Οδηγίες Ασφαλούς Εξ Αποστάσεως Εκπαίδευσης

6ο ΠΕ.Κ.Ε.Σ. ΑΤΤΙΚΗΣ

Περιεχόμενα

1. Γενικές Οδηγίες 3
2. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR) 3
3. Προστασία Προσωπικών Δεδομένων 4
4. Δημιουργία ισχυρού κωδικού πρόσβασης 5
5. Αλληλογραφία σε τρίτους - Κρυφή Κοινοποίηση 6
6. Θάμπωμα φόντου σε βιντεοκλήσεις 7
7. Ασφαλές YouTube 8
8. Η μηχανή αναζήτησης Junior Safe Search 10
9. Πηγές 10

6ο ΠΕ.Κ.Ε.Σ. ΑΤΤΙΚΗΣ

1. Γενικές Οδηγίες

ΠΗΓΗ: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ) της Ελληνικής Αστυνομίας

1) Ενημερώνουμε τα λειτουργικά συστήματα και τις εφαρμογές των συσκευών και εγκαθιστούμε κατάλληλα αντιϊκά (antivirus) προγράμματα.
2) Χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης (εάν είναι εφικτό password managers ή two step verification).
3) Είμαστε προσεκτικοί στη χρήση των συσκευών που χρησιμοποιούμε για εκπαίδευση εξ αποστάσεως, ώστε να μην εγκατασταθούν σε αυτές κακόβουλα προγράμματα.
4) Αποφεύγουμε να δώσουμε προσωπικές πληροφορίες μέσω διαδικτύου, όπως διεύθυνση κατοικίας, τη διαρρύθμισή της κ.α.
5) Όταν χρησιμοποιούμε την κάμερα του υπολογιστή προσέχουμε να μην εμφανίζονται οι χώροι του σπιτιού μας, καθώς και περιουσιακά στοιχεία δηλωτικά της οικονομικής μας κατάστασης.
6) Αναφέρουμε άμεσα τυχόν παραβίαση του λογαριασμού μας και οποιαδήποτε άλλη ύποπτη δραστηριότητα (Τηλ. 11188 – Cyber Alert, Δίωξη Ηλεκτρονικού Εγκλήματος).

2. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)

ΠΗΓΗ: Ελληνικό Κέντρο Ασφαλούς Διαδικτύου

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων, γνωστός και ως General Data Protection Regulation (GDPR), προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Ο όρος «επεξεργασία» καλύπτει ένα ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Χαρακτηριστικά παραδείγματα δεδομένων προσωπικού χαρακτήρα είναι: α) όνομα και επώνυμο, β) διεύθυνση κατοικίας, γ) ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com, δ) δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο).

Χαρακτηριστικά παραδείγματα ευαίσθητων προσωπικών δεδομένων είναι όσα αφορούν σε: α) φυλετική ή εθνική προέλευση, β) πολιτικά φρονήματα, γ) θρησκευτικές ή φιλοσοφικές

ΘΠΕΚΕΣ ΑΤΤΙΚΗΣ

πεποιθήσεις, δ) συμμετοχή σε συνδικαλιστική οργάνωση, ε) υγεία, στ) κοινωνική πρόνοια, ζ) ερωτική ζωή, και η) πληροφορίες για ποινικές διώξεις ή καταδίκες.

