ERASMEDIAH – EDUCATIONAL REINFORCEMENT AGAINST THE SOCIAL MEDIA HYPERCONNECTIVITY
PROJECT NUMBER: 2023-1-HU01-KA220-YOU-000161173

ΕΝΟΤΗΤΑ 5
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (**EACEA**). Η Ευρωπαϊκή Ένωση και ο **EACEA** δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Μάθημα 5.4

Αναγνώριση Κυβερνοαπειλών και Στρατηγικές για την Πρόληψη της Έκθεσης σε Ακατάλληλο Περιεχόμενο

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Διάρκεια: 40 λεπτά

Μάθημα 5.4

Αναγνώριση Κυβερνοαπειλών και Στρατηγικές για την Πρόληψη της Έκθεσης σε Ακατάλληλο Περιεχόμενο

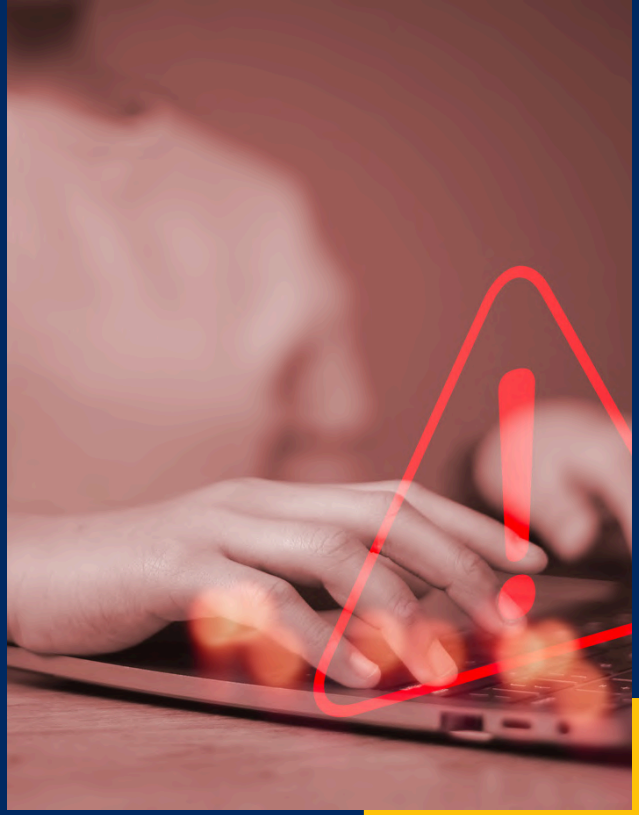
Στόχοι:

- Να ευαισθητοποιηθούν σχετικά με τους διαδεδομένους διαδικτυακούς κινδύνους, όπως η έκθεση σε ακατάλληλο περιεχόμενο, ο διαδικτυακός εκφοβισμός και η σεξουαλική παρενόχληση, με ιδιαίτερη στόχευση σε ευάλωτους χρήστες όπως παιδιά και εφήβους.
- Να ενδυναμώσει τους μαθητές με κρίσιμες δεξιότητες ώστε να αναγνωρίζουν προειδοποιητικά σημάδια κυβερνοαπειλών, όπως ύποπτους συνδέσμους, επιθετική διαδικτυακή συμπεριφορά και χειριστικό περιεχόμενο.
- Να ενθαρρύνουμε προληπτικές συνήθειες στη διαχείριση των διαδικτυακών αλληλεπιδράσεων, ενισχύοντας την κριτική σκέψη, εντοπίζοντας ασφαλείς ψηφιακούς χώρους και διατηρώντας ανοιχτή επικοινωνία σχετικά με τις διαδικτυακές εμπειρίες.

Βασικά Μηνύματα:

- Οι διαδικτυακές απειλές συχνά κρύβονται πίσω από πλατφόρμες ή αλληλεπιδράσεις που μοιάζουν αθώες. Η αναγνώριση των σημαδιών είναι το κλειδί για να παραμείνετε ασφαλείς.
- Απλές πρακτικές όπως η χρήση φίλτρων περιεχομένου και η διατήρηση ισχυρής επικοινωνίας μπορούν να βοηθήσουν στην πρόληψη της έκθεσης σε επιβλαβές περιεχόμενο και κυβερνοαπειλές.

