

Ασφαλής τηλεργασία

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΕΠΙΧΕΙΡΗΣΕΙΣ



Καθορίστε εταιρικές πολιτικές και διαδικασίες (δοκιμάστε τις εκ των προτέρων αν είναι δυνατόν)

Καθορίστε μια σαφή πολιτική τηλεργασίας που περιλαμβάνει οδηγίες πρόσβασης στους εταιρικούς πόρους και υπεύθυνο επικοινωνίας σε περίπτωση προβλήματος. Ορίστε μια σαφή διαδικασία αντιμετώπισης των προβλημάτων ασφάλειας. Εφαρμόστε επιπλέον μέτρα ελέγχου εργασίας με ενημέρωση προς μεσαία και ανώτερα στελέχη για υπογραφή, έγκριση/σχόλια και πληροφορίες.

Ασφαλίστε τον εξοπλισμό τηλεργασίας σας



Εφαρμόστε μέτρα όπως κρυπτογράφηση σκληρού δίσκου, διακοπή σύνδεσης λόγω αδράνειας, φίλτρα οθόνης, έλεγχο ταυτοποίησης, έλεγχο και κρυπτογράφηση εξωτερικών μέσων αποθήκευσης (π.χ. USB flash). Εφαρμόστε τεχνικές εξ' αποστάσεως απενεργοποίησης συσκευών που έχουν χαθεί ή κλαπεί.



Ασφαλής απομακρυσμένη πρόσβαση

Επιτρέψτε στους εργαζομένους σας να συνδέονται στο εταιρικό δίκτυο μόνο μέσω του VPN της εταιρίας και με ταυτοποίηση πολλών σταδίων. Βεβαιωθείτε ότι οι εξ' αποστάσεως συνδέσεις λήγουν αυτόματα και απαιτείται ταυτοποίηση μετά από συγκεκριμένη περίοδο αδράνειας.

Κρατήστε λειτουργικά συστήματα και εφαρμογές ενημερωμένα



Θα μετριάσει τον κίνδυνο που διατρέχουν από εγκληματίες του κυβερνοχώρου που προσπαθούν να εκμεταλλευτούν τρωτά σημεία.



Ασφαλίστε τις εταιρικές επικοινωνίες σας

Εφαρμόστε πρωτόκολλα ταυτοποίησης πολλών σταδίων για πρόσβαση στο εταιρικό email. Παρέχετε ασφαλή κανάλια επικοινωνίας για συνομιλία μεταξύ των εργαζομένων, αλλά και με εξωτερικούς φορείς.

Αυξήστε τους ελέγχους ασφάλειας



Ελέγχετε τακτικά για ύποπτη πρόσβαση απομακρυσμένων χρηστών και αυξήστε τα επίπεδα ελέγχου για εντοπισμό επιθέσεων μέσω VPN.



Αυξήστε την ευαισθητοποίηση του προσωπικού σχετικά με τους κινδύνους της τηλεργασίας

Ενημερώστε τους εργαζομένους σχετικά με την πολιτική τηλεργασίας της εταιρίας. Αυξήστε την ευαισθητοποίησή τους για τις απειλές στον κυβερνοχώρο, ιδιαίτερα το phishing και τους επιτήδειους που προσπαθούν να αποσπάσουν εμπιστευτικές πληροφορίες (social engineering).

Κάντε τακτικούς ελέγχους στο προσωπικό



Ορίστε ρεαλιστικούς στόχους, χρονοδιαγράμματα εργασίας και μηχανισμούς παρακολούθησης. Δείξτε ευελιξία, όπου είναι δυνατόν, λαμβάνοντας υπόψη τις ιδιαιτερότητες του καθενός.

