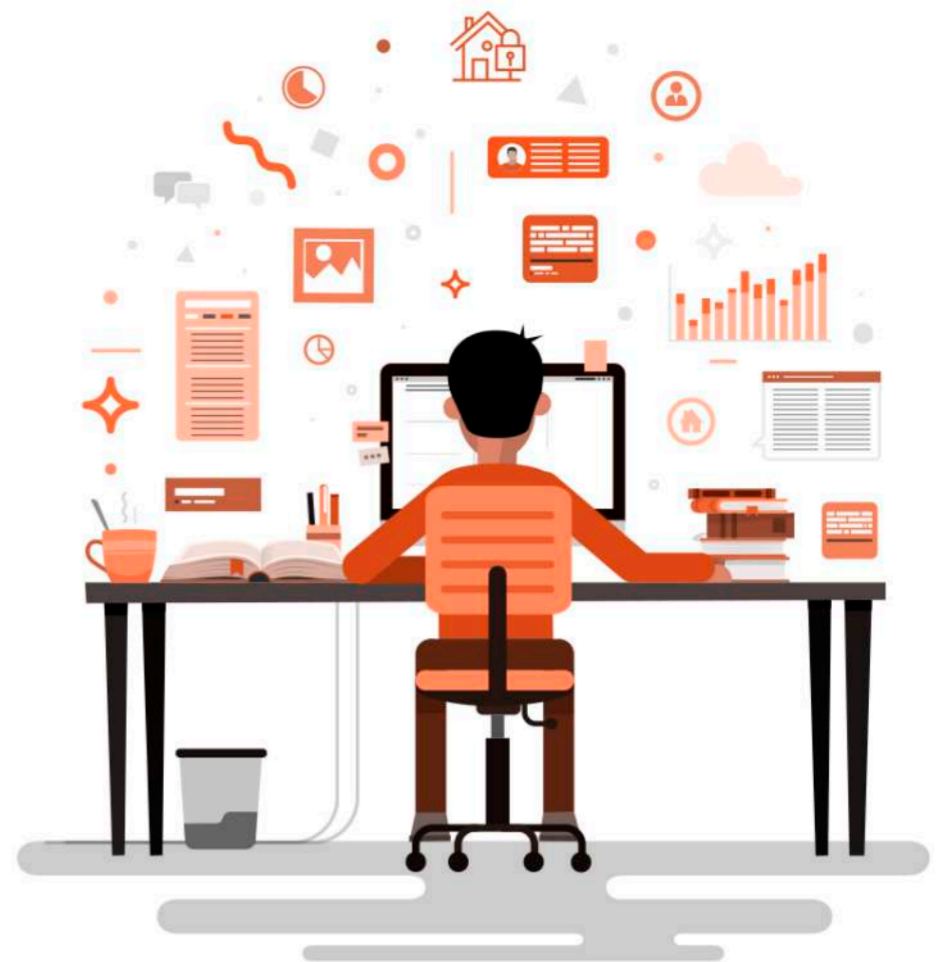


safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

Μένουμε σπίτι. Εργαζόμαστε με ασφάλεια.

