Microsoft Word-6

Κεφάλαιο10-Επεξεργασία Κειμένου
MS Word
Πηγή: https://saferinternet4kids.gr/nea/digitalidentity/

Δραστηριότητα1

Στο παρακάτω κείμενο, εφαρμόστε γραμματοσειρά Arial, μέγεθος 16 στιγμές, με στυλ έντονο και πλάγιο

Πώς μπορούμε να προστατέψουμε την ψηφιακή μας ταυτότητα

Δραστηριότητα2

Στο παρακάτω κείμενο, εφαρμόστε γραμματοσειρά Verdana, διπλή υπογράμμιση και χρώμα μπλε.

Η κλασική έννοια της ταυτότητας ορίζεται μέσω των εξωτερικών γνωρισμάτων μας όπως είναι τα βιομετρικά χαρακτηριστικά μας (χρώμα ματιών, δακτυλικά αποτυπώματα κ.α), το όνομά μας, την ημερομηνία γέννησής μας, την υπογραφή μας.

Δραστηριότητα3

Στο παρακάτω κείμενο, εφαρμόστε πλήρη στοίχιση, γραμματοσειρά Comic Sans MS, μέγεθος 10 στιγμές και χρώμα κόκκινο.

Η διαδικτυακή μας ταυτότητα έχει πιο δυναμικό χαρακτήρα και προκύπτει κυρίως από τα ψηφιακά μας αποτυπώματα: τους διαδικτυακούς φίλους μας, το τι κοινοποιούμε, την εικόνα που προβάλλουμε για τον εαυτό μας. Αν κάποιος υποκλέψει τους κωδικούς μας αυτομάτως μπορεί να γίνει «εμείς» οπότε η προστασία της ψηφιακής μας ταυτότητας είναι βαρύνουσας σημασίας στο διαδίκτυο.

Δραστηριότητα4

Στο παρακάτω κείμενο, εφαρμόστε στην πρώτη γραμμή, γραμματοσειρά Tahoma, μέγεθος 15 στιγμές, χρώμα Ώχρα και έντονη γραφή. Στις υπόλοιπες γραμμές εφαρμόστε γραμματοσειρά Tahoma, μέγεθος 13 στιγμές και πλάγια γραφή. Χωρίστε σε 2 παραγράφους το κείμενο.

Ισχυροί κωδικοί πρόσβασης παντού:
Η δημιουργία ισχυρών κωδικών πρόσβασης, διαφορετικό για κάθε λογαριασμό που χρησιμοποιείτε είναι ένα πολύ σημαντικό βήμα. Ένας ισχυρός κωδικός πρόσβασης περιλαμβάνει τουλάχιστον 8 χαρακτήρες γράμματα, αριθμούς και σύμβολα, είναι εύκολος στο να τον θυμάστε εσείς και δύσκολος για τους άλλους να τον μαντέψουν. Για ακόμα μεγαλύτερη προστασία μπορείτε να χρησιμοποιήσετε έλεγχο ταυτότητας πολλαπλών παραγόντων (2 Factor Authentication) ο οποίος θα ενισχύσει τους διαδικτυακούς λογαριασμούς σας ενεργοποιώντας τα ισχυρότερα διαθέσιμα εργαλεία ελέγχου ταυτότητας όπως βιομετρικά στοιχεία ή έναν κωδικό μιας χρήσης που αποστέλλεται στο τηλέφωνό σας. Έναν αναλυτικό οδηγό μπορείτε να διαβάσετε εδώ. Για να δημιουργήσετε και να θυμηθείτε διαφορετικούς, σύνθετους κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς σας μπορείτε να χρησιμοποιήσετε password manager. Αυτή η λύση ενδείκνυται κυρίως για προχωρημένους χρήστες που έχουν να διαχειριστούν πολλούς διαφορετικούς κωδικούς και έχουν διαδικτυακή δραστηριότητα που μπορεί να προσελκύσει χάκερς.

Δραστηριότητα5

Στο παρακάτω κείμενο, διορθώστε τα λάθη και αφαιρέστε το έντονο και πλάγιο στυλ.

Διατηρήστε τη συσκευή σας «καθαρή»:
Εγκαταστήστε **antivirus** σε όλες τις σισκευές σας και φροντιστε να το ανανεώνεται τακτικά με τις νεοτερες εκδωσεις. Με αυτόν τον τροπο προστατεύεστε από τον **συχνοτερο** κίνδυνο που υπαρχει, να προσβλιθεί η σησκευή σας από κάποιο **κακόβουλο** λογεισμικό. Τα διάφορα antivirus *διαφέρουν* σε ότι αφορά τις *μεθόδους* τους, ωστωσο όλα έχουν τον ίδιο στοχο: *να προστατέψουν τις συσκευές σας*.

Δραστηριότητα6

Στους παρακάτω τύπους, εφαρμόστε στον αριθμό 3 το εφέ δείκτη και στον αριθμό 2 το εφέ εκθέτη. Έπειτα μέσω internet βρείτε πληροφορίες για τον τύπο e=m*c2 και αντιγράψτε το κείμενο που θα βρείτε μέσα στο πλαίσιο. Χρησιμοποιήστε το πινέλο μορφοποίησης και διαμορφώστε το κείμενο σας σύμφωνα με την λέξη: ***Αϊνστάιν***

CO3

e=m*c2

Δραστηριότητα7

Στο παρακάτω κείμενο, κάντε όλα τα γράμματα κεφαλαία

Σκεφτείτε πριν ανοίξετε οποιοδήποτε link σας έχει αποσταλεί

Δραστηριότητα8

Στο παρακάτω κείμενο, εφαρμόστε εναλλαγή πεζών – κεφαλαίων

ΕΆν λάβΕΤΕ μια δελΕΑΣΤΙκή ΠΡΟΣφορά μέΣω ηλεΚΤΡΟνικού ταχΥΔΡΟμείου ή μΈσω μηνύματος, μη ΒΙΑστείτε να ΑΝΟΊξετε το σύνδΕΣΜΟ