Τηλεργασία και COVID-19:

Τι χρειάζεται προσοχή από χρήστες και οργανισμούς

Μαθητική Ομάδα: *Γ' τάξη ΕΠΑΛ - ΕΚ (Εργαστηριακού Κέντρου) Λιβαδειάς της ειδικότητας Τεχνικός Εφαρμογών* Πληροφορικής.

Υπεύθυνη εκπ/κός: Κοντογιάννη Παναγιούλα

Τηλεργασία ή εργασία από απόσταση είναι μια νέα μορφή εργασίας κατά την οποία οι εργαζόμενοι έχουν τη δυνατότητα να εργάζονται από οπουδήποτε και οποιαδήποτε μέρα και ώρα. Με άλλα λόγια, η καθημερινή μεταφορά τους σε ένα κεντρικό τόπο δουλειάς αντικαθίστανται από τη δυνατότητα εργασίας κάνοντας χρήση των σύγχρονων μορφών τηλεπικοινωνίας

Με την απόφαση των κυβερνήσεων να κλείσουν εκπαιδευτικά ιδρύματα και χώροι εργασίας σε μια προσπάθεια να περιοριστεί η εξάπλωση του COVID-19/Coronavirus, πολλοί από εμάς θα χρειαστεί να συνδεθούμε εξ αποστάσεως σε εργασιακά/σχολικά δίκτυα, επιβαρύνοντας ακόμα περισσότερο τους διαδικτυακούς πόρους. Επίσης ένας μεγάλος αριθμός εργαζομένων πρέπει να εργαστεί από το σπίτι, χωρίς τη συνηθισμένη προστασία των εταιρικών δικτύων.

Η εργασία ή η εκπαίδευση από το σπίτι για πρώτη φορά μπορεί να μοιάζουν τρομακτικές, ειδικά για εκείνους που είναι δεν είναι συνηθισμένοι να είναι ίδιοι υπεύθυνοι για την ψηφιακή τους ασφάλεια. Η σύνδεση εξ αποστάσεως σε σχολικά ή εργασιακά δίκτυα προσφέρει ευελιξία στο πού και πώς δουλεύουμε, αλλά μπορεί επίσης να παρουσιάσει κάποιες προκλήσεις και πιθανούς κινδύνους για την ασφάλεια.

Επιπλέον, πολλοί οργανισμοί δεν είναι προσανατολισμένοι στην τηλεργασία και έτσι προσπαθούν να κατανοήσουν τις προκλήσεις σε πραγματικό χρόνο, υπό εξαιρετικές περιστάσεις, ενώ για κάποιους είναι πιο συνηθισμένο και αποτελεί ευκαιρία να επανεξετάσουν την ασφάλεια γύρω από την απομακρυσμένη πρόσβαση στα εταιρικά συστήματα. Μόλις μια συσκευή βρεθεί εκτός της υποδομής εταιρικού δικτύου και συνδεθεί με νέα δίκτυα και WIFI, οι κίνδυνοι διευρύνονται και αυξάνονται. Ακολουθούν κάποια απλά βήματα που χρήστες και οργανισμοί μπορούν να ακολουθήσουν για να μειώσουν τους ψηφιακούς κινδύνους που σχετίζονται με την απομακρυσμένη σύνδεση.

Συμβουλές προς χρήστες:

1. Προστατέψτε όλες τις συσκευές σας με ένα αξιόπιστο προϊόν διαδικτυακής ασφάλειας, συμπεριλαμβανομένων των φορητών συσκευών.
2. Πάντα να εφαρμόζετε τις πιο πρόσφατες ενημερώσεις στα λειτουργικά συστήματα και τις εφαρμογές σας μόλις αυτές γίνουν διαθέσιμες.
3. Χρησιμοποιείτε μόνο εφαρμογές από αξιόπιστες πηγές, π.χ. το αξιόπιστο εκπαιδευτικό portal που χρησιμοποιείτε ή εκείνα που σας παρέχονται από την εργασία ή το εκπαιδευτικό σας ίδρυμα.
4. Χρησιμοποιείτε μόνο αξιόπιστα δίκτυα για δραστηριότητες στο διαδίκτυο. Εάν δεν είναι το δίκτυό σας και πρέπει να συνδεθείτε στο διαδίκτυο, χρησιμοποιήστε ένα VPN (Εικονικό Ιδιωτικό Δίκτυο) για να διασφαλίσετε τη σύνδεσή σας.
5. Πάντα να πληκτρολογείτε τις διευθύνσεις ιστού. Μην κάνετε κλικ σε συνδέσμους ή συνημμένα και μην απαντάτε σε ανεπιθύμητα μηνύματα.
6. Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας τακτικά σε μια εξωτερική μονάδα δίσκου που κρατάτε εκτός σύνδεσης για να αποφύγετε την απώλεια της εργασίας σας.

Συμβουλές προς οργανισμούς:

1. Παρέχετε ένα VPN ώστε το προσωπικό να συνδεθεί με ασφάλεια στο εταιρικό δίκτυο.
2. Όλες οι εταιρικές συσκευές – συμπεριλαμβανομένων των κινητών και των φορητών υπολογιστών – θα πρέπει να προστατεύονται με κατάλληλο λογισμικό ασφαλείας (π.χ. να επιτρέπεται η διαγραφή δεδομένων από συσκευές που έχουν αναφερθεί ως χαμένες ή έχουν κλαπεί, διαχωρίζοντας προσωπικά δεδομένα και δεδομένα εργασίας και περιορίζοντας τις εφαρμογές που μπορούν να εγκατασταθούν).
3. Να εφαρμόζετε πάντα τις πιο πρόσφατες ενημερώσεις σε λειτουργικά συστήματα και εφαρμογές.
4. Περιορίστε τα δικαιώματα πρόσβασης των ατόμων που συνδέονται στο εταιρικό δίκτυο.
5. Βεβαιωθείτε ότι το προσωπικό γνωρίζει τους κινδύνους απόκρισης σε ανεπιθύμητα μηνύματα.

Πηγές :

https://www.techpress.gr/index.php/archives/147257

https://el.wikipedia.org/wiki/%CE%A4%CE%B7%CE%BB%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1