Για εργαζόμενους



- Χρησιμοποιείτε τις προσωπικές σας συσκευές ή τις συσκευές που σας παρέχει η εταιρεία / ο φορέας σας. Σε κάθε περίπτωση, σιγουρευτείτε ότι το λειτουργικό σύστημα και οι εφαρμογές σας είναι ενημερωμένες, ότι έχετε εγκαταστήσει τα κατάλληλα αντιϊικά προγράμματα και ότι η σύνδεση σας στο διαδίκτυο είναι ασφαλής.
- Αποφεύγετε να κάνετε προσωπική χρήση τυχόν εξοπλισμού που σας έχει παρασχεθεί από την εταιρεία / τον φορέα σας στο πλαίσιο της Τηλεργασίας.
- Στην περίπτωση που η εταιρεία / ο φορέας σας, σας έχει προμηθεύσει με σχετικό εξοπλισμό (π.χ. φορητό Η/Υ), μην αφήνετε τα μέλη της οικογένειάς σας να αποκτούν πρόσβαση σε αυτόν. Κλειδώνετε ή απενεργοποιείτε τον εξοπλισμό, όταν δεν είστε παρόντες και κρατάτε τον σε ασφαλή τοποθεσία για να αποτρέψετε τυχόν απώλεια, βλάβη από άσκοπη χρήση ή κλοπή.
- Χρησιμοποιείτε δυνατούς κωδικούς (αν είναι εφικτό password managers ή two-step verification).
- Πριν ξεκινήσετε να δουλεύετε μέσω Τηλεργασίας εξοικειωθείτε με τις εταιρικές / υπηρεσιακές διαδικασίες και πολιτικές.
- Στην περίπτωση που χρειαστεί να συνδεθείτε με το εταιρικό δίκτυο ή το εσωτερικό δίκτυο του φορέα σας να χρησιμοποιείτε, εφόσον υπάρχει τέτοια δυνατότητα, VPN, σύμφωνα με τις οδηγίες που θα σας παράσχει το εξειδικευμένο προσωπικό της εταιρείας / του φορέα σας.
- Εάν εντοπίσετε ασυνήθιστη ή ύποπτη δραστηριότητα σε οποιαδήποτε συσκευή χρησιμοποιείτε για την Τηλεργασία, επικοινωνήστε άμεσα με την εταιρεία / τον φορέα σας μέσω των ενδεδειγμένων καναλιών.
- Μείνετε σε επαγρύπνηση για οποιαδήποτε ύποπτη δραστηριότητα, ειδικά για αιτήματα που αφορούν οικονομικές συναλλαγές ακόμα και εάν φαίνονται να προέρχονται από άτομα που γνωρίζετε. Αυτό μπορεί να αποτελεί μία ακόμα περίπτωση κυβερνοαπάτης (cyberfraud). Επαληθεύετε και διασταυρώνετε οποιοδήποτε παρόμοιο μήνυμα / αίτημα.
- Μην ανοίγετε συνδέσμους ή επισυναπτόμενα αρχεία που λαμβάνετε από μηνύματα ηλεκτρονικού ταχυδρομείου από αποστολείς που δεν γνωρίζετε.
- Μην δίνετε προσωπικές πληροφορίες ή κωδικούς πρόσβασης, ακόμα και εάν φαίνεται με την πρώτη ματιά, να σας τα ζητούν νόμιμες εταιρείες / γνωστοί εθνικοί ή διεθνείς φορείς. Κανένας δημόσιος Οργανισμός (Ε.Ο.Δ.Υ., Υπουργείο Υγείας, Ο.Α.Ε.Δ., Παγκόσμιος Οργανισμός Υγείας κ.α.) ή ιδιωτικός φορέας (τράπεζες, τηλεπικοινωνιακοί πάροχοι κ.α.) δεν πρόκειται να σας ζητήσει ποτέ προσωπικούς κωδικούς πρόσβασης.
- Επαληθεύετε και διασταυρώνετε με οποιονδήποτε πρόσφορο τρόπο τη γνησιότητα των ηλεκτρονικών μηνυμάτων που λαμβάνετε και σας ζητούν να κλικάρετε ηλεκτρονικούς συνδέσμους (links) ή να μοιραστείτε κωδικούς πρόσβασης και άλλες προσωπικές σας πληροφορίες.
- Δημιουργήστε συγκεκριμένο πλάνο συνεργασίας με τα υπόλοιπα μέλη των ομάδων εργασίας για την περίοδο που θα δουλεύετε μέσω Τηλεργασίας, όπως τον τρόπο που θα ανατίθενται οι επιμέρους υποχρεώσεις για κάθε έργο / παραδοτέο, θα τηρούνται οι προθεσμίες, θα αξιολογείται η απόδοση και θα αξιοποιούνται τα διαθέσιμα κανάλια επικοινωνίας.