ΕΙΔΟΣ ΜΑΘΗΜΑΤΟΣ:



Επισκόπηση μαθήματος

Στο σημερινό υπερ-διασυνδεδεμένο ψηφιακό περιβάλλον, η έκθεση σε ακατάλληλο περιεχόμενο και κυβερνοαπειλές αποτελεί έναν διαρκή κίνδυνο. Αυτό το μάθημα έχει σχεδιαστεί για να παρέχει μια ολοκληρωμένη κατανόηση της φύσης και των κινδύνων αυτών των απειλών, πρακτικά εργαλεία για τον μετριασμό τους και στρατηγικές για την ενίσχυση ασφαλέστερων διαδικτυακών αλληλεπιδράσεων. Μέσω συναρπαστικών ασκήσεων και πρακτικών συμβουλών, θα ολοκληρώσετε το μάθημα καλύτερα προετοιμασμένοι για να πλοηγηθείτε στον ψηφιακό κόσμο με ασφάλεια και υπευθυνότητα.

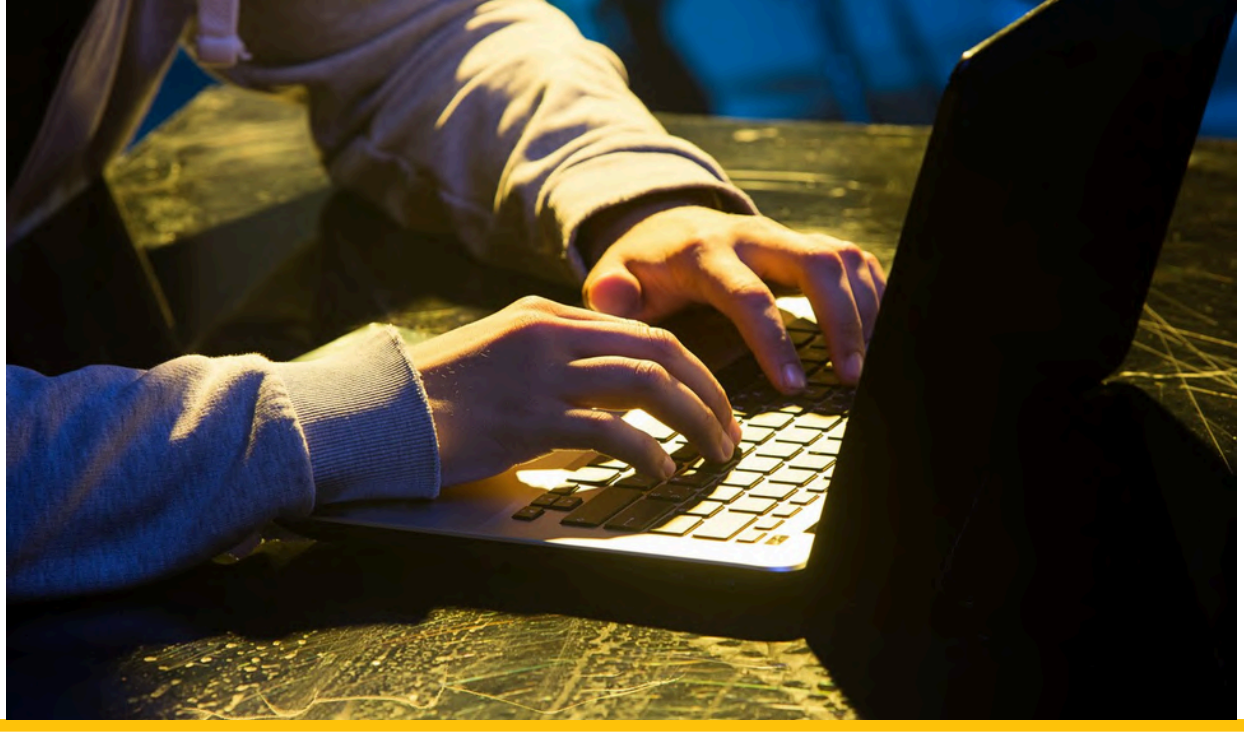
Το εργαστήριο οργανώνεται σε 4 βήματα:

1: Βασικά στοιχεία για τις κυβερνοαπειλές και το ακατάλληλο περιεχόμενο (10 λεπτά)

2: Αναγνώριση προειδοποιητικών σημαδιών και κινδύνων (15 λεπτά)

3: Προσεγγίσεις για την πρόληψη και τον μετριασμό (10 λεπτά)

4: Στοχασμός και εφαρμογή (5 λεπτά)



