Σε περίπτωση συμβάντος κυβερνοεπίθεσης

- Αφαιρέστε **άμεσα** τον υπολογιστή από το δίκτυο για αποφυγή μετάδοσης του κακόβουλου λογισμικού στο υπόλοιπο δίκτυο.
- Αφαιρέστε άμεσα περιφερειακές συσκευές που φυλάσσουν δεδομένα όπως USB Flash Drives, External Disks και άλλα.
- **ΜΗΝ** διαγράψετε οποιοδήποτε αρχείο από τον υπολογιστή καθώς πιθανόν να διαγράψετε την μοναδική μαρτυρία που θα έχουν οι ανακριτές στην διάθεση τους.
- **ΜΗΝ** έρχεστε ποτέ σε επαφή με τους εγκληματίες και ούτε να αποστέλλετε χρήματα σε αυτούς.
- Ειδοποιήστε άμεσα το Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος στο τηλ. 22808200 ή καταχωρίστε το παράπονο σας μέσω της ιστοσελίδας της Αστυνομίας.

Αρχηγείο Αστυνομίας

Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος

Επικοινωνία

Τηλέφωνο: +357 22808200
Φαξ: +357 22808465
Ηλεκτρονικό ταχυδρομείο:
cybercrime@police.gov.cy
Web: www.police.gov.cy

Αρχηγείο Αστυνομίας
Οδός Αντιστράτηγου Ευάγγελου Φλωράκη, τ.κ.1478
Λευκωσία - Κύπρος

ΤΑΜΕΙΑ ΕΣΩΤΕΡΙΚΩΝ ΥΠΟΘΕΣΕΩΝ
ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
Διαχείριση Ευρωπαϊκών Έργων

ΔΡΑΣΗ ΣΥΓΧΡΗΜΑΤΟΔΟΤΟΥΜΕΝΗ ΑΠΟ ΤΟ ΤΑΜΕΙΟ ΕΣΩΤΕΡΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Βρείτε μας:

www.cypruspolicenews.com | www.facebook.com/cypolice | www.twitter.com/Cyprus_Police

Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος

Αστυνομία Κύπρου

ΒΑΣΙΚΕΣ ΣΥΜΒΟΥΛΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οδηγός Επιχειρήσεων

Βασικές Συμβουλές Κυβερνοασφάλειας των Επιχειρήσεων

Οι απειλές που σχετίζονται με την κυβερνοασφάλεια είναι αληθινές και οι επιχειρήσεις πρέπει να υλοποιήσουν τις καλύτερες πρακτικές και πολιτικές για να προστατέψουν τις ίδιες, τους πελάτες τους και τα δεδομένα τους.

- ***Εκπαίδευση του προσωπικού.*** Δημιουργήστε απλές πρακτικές και πολιτικές ασφάλειας για τους υπαλλήλους, όπως τη χρήση ισχυρών κωδικών πρόσβασης και πολιτικές χρήσης του διαδικτύου.

- ***Προστασία υπολογιστών και δικτύων από κυβερνοεπιθέσεις***. Οι υπολογιστές θα πρέπει να είναι πάντοτε ενημερωμένοι με λογισμικά κατά των ιών, και λειτουργικά συστήματα. Η αυτόματη ενημέρωση των λογισμικών θα πρέπει πάντα να είναι ενεργή.

- ***Η σύνδεση στο Διαδίκτυο θα πρέπει να είναι πάντα πίσω από τείχος ασφαλείας (Firewall).*** Firewall είναι το σύνολο των προγραμμάτων που αποτρέπουν άτομα εκτός της επιχείρησης να αποκτούν πρόσβαση σε δεδομένα του ιδιωτικού δικτύου της επιχείρησης.

- ***Δημιουργία αντιγράφων ασφαλείας των σημαντικών δεδομένων.(Backup)***

"Η καλύτερη πρακτική για επιχειρήσεις είναι όπως γίνονται σε τακτικά χρονικά διαστήματα αντίγραφα ασφαλείας. Τα αντίγραφα ασφαλείας να φυλάσσονται σε χώρο εκτός της επιχείρησης"

- ***Έλεγχος της φυσικής πρόσβασης στους υπολογιστές***. Απαγορεύεται η χρήση των υπολογιστών από μη εξουσιοδοτημένα άτομα.

- ***Ασφαλίστε τα ασύρματα δίκτυα (Wi-Fi).*** Τα ασύρματά δίκτυα θα πρέπει να μένουν κρυφά και ασφαλισμένα.

- ***Χρησιμοποιείτε προσεκτικά τους διαδικτυακούς τόπους κοινωνικής δικτύωσης***. Εάν θεωρείτε σκόπιμο τοποθετήστε φραγή πρόσβασης σε αυτούς.

- ***Σταματήστε τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου***. Μην ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου και επισυναπτόμενα αρχεία που προέρχονται από άγνωστους αποστολείς.

Προστατέψτε πληροφορίες Επιχειρηματικού χαρακτήρα εκτός της επιχείρησής σας

- Βεβαιωθείτε ότι διατηρείτε τις ευαίσθητες πληροφορίες ασφαλείς: Όταν βρίσκεστε εκτός της επιχείρησης σας, διασφαλίστε ότι οι ευαίσθητες πληροφορίες και ο σχετικός εξοπλισμός είναι ασφαλείς και δεν διατρέχουν κίνδυνο κλοπής ή απώλειας.

- Διατηρήστε τις πληροφορίες που αφορούν την επιχείρησή σας εμπιστευτικές: Μην γνωστοποιείτε εμπιστευτικές πληροφορίες που αφορούν την επιχείρησή σας.

- Χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο με σύνεση: Ο κύριος όγκος κακόβουλων λογισμικών (malware, cryptolocker) προέρχεται από μηνύματα ηλεκτρονικού ταχυδρομείου.