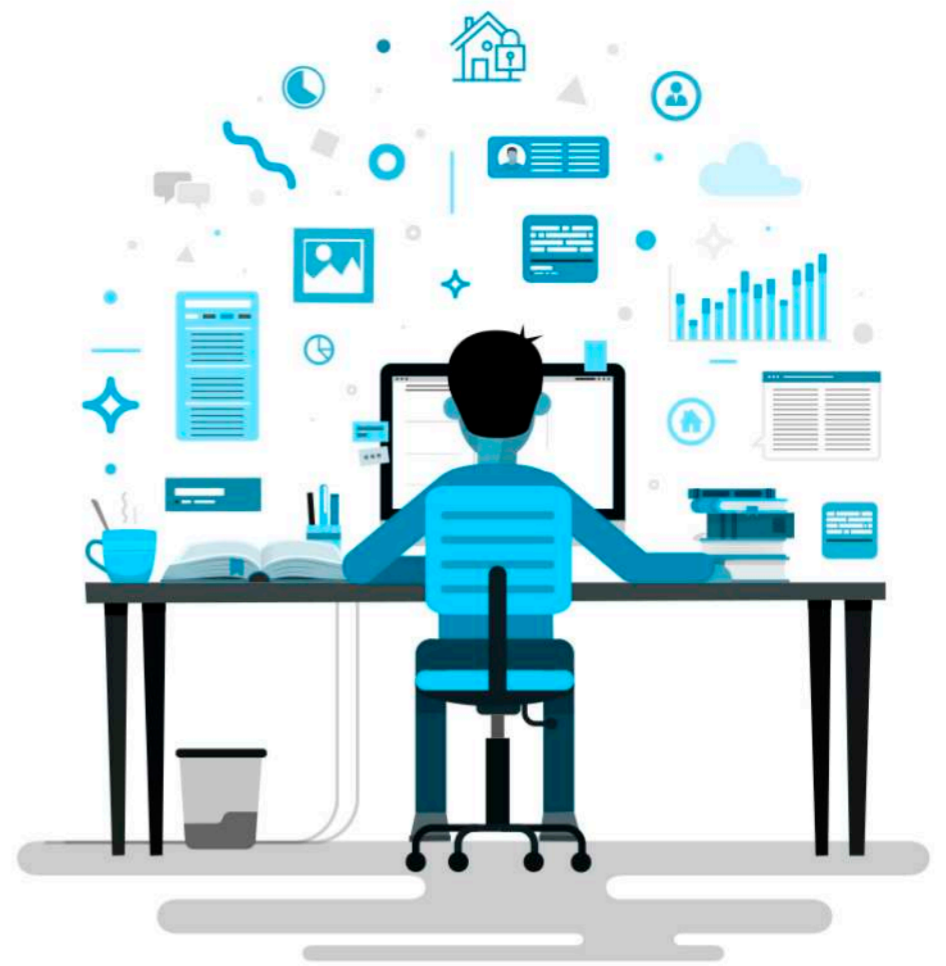
safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

Μένουμε σπίτι. Εργαζόμαστε με ασφάλεια.