Βήμα 1

Βασικά στοιχεία για τις κυβερνοαπειλές και το ακατάλληλο περιεχόμενο

Έχετε ποτέ συναντήσει κάτι στο διαδίκτυο που σας έκανε να νιώσετε άβολα ή ανασφαλείς;
Οι **κυβερνοαπειλές** είναι επιβλαβείς δραστηριότητες που στοχεύουν άτομα ή συστήματα στο διαδίκτυο, με στόχο την κλοπή πληροφοριών, την πρόκληση βλάβης ή την εκμετάλλευση τρωτών σημείων. Παραδείγματα περιλαμβάνουν:

- Κυβερνοεκφοβισμός: Χρήση διαδικτυακών πλατφορμών για παρενόχληση ή εκφοβισμό.
- Ηλεκτρονικό ψάρεμα (phishing): Αποστολή παραπλανητικών μηνυμάτων με σκοπό την εξαπάτηση ατόμων ώστε να αποκαλύψουν προσωπικά στοιχεία.
- Globeing: Η οικοδόμηση μιας σχέσης με κάποιον στο διαδίκτυο με σκοπό την εκμετάλλευσή του αργότερα, συχνά με ακατάλληλο τρόπο.

Τι συνιστά **ακατάλληλο περιεχόμενο;**
Περιεχόμενο που είναι επιβλαβές, άσεμνο ή ακατάλληλο για ορισμένες ηλικιακές ομάδες, όπως:

- Άσεμνες εικόνες ή βίντεο.
- Χειριστικά ή επιθετικά μηνύματα.
- Βίαιο ή μισητό υλικό.

Βήμα 1

Βασικά στοιχεία για τις κυβερνοαπειλές και το ακατάλληλο περιεχόμενο

Η έκθεση σε τέτοιο περιεχόμενο μπορεί να προκαλέσει συναισθηματική δυσφορία, να βλάψει τις σχέσεις και να οδηγήσει σε μακροπρόθεσμες συνέπειες όπως κλοπή ταυτότητας ή εκμετάλλευση.

Δραστηριότητα

Τώρα, θα χωριστούμε σε μικρές ομάδες. Κάθε ομάδα θα έχει ένα σενάριο προς ανάλυση:

Σενάριο 1: Λαμβάνετε ένα email από έναν άγνωστο που σας ζητά προσωπικά στοιχεία.

Σενάριο 2: Βλέπετε έναν ύποπτο σύνδεσμο σε ένα email.

Σενάριο 3: Συναντάτε ένα ακατάλληλο σχόλιο στα μέσα κοινωνικής δικτύωσης.

Η εργασία σας είναι να απαντήσετε στις ερωτήσεις της ομάδας σας:

- Τι επικίνδυνο υπάρχει σε αυτή την κατάσταση;
- Πώς μπορείτε να αντιδράσετε με ασφάλεια;

Μόλις οι ομάδες ολοκληρώσουν τις εργασίες τους, μοιραστείτε τα συμπεράσματά σας.

Βήμα 2 Αναγνώριση προειδοποιητικών σημαδιών και κινδύνων

Ρίξτε μια ματιά στα παρακάτω παραδείγματα και σκεφτείτε αν έχετε δει ποτέ κάτι παρόμοιο στο Διαδίκτυο. Κατά την ανταλλαγή ιδεών, συζητήστε ως ομάδα ποια από αυτά τα προειδοποιητικά σημάδια είναι τα πιο συνηθισμένα και πώς μπορείτε να τα αντιμετωπίσετε.

1. Άγνωστος ή ύποπτος αποστολέας

- Λαμβάνετε ένα μήνυμα από κάποιον που δεν γνωρίζετε, το οποίο σας ζητά προσωπικά στοιχεία ή σας προτρέπει να κάνετε κλικ σε έναν σύνδεσμο.
- Η διεύθυνση ηλεκτρονικού ταχυδρομείου φαίνεται ασυνήθιστη, όπως "bank123random@mail.com" αντί για επίσημη διεύθυνση.
- *Ερώτηση για συζήτηση:* «Τι κάνετε όταν λαμβάνετε ένα μήνυμα από κάποιον που δεν αναγνωρίζετε;»

2. Ορθογραφικά ή γραμματικά λάθη

- Το μήνυμα είναι γεμάτο ορθογραφικά λάθη ή περίεργες διατυπώσεις.
- Παράδειγμα: "Ο λογαριασμός σας έχει αποκλειστεί! Κάντε κλικ εδώ για να αντιδράσετε"
- Ερώτηση για συζήτηση: «Σας κάνουν τα λάθη σε ένα μήνυμα καχύποπτους; Γιατί ή γιατί όχι;»