Ο GDPR καθορίζει σε ποιες περιπτώσεις επιτρέπεται να χρησιμοποιούνται, αποθηκεύονται, διαγράφονται, μεταβιβάζονται και εν γένει επεξεργάζονται τα προσωπικά μας δεδομένα και κυρίως, με ποιον τρόπο μπορούμε να τα προστατεύουμε. Ο GDPR επηρεάζει κάθε οργανισμό στην Ευρώπη, ο οποίος διαχειρίζεται με οποιονδήποτε τρόπο προσωπικά δεδομένα, αλλά και κάθε εταιρεία που συναλλάσσεται στην επικράτεια της Ευρωπαϊκής Ένωσης. Οι κανόνες είναι πολύπλοκοι και τα πρόστιμα για μη συμμόρφωση πολύ αυστηρά και μπορούν να φτάσουν έως τα 20 εκατομμύρια ευρώ. Οι βασικές αλλαγές που θα πρέπει να γνωρίζουν οι εκπαιδευτικοί είναι:

- Προστασία των δικαιωμάτων των παιδιών: Το τοπίο στα social media αλλάζει. Βάσει του νέου κανονισμού απαγορεύεται τη χρήση των social media σε παιδιά έως 16 ετών παρά μόνο με τη συγκατάθεση των γονέων. Στην Ελλάδα ως ηλικία ψηφιακής συναίνεσης έχουν οριστεί τα 15 έτη.
- Δικαίωμα στη λήθη: Ο χρήστης έχει το δικαίωμα να ζητήσει τη διαγραφή των δεδομένων του και ο υπεύθυνος επεξεργασίας έχει υποχρέωση άμεσα να τα διαγράψει και, αν τα έχει δημοσιοποιήσει, να ενημερώσει και όλους τους άλλους που τα έχουν αναδημοσιεύσει ότι έχει ζητηθεί η διαγραφή τους.
- Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα: Ο χρήστης έχει περισσότερη και σαφέστερη ενημέρωση κατά τη συλλογή των δεδομένων του για την επεξεργασία τους και το δικαίωμα πρόσβασης σε αυτά.
- Δικαίωμα διόρθωσης: Ο χρήστης έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών στοιχείων καθώς και τη συμπλήρωση ελλιπών δεδομένων που τον αφορούν.
- Δικαίωμα εναντίωσης στην επεξεργασία: Ο χρήστης έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των δεδομένων του υπό συγκεκριμένες προϋποθέσεις, ιδίως όταν πρόκειται για κατάρτιση «προφίλ» ή για σκοπούς απευθείας εμπορικής προώθησης.

Η ρυθμιστική αρχή στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία λειτουργεί ως μια συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή. Η διενέργεια διοικητικών ελέγχων καθώς και η εξέταση σχετικών καταγγελιών, προσφυγών και ερωτημάτων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων, όταν αυτά θίγονται από την επεξεργασία δεδομένων, περιλαμβάνονται μεταξύ των ελεγκτικών αρμοδιοτήτων της Αρχής.

3. Προστασία Προσωπικών Δεδομένων

ΠΗΓΗ: Ελληνικό Κέντρο Ασφαλούς Διαδικτύου

Η προστασία των προσωπικών δεδομένων είναι σημαντική γιατί δεν ξέρουμε ποτέ πώς θα χρησιμοποιηθούν οι ιδιωτικές μας πληροφορίες αν βρεθούν σε λάθος χέρια. Διαφυλάσσοντας τα προσωπικά μας δεδομένα και αυτά των μαθητών μας προστατεύουμε την ιδιωτικότητά μας που είναι πολύτιμη.

Συχνά, οι εκπαιδευτικοί κοινοποιούν εικόνες από την εκπαιδευτική διαδικασία στην ιστοσελίδα του σχολείου ή σε προσωπικούς τους λογαριασμούς στα μέσα κοινωνικής δικτύωσης. Είναι σημαντικό όμως προτού αναρτήσουν οποιαδήποτε εικόνα να λαμβάνουν υπόψη τα ακόλουθα:

60 ΠΕ.Κ.Ε.Σ. ΑΤΤΙΚΗΣ

- Με ποιον τη μοιράζομαι;
- Ποιος άλλος μπορεί να τη δει;
- Εκείνοι που θα τη δουν τι θα μάθουν για μένα;
- Εκείνοι που θα τη δουν τι θα μάθουν για τους υπόλοιπους που απεικονίζονται στη φωτογραφία;