Για εργοδότες

- Δημιουργήστε εσωτερικές πολιτικές και διαδικασίες και κάντε δοκιμές (tests) πριν τεθούν σε επιχειρησιακή λειτουργία. Είναι σημαντικό να έχετε ξεκάθαρες πολιτικές για την πρόσβαση σε εσωτερικές δομές / συστήματα καθώς και για το ποιος θα πρέπει να κληθεί σε περίπτωση προβλήματος. Δημιουργήστε ξεκάθαρες διαδικασίες για την αντιμετώπιση ενός περιστατικού ασφαλείας. Να λαμβάνετε επιπλέον μέτρα όταν πρόκειται για διαδικασία έγκρισης και υπογραφής εγγράφων από τη Διοίκηση.
- Λαμβάνετε περισσότερα μέτρα ασφαλείας, όπως ενδεικτικά, κρυπτογράφηση σκληρών δίσκων, αποσύνδεση ανενεργών χρηστών, προστασία ιδιωτικότητας οθόνης από τρίτους, ισχυρή αυθεντικοποίηση και έλεγχος των φορητών μέσων αποθήκευσης. Δημιουργήστε διαδικασίες εξ αποστάσεως απενεργοποίησης πρόσβασης σε συσκευές που χάθηκαν ή κλάπηκαν.
- Εφόσον τούτο είναι εφικτό, να επιτρέπετε στους εργαζόμενους σας να συνδέονται στο εσωτερικό δίκτυο μόνο μέσω του εταιρικού VPN με έλεγχο πολλαπλών παραγόντων. Βεβαιωθείτε ότι οι συνδέσεις με το εσωτερικό δίκτυο / συστήματα έχουν ρυθμιστεί και λήγουν αυτόματα μετά από μια περίοδο που ο χρήστης είναι ανενεργός, με απαίτηση νέας αυθεντικοποίησης για την εκ νέου σύνδεση.
- Διατηρείτε το λειτουργικό σύστημα και τις εφαρμογές των συσκευών ενημερωμένες μειώνοντας τις αδυναμίες των συστημάτων που θα μπορούσαν να εκμεταλλευτούν κακόβουλοι χρήστες.
- Ασφαλίζετε τα κανάλια επικοινωνίας εφαρμόζοντας έλεγχο παραγόντων δύο σημείων για την είσοδο στους λογαριασμούς ηλεκτρονικού ταχυδρομείου των εργαζομένων σας.
- Εδραιώνετε ασφαλείς επικοινωνίες μεταξύ των υπαλλήλων, αλλά και με εξωτερικούς συνεργάτες ή προμηθευτές.
- Ελέγχετε συχνά στο VPN για ασυνήθιστη δραστηριότητα χρηστών.
- Επικοινωνείτε τακτικά με το προσωπικό θέτοντας ρεαλιστικούς στόχους και χρονοδιαγράμματα, όπως και μηχανισμούς επιτήρησης αυτών, λαμβάνοντας υπόψη τις ιδιαίτερες καταστάσεις της εποχής.
- Ενημερώνετε - εκπαιδεύετε τους εργαζομένους σας για την πολιτική της Τηλεργασίας και τους κινδύνους από επιθέσεις στον κυβερνοχώρο και ειδικότερα για τη μέθοδο αλίευσης δεδομένων και κωδικών πρόσβασης τύπου "phishing", καθώς και για τη μέθοδο της κοινωνικής μηχανικής (social engineering).



safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

**Μένουμε σπίτι.
Εργαζόμαστε με ασφάλεια.**



Για εργαζόμενους

safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

**Μένουμε σπίτι.
Εργαζόμαστε με ασφάλεια.**



Για εργοδότες



ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ



CYBER
CRIME
DIVISION

ΔΙΩΣΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

safe@home

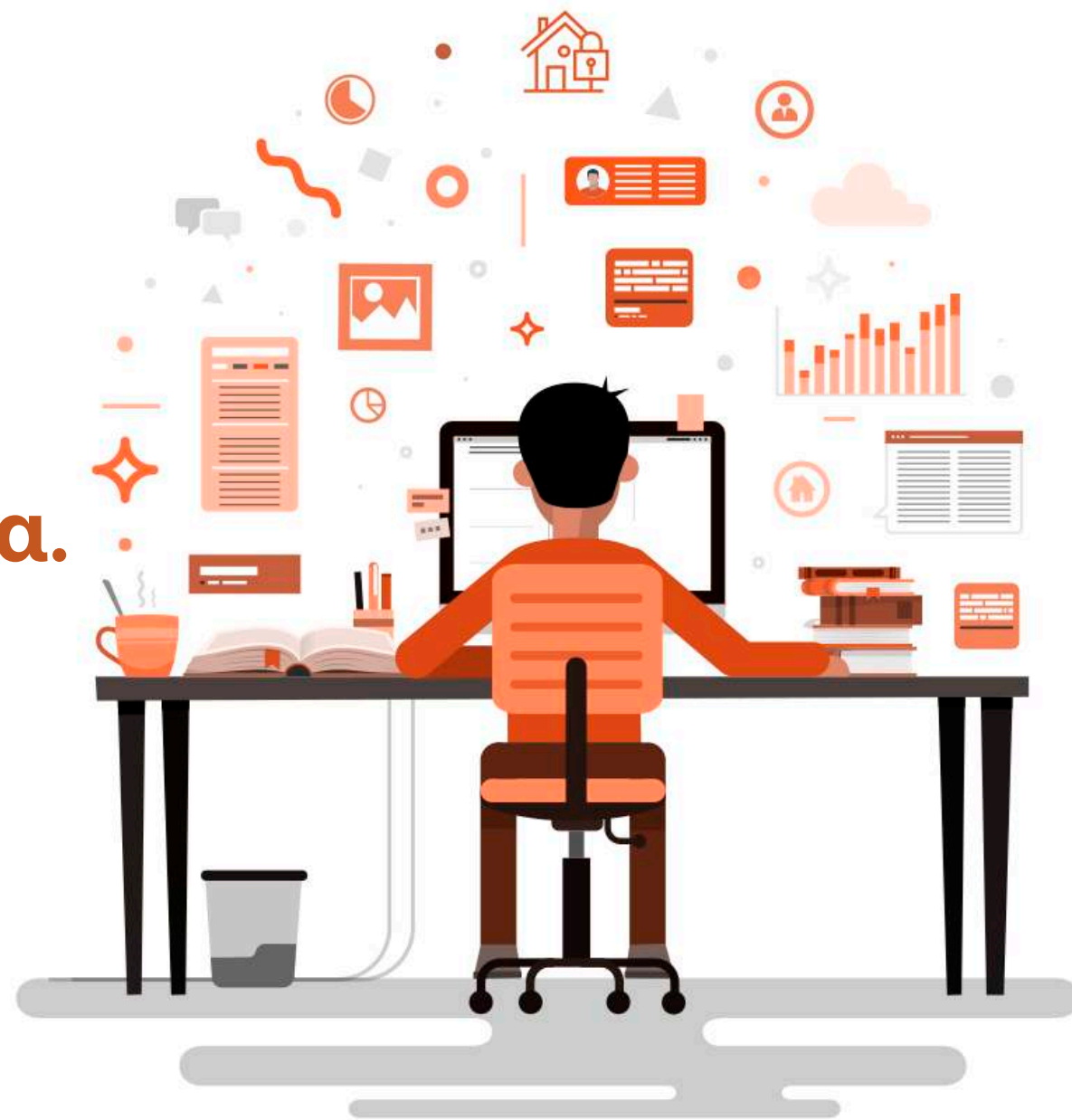
ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

Μένουμε σπίτι.
Εργαζόμαστε με ασφάλεια.

Για εργαζόμενους


ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ


CYBER
CRIME
DIVISION
ΔΙΩΣΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ



Ενημερωθείτε εδώ ►

safe@home

ΟΔΗΓΟΣ ΑΣΦΑΛΟΥΣ ΤΗΛΕΡΓΑΣΙΑΣ
από την Ε.Α.Δ. και την ΕΛ.ΑΣ. / ΔΙ.Δ.Η.Ε.

Μένουμε σπίτι.
Εργαζόμαστε με ασφάλεια.