Βήμα 2

Αναγνώριση προειδοποιητικών σημαδιών και κινδύνων

3. Επείγοντα αιτήματα ή απειλές
   - Μηνύματα όπως: "Εάν δεν πληρώσετε εντός 24 ωρών, ο λογαριασμός σας θα απενεργοποιηθεί!"
   - Το περιεχόμενο προσπαθεί να σας τρομάξει ή να σας πιέσει να δράσετε γρήγορα.
   - *Ερώτηση για συζήτηση:* «Πώς μπορείτε να διακρίνετε τη διαφορά μεταξύ μιας πραγματικής προειδοποίησης και μιας απάτης;»
4. Πολύ καλές για να είναι αληθινές προσφορές
   - Διαφημίσεις που υπόσχονται απίστευτες ανταμοιβές: "Κερδίσατε ένα ολοκαίνουργιο iPhone! Κάντε κλικ εδώ για να διεκδικήσετε το βραβείο σας"
   - Ιστότοποι που προσφέρουν μη ρεαλιστικά οφέλη με ελάχιστη προσπάθεια.
   - *Ερώτηση για συζήτηση:* «Γιατί αυτού του είδους οι προσφορές είναι επικίνδυνες;»

Βήμα 2

Αναγνώριση προειδοποιητικών σημαδιών και κινδύνων

5. Άγνωστοι σύνδεσμοι ή συνημμένα

- Λαμβάνετε έναν σύνδεσμο που δεν φαίνεται αξιόπιστος, όπως "www.freegift.now".
- Συνημμένα από άγνωστους αποστολείς που ενδέχεται να περιέχουν ιούς.
- *Ερώτηση για συζήτηση:* «Πώς μπορείτε να ελέγξετε αν ένας σύνδεσμος ή ένα συνημμένο είναι ασφαλές;»

Στην ομάδα σας, διαλέξτε ένα από αυτά τα προειδοποιητικά σημάδια και συζητήστε πώς θα χειριζόσασταν την κατάσταση.

Στο τέλος, κάθε ομάδα θα μοιραστεί τις γνώσεις και τις ιδέες της σχετικά με το πώς να αποφύγει αυτούς τους κινδύνους στις καθημερινές διαδικτυακές δραστηριότητες.

Βήμα 3

Προσεγγίσεις για την πρόληψη και τον μετριασμό

Ο καλύτερος τρόπος για να παραμείνετε ασφαλείς στο διαδίκτυο είναι να λαμβάνετε προληπτικά μέτρα που προστατεύουν τα δεδομένα σας και αποτρέπουν τους κινδύνους πριν συμβούν. Ας εξερευνήσουμε απλές στρατηγικές που μπορείτε να αρχίσετε να χρησιμοποιείτε αμέσως.

Ας μείνουμε στις ίδιες ομάδες. Διαβάστε την ακόλουθη λίστα με απλές ενέργειες που μπορείτε να κάνετε για να μειώσετε τους κινδύνους στο διαδίκτυο:

- **Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης** και ενημερώνετέ τους τακτικά.
- **Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)** για σημαντικούς λογαριασμούς.
- **Αποφύγετε ύποπτους συνδέσμους και συνημμένα** - επαληθεύετε πάντα την πηγή.
- **Ελέγξτε τις ρυθμίσεις απορρήτου** στα μέσα κοινωνικής δικτύωσης και στις εφαρμογές για να ελέγχετε ποιος βλέπει τις πληροφορίες σας.
- **Διατηρήστε το λογισμικό ενημερωμένο** για την επιδιόρθωση ευπαθειών ασφαλείας.

Στην ομάδα σας, συζητήστε ποιες από αυτές τις ενέργειες εφαρμόζετε ήδη και ποιες μπορεί να δυσκολευτείτε να εφαρμόσετε.
Απαντήστε μαζί στις παρακάτω ερωτήσεις:

- «Ποια στρατηγική πιστεύετε ότι είναι η πιο αποτελεσματική για να παραμείνετε ασφαλείς στο διαδίκτυο;»

Βήμα 3

Προσεγγίσεις για την πρόληψη και τον μετριασμό

«Πώς μπορείτε να υπενθυμίσετε στον εαυτό σας να αναπτύξει καλύτερες συνήθειες, όπως τον έλεγχο των ρυθμίσεων απορρήτου ή την αποφυγή επικίνδυνων συνδέσμων;» Μετά την ανταλλαγή ιδεών, κάθε ομάδα μοιράζεται μια **νέα** στρατηγική που σχεδιάζει να υιοθετήσει και εξηγεί με λίγα λόγια γιατί είναι σημαντική.