Πώς αλλιώς αποκαλύπτουμε προσωπικά δεδομένα χωρίς να το συνειδητοποιούμε;

- Όταν δεν έχουμε ενεργοποιήσει τις ρυθμίσεις απορρήτου στα κοινωνικά δίκτυα που χρησιμοποιούμε, ο οποιοσδήποτε έχει πρόσβαση στα προσωπικά μας δεδομένα.
- Μέσω σχολίων ή φωτογραφιών που μας αφορούν και κοινοποιούνται από τρίτους.
- Μέσω εφαρμογών που κατεβάζουμε.

Σκεφτείτε πριν αποκαλύψετε δεδομένα:

- Αν λαμβάνετε γράμματα, e-mails, μηνύματα στο κινητό ή στο Facebook που σας ζητούν πληροφορίες, μην απαντήσετε αν δεν είστε σίγουροι από ποιον προέρχονται.
- Αν σας ζητούνται δεδομένα, θα πρέπει πάντα να σκέφτεστε αν αυτό είναι δικαιολογημένο και αν απαιτείται για την πραγματοποίηση της συγκεκριμένης επικοινωνίας.

Να θυμάστε πως:

- Ό,τι αναρτούμε στο διαδίκτυο μπορεί να παραμείνει εκεί για πάντα και να έχει πρόσβαση σε αυτό το περιεχόμενο ο οποιοσδήποτε. Οπότε, είναι πολύ σημαντικό να ΣΚΕΦΤΟΜΑΣΤΕ ΔΙΠΛΑ πριν κοινοποιήσουμε το οτιδήποτε.
- Όταν επεξεργαζόμαστε δεδομένα άλλων, ακόμα και αν είναι φίλοι μας, πρέπει αντίστοιχα να έχουμε τη συγκατάθεσή τους. Για παράδειγμα, πριν ανεβάσουμε στο Facebook φωτογραφία από μια κοινωνική εκδήλωση, πρέπει να είμαστε σίγουροι ότι όλοι οι εικονιζόμενοι σε αυτήν συμφωνούν με τη δημοσίευσή της.
- Δεν πρέπει να επισκέπτεστε ιστοσελίδες που δεν θα θέλατε οι άλλοι να γνωρίζουν, όταν χρησιμοποιείτε «κοινόχρηστους» υπολογιστές.
- Πρέπει να αποσυνδέεστε από τις ιστοσελίδες, στις οποίες έχετε εισέλθει/συνδεθεί με χρήση συνθηματικών.

4. Δημιουργία ισχυρού κωδικού πρόσβασης

Αυτό που διασφαλίζει την ιδιωτικότητα και την προστασία σας στο διαδίκτυο είναι οι κωδικοί ασφαλείας. Τα πολύ εύκολα passwords μπορεί να σας διευκολύνουν γιατί τα θυμάστε εύκολα, αλλά το ίδιο εύκολα μπορεί να παραβιαστούν από τρίτους. Ακολουθούν μερικές συμβουλές για το πώς μπορείτε να δημιουργήσετε έναν ισχυρό κωδικό ασφαλείας.

- Αποφύγετε το προφανές: Δεν χρησιμοποιούμε passwords όπως «123456» ή τη λέξη «password».
- Δημιουργήστε έναν δικό σας κωδικό από μια αγαπημένη σας φράση χρησιμοποιώντας τα αρχικά των λέξεων.
- Χρησιμοποιήστε γράμματα μαζί με αριθμούς και σύμβολα.