Ασφαλής Τηλεργασία

ΣΥΜΒΟΥΛΕΣ

ΓΙΑ ΕΡΓΑΖΟΜΕΝΟΥΣ



Προσπελαύνετε τα δεδομένα της εταιρείας με τον εταιρικό εξοπλισμό

Χρησιμοποιείτε μόνο συσκευές και λογισμικό που παρέχονται από την εταιρεία. Δημιουργήστε ισχυρούς κωδικούς πρόσβασης, μην τους καταγράφετε πουθενά και προσέχετε να μην είναι ορατοί σε τρίτους όταν τους πληκτρολογείτε. Αποφύγετε τη χρήση άλλων μέσων στην εργασία σας, ακόμη και αν σας φαίνονται κατάλληλα.



Σταμάτα. Σκέψου. Συνδέσου.

Πριν ξεκινήσετε την τηλεργασία, εξοικειωθείτε με τις συσκευές, πολιτικές και διαδικασίες της εταιρείας. Σιγουρευτείτε ότι γνωρίζετε την ορθή χρήση του εξοπλισμού καθώς και πού μπορείτε να απευθυνθείτε για βοήθεια.



Προσέξτε την ασφάλεια στην εξ' αποστάσεως πρόσβαση

Συνδεθείτε στο εταιρικό δίκτυο μόνο μέσω του VPN της εταιρείας και προστατέψτε τα στοιχεία που έχετε στην κατοχή σας (π.χ. έξυπνη κάρτα) για σύνδεση στο VPN.

Προστατέψτε τον εξοπλισμό και το περιβάλλον τηλεργασίας σας



Μην επιτρέπετε στα μέλη της οικογενείας σας πρόσβαση στις συσκευές της εργασίας σας. Απενεργοποιήστε τις όταν δεν είναι υπό την επίβλεψή σας και κρατήστε τις σε ασφαλές μέρος προς αποφυγή απώλειας, βλάβης ή κλοπής. Προσέξτε ώστε η οθόνη σας να μην είναι ορατή σε τρίτους με τη χρήση φίλτρων οθόνης και μην την έχετε στραμμένη προς παράθυρα ή κάμερες.



Κάντε αναφορά

Αν αντιληφθείτε ύποπτη ή ασυνήθιστη δραστηριότητα σε κάποια συσκευή που χρησιμοποιείτε για τηλεργασία, επικοινωνήστε αμέσως με τον εργοδότη σας.



Μείνετε σε επαγρύπνηση

Προσέξτε για οποιαδήποτε ύποπτη κίνηση και αιτήματα, ειδικά για οικονομικά θέματα. Θα μπορούσε να είναι απάτη CEO! Σε περίπτωση αμφιβολίας, καλέστε τον ενδιαφερόμενο για επιβεβαίωση. Μην κάνετε κλικ σε συνδέσμους ή συνημμένα σε ανεπιθύμητα μηνύματα και μηνύματα κειμένου.



Αποφύγετε την παροχή προσωπικών πληροφοριών

Ποτέ μην δίνετε τα προσωπικά σας στοιχεία όταν απαντάτε σε μηνύματα, ακόμη και αν ισχυρίζονται ότι είναι από νόμιμη επιχείρηση. Αντί αυτού, επικοινωνήστε απευθείας με την επιχείρηση για επιβεβαίωση.



Αποκτήστε νέες συνήθειες

Συζητάτε τα σχέδια εργασίας με τον προϊστάμενό σας και τα άλλα μέλη της ομάδας κατά τη διάρκεια τηλεσυνεργασίας, συμπεριλαμβανομένου της κατανομής των καθηκόντων, της προθεσμίας των εργασιών και των τρόπων επικοινωνίας.



Χρήση προσωπικών συσκευών

Εάν η χρήση της προσωπικής σας συσκευής είναι η μόνη επιλογή και ο εργοδότης σας το επιτρέπει, βεβαιωθείτε ότι το λειτουργικό σύστημα και το λογισμικό της είναι ενημερωμένα, συμπεριλαμβανομένου του antivirus/ antimalware και ότι για εξ' αποστάσεως εργασία είστε συνδεδεμένοι πάντα μέσω του VPN της εταιρείας σας.



Διαχωρίστε τη δουλειά από τον ελεύθερο χρόνο σας

Αποφεύγετε την χρήση της συσκευής τηλεργασίας σας για προσωπικά θέματα.