόν παραβίαση αυτών δύναται να επιφέρει σημαντικούς νομικούς κινδύνους και οικονομική ζημία στην εταιρεία. Συνεπώς, κατά την τηλεργασία, φροντίζουμε να εφαρμόζουμε το ίδιο επίπεδο προστασίας των δεδομένων και πληροφοριών με αυτό που θα διασφαλίζαμε εάν εργαζόμασταν στις εταιρικές εγκαταστάσεις.

1. Προκειμένου να συνδεθούμε απομακρυσμένα στον εταιρικό υπολογιστή χρησιμοποιούμε αποκλειστικά τον εξοπλισμό που έχει παραχωρήσει σε εμάς η εταιρεία, όπου υπάρχει εγκατεστημένο λογισμικό προστασίας από ιούς και η σύνδεση γίνεται μόνο μέσω ασφαλούς δικτύου (VPN).
2. Διασφαλίζουμε τη φυσική ασφάλεια των ηλεκτρονικών συσκευών μας (υπολογιστών, κινητών τηλεφώνων, tablets κ.λπ.).
3. Αποφεύγουμε να χρησιμοποιούμε τσάντες μεταφοράς ή αποθηκευτικά μέσα που φανερώνουν το περιεχόμενο αυτών (λ.χ. με την επωνυμία της κατασκευάστριας εταιρείας).
4. Δεν επιτρέπουμε σε μέλη της οικογένειάς μας ή σε τρίτους εν γένει να χρησιμοποιούν τις εταιρικές συσκευές μας.
5. Αλλάζουμε τους κωδικούς πρόσβασης με τη συχνότητα και τους κανόνες που ορίζει η Πολιτική της εταιρείας και δεν αφήνουμε ξεκλείδωτες τις ηλεκτρονικές συσκευές μας.
6. Δεν κοινοποιούμε τους εταιρικούς κωδικούς πρόσβασης σε μέλη της οικογένειάς μας (και, βεβαίως, σε κανένα άλλο τρίτο πρόσωπο).
7. Κατά την επιλογή χρήσης εφαρμογών που έχουν αναπτύξει τρίτοι σε σχέση με την τηλεδιάσκεψη, την απομακρυσμένη εργασία κ.λπ. δείχνουμε τη δέουσα επιμέλεια σχετικά με την προστασία των προσωπικών δεδομένων, όπως και απόρρητων – εμπιστευτικών εταιρικών δεδομένων, καθώς οι εφαρμογές αυτές δεν είναι πάντοτε πιστοποιημένες για τη μεταφορά και αποθήκευση τέτοιων δεδομένων .
8. Χρησιμοποιούμε αποκλειστικά τα εταιρικά emails προκειμένου να αποστείλουμε ή να παραλάβουμε προσωπικά δεδομένα ή εταιρικές πληροφορίες.
9. Κατά τη διάρκεια τηλεδιασκέψεων διατηρούμε την εμπιστευτικότητα αυτών και τις πραγματοποιούμε σε χώρο όπου, κατά τη διάρκεια των επικοινωνιών, αποκλείουμε την πρόσβαση τρίτων.
10. Δεν συνδεόμαστε σε ιστοσελίδες που ενέχουν υψηλό κίνδυνο μόλυνσης με κακόβουλο λογισμικό (gambling, porn sites κ.ά.).
11. Αποφεύγουμε εν γένει την άσκοπη περιήγηση στο διαδίκτυο μέσω του εταιρικού εξοπλισμού. Συχνά ακόμη και νόμιμοι ιστότοποι ενέχουν κινδύνους μετάδοσης κακόβουλου λογισμικού.
12. Ενημερώνουμε άμεσα το λογισμικό του εταιρικού ή προσωπικού υπολογιστή μας, όταν εμφανίζεται το σχετικό μήνυμα.
13. Προστατεύουμε (και) τους προσωπικούς υπολογιστές με αντιϊκό λογισμικό.
14. Αποφεύγουμε τη σύνδεση σε ασύρματα δημόσια δίκτυα ή δίκτυα τρίτων.
15. Προστατεύουμε το οικιακό ασύρματο δίκτυο με ισχυρό κωδικό και δεν το αφήνουμε ξεκλείδωτο.
16. Αλλάζουμε τον προεπιλεγμένο κωδικό πρόσβασης στο Internet Router.
17. Δεν αποθηκεύουμε εταιρικές πληροφορίες σε οικιακά αποθηκευτικά μέσα (μη κρυπτογραφημένα USB) ή σε ιστοχώρους αποθήκευσης δεδομένων (Dropbox, OneDrive κ.λπ.), που είναι συνδεμένοι με προσωπικούς μας λογαριασμούς.
18. Αποθηκεύουμε τακτικά τις αλλαγές που κάνουμε σε αρχεία που είναι αποθηκευμένα στο κεντρικό αποθηκευτικό μέσο της εταιρείας μας, όταν αυτό είναι εφικτό, όπου τηρούνται οι πολιτικές backup της εταιρείας, συνεπώς εξασφαλίζεται η ακέραιη διατήρηση των δεδομένων.

19. Φροντίζουμε να διασφαλίσουμε οιαδήποτε εμπιστευτική ή προσωπική πληροφορία, είτε είναι σε ηλεκτρονική μορφή είτε σε έντυπη, προτού φύγουμε από τις εγκαταστάσεις της εταιρείας. Οι εμπιστευτικές ή προσωπικές πληροφορίες, σε κάθε περίπτωση μεταφοράς αυτών εκτός των εταιρικών εγκαταστάσεων, είτε με ηλεκτρονική είτε με έγχαρτη μορφή, πρέπει να περιορίζονται στις απολύτως απαραίτητες για την εκπλήρωση της εργασίας.
20. Σε περίπτωση εντοπισμού ύποπτης συμπεριφοράς ή δυσλειτουργίας στο λογισμικό μας, επικοινωνούμε άμεσα με το Τμήμα IT της WIN MEDICA.
21. Δεν ανοίγουμε e-mails με ύποπτο περιεχόμενο ή όταν προέρχονται από άγνωστους αποστολείς. Η ΕΛ.ΑΣ. προειδοποιεί ότι αυτή τη περίοδο διάφοροι επιτήδειοι προσπαθούν να εγκαταστήσουν κακόβουλο λογισμικό στους υπολογιστές μας αποστέλλοντας e-mails με θέμα τον Covid-19 (phishing e-mails κ.λπ.).

ΓΕΝΙΚΕΣ ΟΔΗΓΙΕΣ:

- Λάβετε μέτρα για να διαχειριστείτε την ευημερία και την καλή ψυχική σας διάθεση, ενώ εργάζεστε από το σπίτι. Εάν έχετε λιγότερο άγχος και είσαστε λιγότερο αποσπασμένοι, είναι λιγότερο πιθανό να κάνετε κάποιο λάθος κατά το χειρισμό των προσωπικών δεδομένων ή εταιρικών εμπιστευτικών πληροφοριών.
- Ορίστε τη δομή και τα χρονικά όρια γύρω από την εργασία σας από το σπίτι. Εάν είναι δυνατό, δημιουργήστε έναν ειδικό χώρο εργασίας μέσα στο σπίτι όπου θα μπορείτε να ΄πηγαίνετε στο γραφείο΄.
- Κάνετε διαλείμματα μέσα στην ημέρα.
- Προσπαθήστε να διαχωρίσετε την ΄εργασία΄ στο σπίτι από τη ΄διαβίωση΄ στο σπίτι.