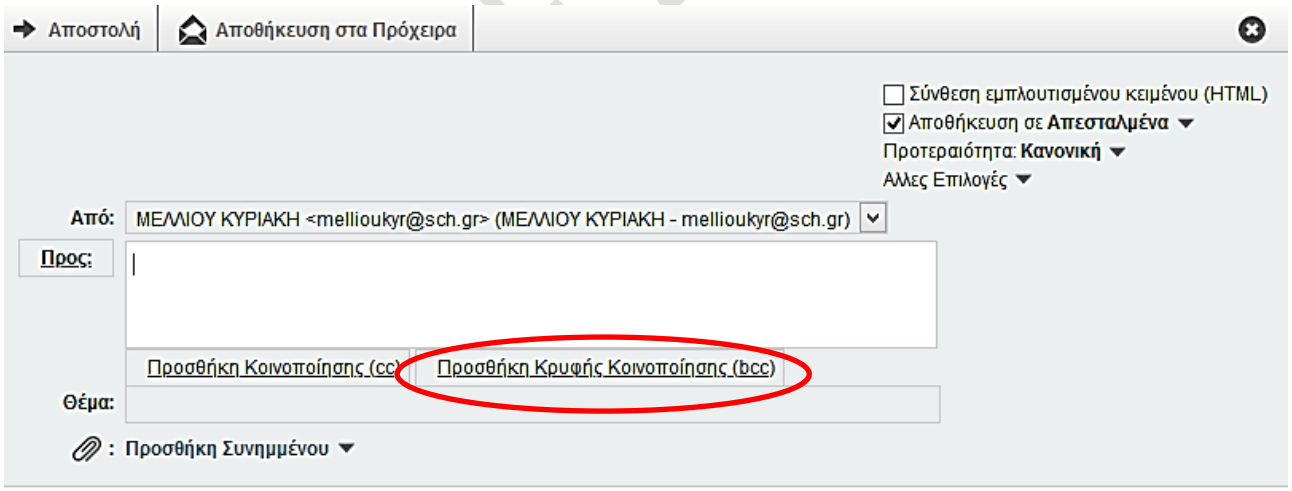
6ο ΠΕ.Κ.Ε.Σ. ΑΤΤΙΚΗΣ

- Χρησιμοποιήστε περισσότερους από 8 χαρακτήρες.
- Μη χρησιμοποιείτε λέξεις που υπάρχουν στο λεξικό.
- Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε όλους τους λογαριασμούς σας: Αν για παράδειγμα συνηθίζετε να χρησιμοποιείτε ως κωδικό το 2A468 και θέλετε να δημιουργήσετε κωδικό στο Skype, τότε μετατρέψτε τον σε «SKP» και στη συνέχεια τοποθετήστε τον κωδικό 2A468 που χρησιμοποιείτε (SKP2A468).
- Μη μένετε ποτέ συνδεδεμένοι στους λογαριασμούς σας.
- Μην εμπιστεύεστε σε κανέναν τον κωδικό ασφαλείας σας.
- Ενεργοποιήστε την επαλήθευση των δύο κινήσεων: Η επαλήθευση των δύο κινήσεων απαιτεί από όποιον την έχει ενεργοποιήσει πέρα από τον κωδικό του, να πληκτρολογήσει και τον αριθμό που θα του σταλεί σε μήνυμα στο κινητό που έχει δηλώσει.

5. Αλληλογραφία σε τρίτους - Κρυφή Κοινοποίηση

Η κρυφή κοινοποίηση που εμφανίζεται με τα αρχικά Bcc (Blind Carbon Copy) σας δίνει τη δυνατότητα να προσθέτετε παραλήπτες σε μήνυμα ηλεκτρονικού ταχυδρομείου, οι οποίοι δεν θα είναι ορατοί στους άλλους παραλήπτες που λαμβάνουν το μήνυμα.