Για εργοδότες

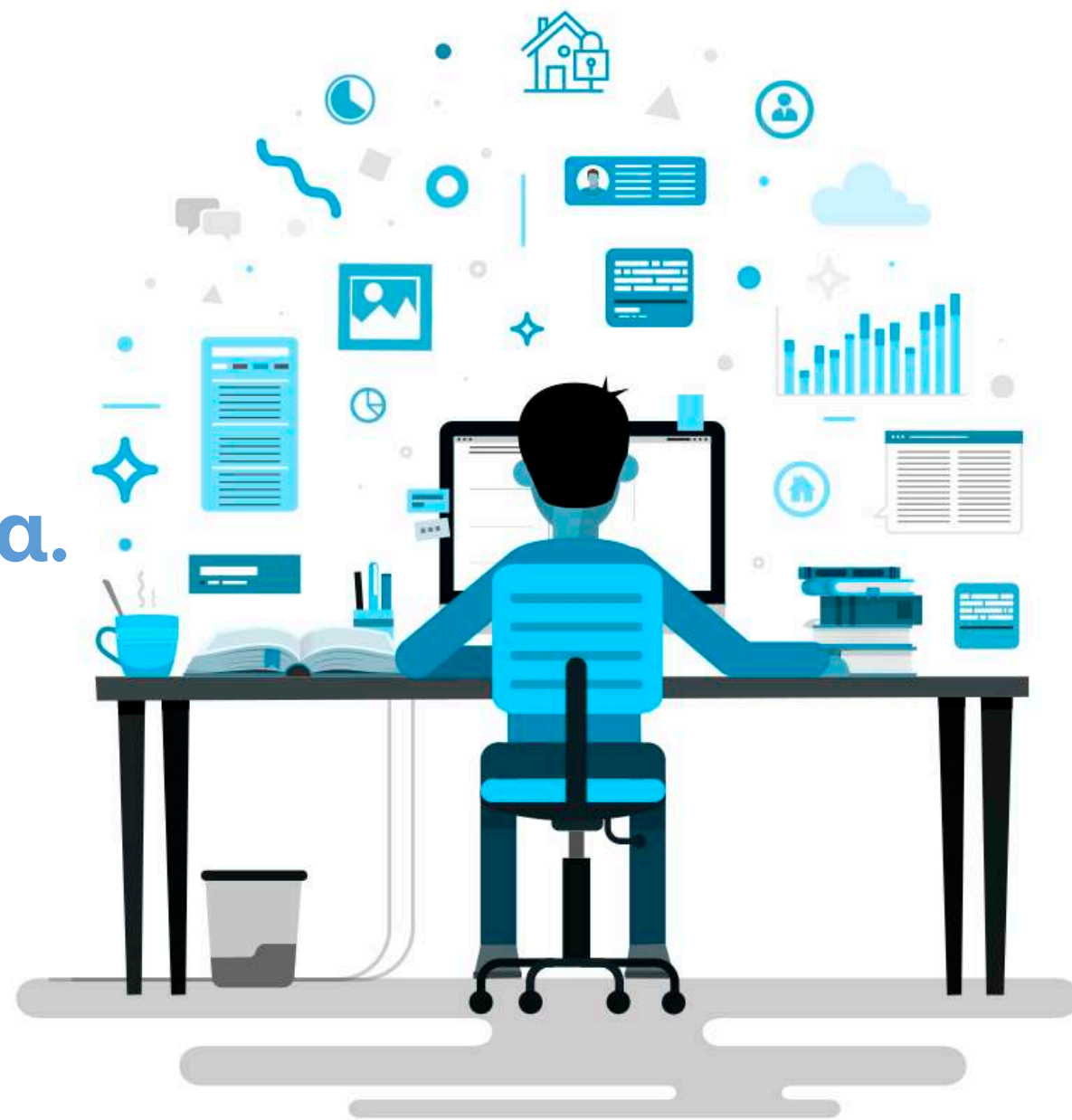


ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ



CYBER
CRIME
DIVISION

ΔΙΩΣΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ



Ενημερωθείτε εδώ ►