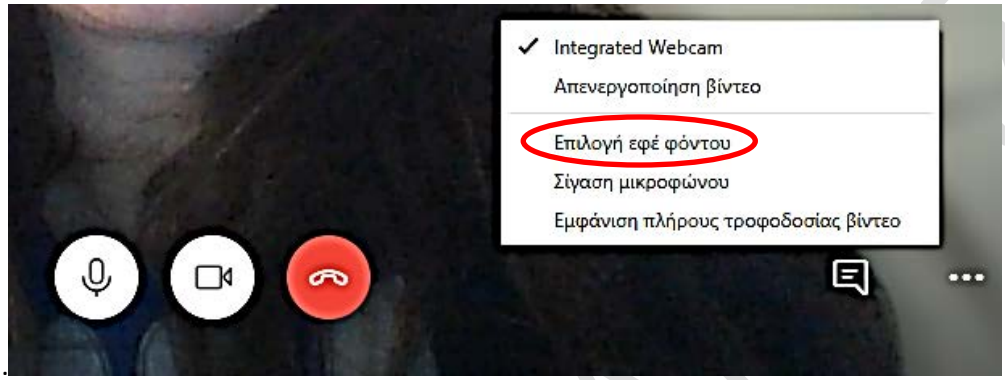
Δημιουργήστε ένα μήνυμα και στο πλαίσιο με την ένδειξη «ΠΡΟΣ» επιλέξτε το εικονίδιο «Προσθήκη Κρυφής Κοινοποίησης» (bcc) ώστε να προσθέσετε τους παραλήπτες (Εικ. 1). Μόλις ολοκληρώσετε τη διαδικασία, επιλέξτε Αποστολή.



Εικόνα 1: Πεδίο προσθήκης Κρυφής Κοινοποίησης

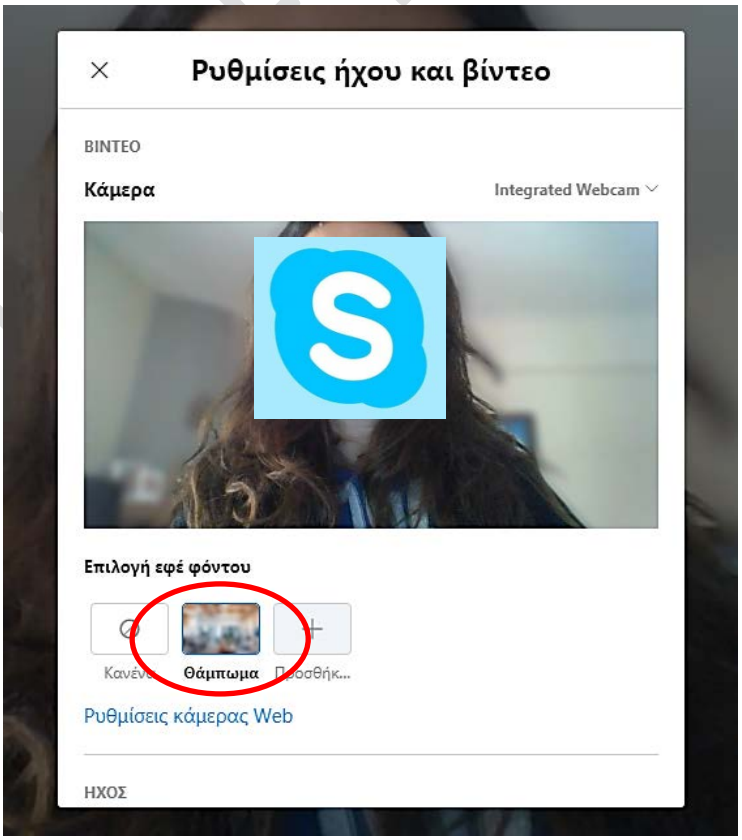
6. Θάμπωμα φόντου σε βιντεοκλήσεις

Η λειτουργία, η οποία τεχνητά θολώνει το φόντο, είναι διαθέσιμη στις ζωντανές κλήσεις βίντεο που πραγματοποιούνται μέσω Skype και Microsoft Teams. Με μια απλή εναλλαγή ή δεξί κλικ ή ακόμα και μέσω των ρυθμίσεων του λογισμικού, το φόντο σας θα είναι άμεσα θαμπωμένο. Για να το χρησιμοποιήσετε, ξεκινήστε μια κλήση βίντεο και στη συνέχεια κάντε δεξί κλικ στην οθόνη. Θα εμφανιστεί ένα αναπτυσσόμενο μενού, στο οποίο θα επιλέξετε την ενέργεια «Επιλογή εφέ φόντου» (Εικ. 2).



Εικόνα 2: Επιλογή εφέ φόντου

Κάντε κλικ στο εικονίδιο και στη συνέχεια θα εμφανιστεί το πλαίσιο «Ρυθμίσεις ήχου και βίντεο» από το οποίο θα επιλέξετε το «Θάμπωμα» (Εικ. 3). Για να απενεργοποιήσετε την επιλογή σας, κλικάρετε εκ νέου πάνω στην επιλογή «Θάμπωμα».



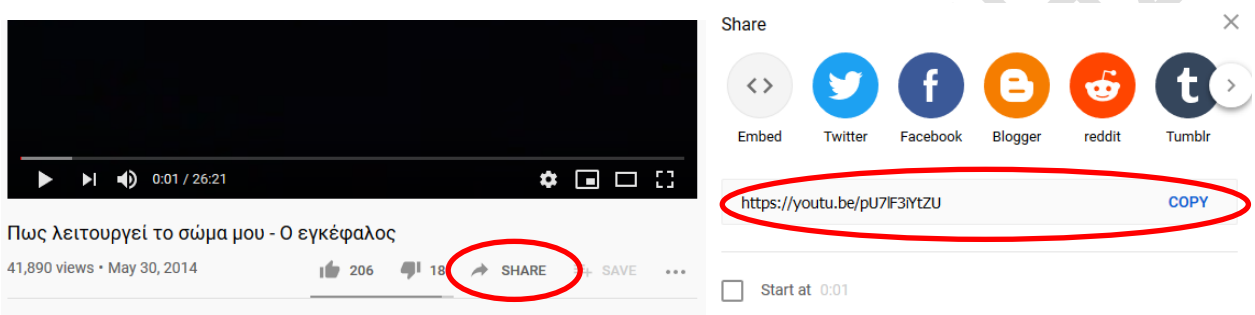
Εικόνα 3: Θάμπωμα φόντου

7. Ασφαλές YouTube

Για όσους εκπαιδευτικούς χρησιμοποιούν στη διδακτική τους πρακτική το YouTube και επιθυμούν να μοιράζονται βίντεο με μαθητές στην τάξη με ασφαλή και φιλικό τρόπο χωρίς περισπασμούς ή προσβλητικά σχόλια προτείνεται να χρησιμοποιούν το «Ασφαλές YouTube» (Safe YouTube).

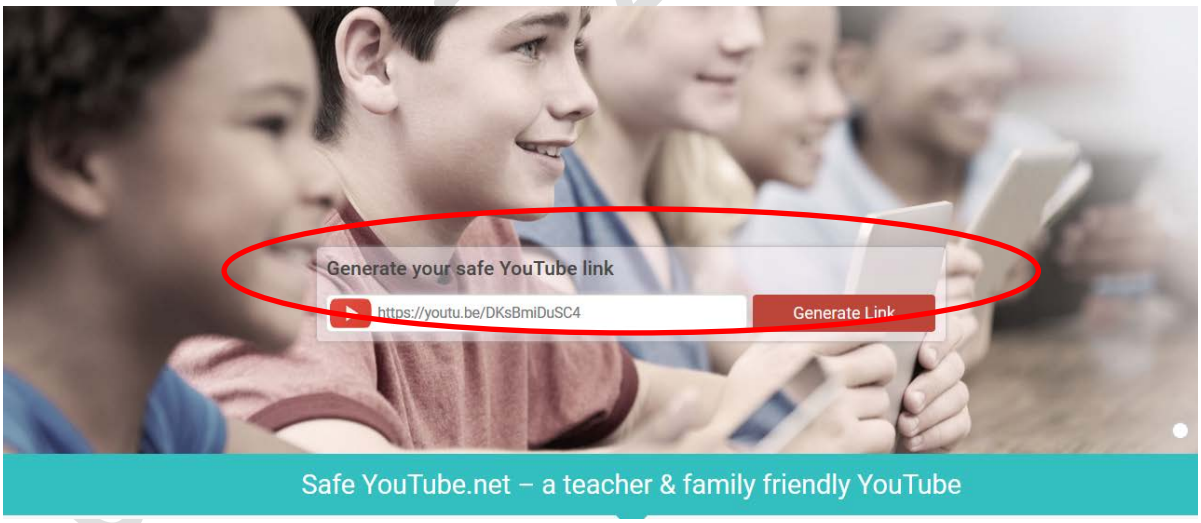
Η διαδικασία είναι απλή:

1. Πηγαίνετε στο YouTube και βρίσκετε το βίντεο που σας ενδιαφέρει. Στη συνέχεια από την επιλογή «Κοινοποίηση» (Share) αντιγράφετε τον σύνδεσμο (Εικ. 4)



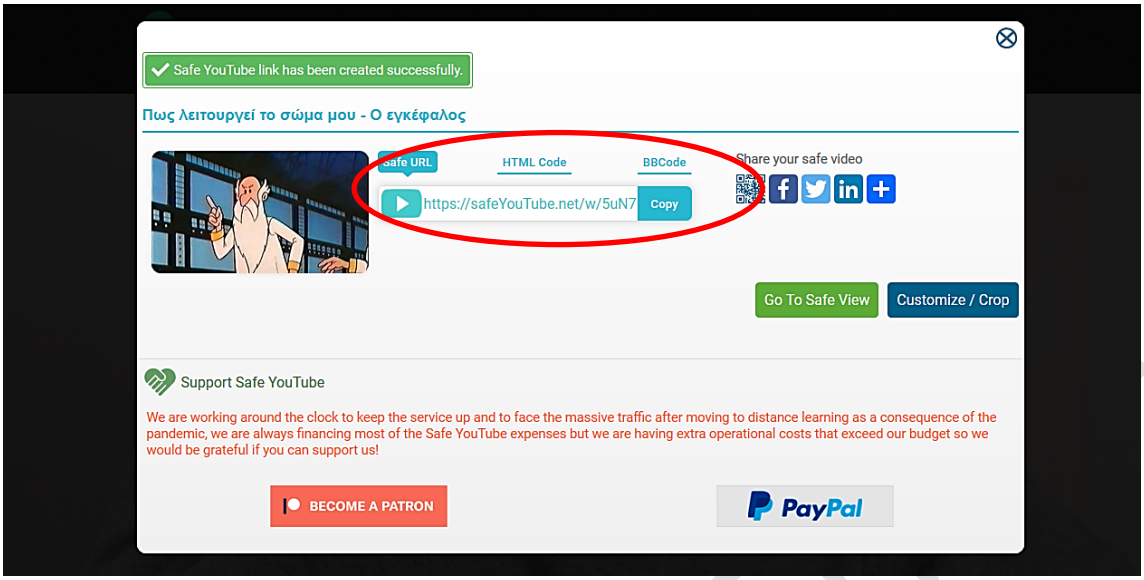
Εικόνα 4: Αντιγραφή συνδέσμου βίντεο YouTube

2. Στη συνέχεια επικολλάτε στο πλαίσιο «Generate your safe YouTube link» που θα βρείτε στον ιστότοπο Safe YouTube και πατάτε το εικονίδιο “Generate Link” (Εικ. 5).



Εικόνα 5: Επικόλληση συνδέσμου βίντεο

3. Από εκεί θα μεταφερθείτε σε μία νέα σελίδα όπου θα βρείτε τον ασφαλή σύνδεσμο για το βίντεο που έχετε επιλέξει (Εικ. 6).



Εικόνα 6: Εμφάνιση του ασφαλούς συνδέσμου βίντεο

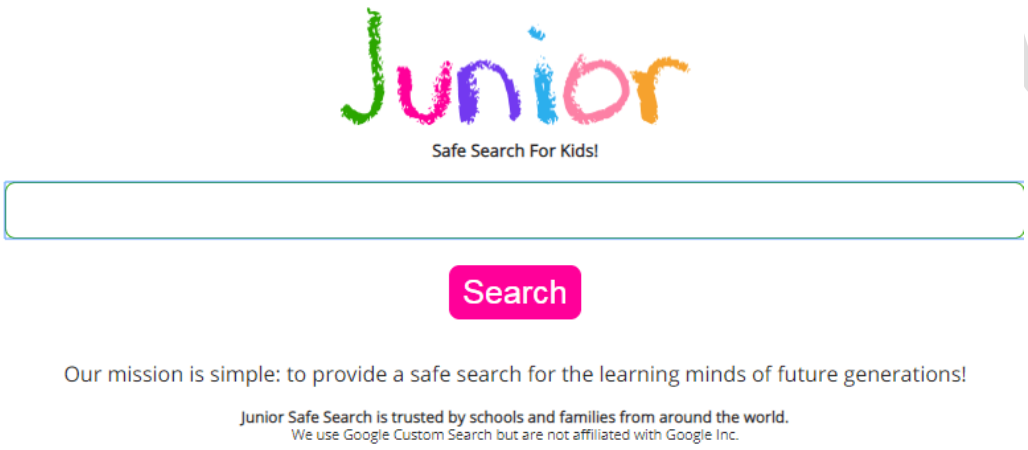
4. Αντιγράψτε τον σύνδεσμο και ανοίξτε μία νέα σελίδα στον φυλλομετρητή σας για να κάνετε επικόλληση και μετάβαση. Το βίντεο θα ανοίξει σε μία ασφαλή τοποθεσία, απαλλαγμένη από διαφημίσεις και σχόλια (Εικ. 7).

Εικόνα 7: Ασφαλής προβολή βίντεο YouTube

8. Η μηχανή αναζήτησης Junior Safe Search

ΠΗΓΗ: Edtech.gr - Junior Safe Search

Στους προβληματισμούς πολλών εκπαιδευτικών και γονέων σχετικά με την περιήγηση των παιδιών στο διαδίκτυο, στα πλαίσια σχολικών εργασιών και την περίπτωση «ανοίγματος» εικόνων και βίντεο με ακατάλληλο περιεχόμενο ή επαφής με κακόβουλο λογισμικό, έρχεται να δώσει η μηχανή αναζήτησης Junior Safe Search που υποστηρίζεται από την Google (Εικ. 8).



Εικόνα 8: Η μηχανή αναζήτησης JuniorSafeSearch

Πρόκειται για μία μηχανή αναζήτησης που παρέχει στους νεαρούς χρήστες μια ασφαλή Google αναζήτηση αποτρέποντας το ακατάλληλο περιεχόμενο. Η εφαρμογή αντλεί δεδομένα από γνωστές παιδικές ιστοσελίδες, ώστε να τις παρουσιάζει κατά προτεραιότητα, ενώ παράλληλα αξιοποιεί πληροφορίες από τους χρήστες σε περίπτωση που κάποια ακατάλληλη σελίδα εμφανιστεί, ώστε να αποτρέψει παρόμοια μελλοντικά περιστατικά.

9. Πηγές

Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: https://www.dpa.gr/

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194

Edtech.gr - Junior Safe Search: https://edtech.gr/junior-safe-search-google/

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου: https://saferinternet4kids.gr/

6ο ΠΕ.Κ.Ε.Δ.