Ως τελική σκέψη, αφιερώστε λίγο χρόνο για να σκεφτείτε μια συγκεκριμένη συνήθεια ή εργαλείο που θα δεσμευτείτε να χρησιμοποιήσετε αμέσως για να βελτιώσετε την ασφάλειά σας στο διαδίκτυο. Σημειώστε το σε ένα αυτοκόλλητο χαρτί και σκεφτείτε πώς μπορείτε να βοηθήσετε άλλους να υιοθετήσουν τις ίδιες συνήθειες. Μοιράζοντας τις γνώσεις σας, μπορείτε να δημιουργήσετε ένα ασφαλέστερο διαδικτυακό περιβάλλον όχι μόνο για τον εαυτό σας αλλά και για τους φίλους, την οικογένεια και την κοινότητά σας.

Βήμα 4

Στοχασμός και εφαρμογή

Τώρα που εξερευνήσαμε τους διαδικτυακούς κινδύνους και τις στρατηγικές πρόληψης, ήρθε η ώρα να αναλογιστούμε όσα μάθατε και πώς μπορείτε να τα εφαρμόσετε στην καθημερινή σας ψηφιακή ζωή.

Αφιερώστε λίγο χρόνο για να απαντήσετε στην ερώτηση σιωπηλά:

- «Ποια είναι μια συνήθεια που έχεις αυτή τη στιγμή και μπορεί να σε θέσει σε κίνδυνο στο διαδίκτυο;»

Γράψτε την απάντησή σας σε ένα αυτοκόλλητο σημείωμα.

Ως επόμενο βήμα, δημιουργήστε ζευγάρια με έναν/μία συνεργάτη/συνεργάτιδα και μοιραστείτε τις σκέψεις σας:

- Εξηγήστε την επικίνδυνη συνήθεια που εντοπίσατε και γιατί μπορεί να αποτελεί πρόβλημα.
- Κοινοποιήστε την ενέργεια ή το εργαλείο που σκοπεύετε να υιοθετήσετε για να μετριάσετε αυτόν τον κίνδυνο.
- Προσφέρετε ο ένας στον άλλον σχόλια ή επιπλέον ιδέες για να ενισχύσετε τα σχέδιά σας.
- Συζητήστε πώς αυτές οι στρατηγικές μπορούν να εφαρμοστούν σε διαφορετικές καταστάσεις, όπως η χρήση δημόσιου Wi-Fi, η κοινοποίηση προσωπικών πληροφοριών ή η αποφυγή της grooming και του ηλεκτρονικού "ψαρέματος" (phishing).

Σύνοψη των βασικών συμπερασμάτων

- **Η ευαισθητοποίηση είναι το πρώτο βήμα προς την προστασία.**
- **Προειδοποιητικά σημάδια υπάρχουν παντού, αλλά μόλις μάθετε να τα αναγνωρίζετε και να αντιδράτε κατάλληλα, μπορείτε να βελτιώσετε σημαντικά την ασφάλειά σας στο διαδίκτυο!**
- **Η κατανόηση των απειλών στον κυβερνοχώρο και του ακατάλληλου περιεχομένου σάς δίνει τη δυνατότητα να εντοπίζετε πιθανούς κινδύνους και να αντιδράτε με αυτοπεποίθηση.**
- **Η αναγνώριση των κινδύνων σε καθημερινές διαδικτυακές καταστάσεις σάς επιτρέπει να ενεργείτε γρήγορα και να αποφεύγετε τους κινδύνους.**
- **Διαδίδοντας την ευαισθητοποίηση, βοηθάτε στη δημιουργία μιας ασφαλέστερης διαδικτυακής κοινότητας για όλους.**

Οδηγίες για εργαζόμενους στον τομέα της νεολαίας, εκπαιδευτικούς και δασκάλους

Σκοπός:
Αυτό το μάθημα έχει σχεδιαστεί για να ευαισθητοποιήσει τους συμμετέχοντες σχετικά με τους διαδικτυακούς κινδύνους, συμπεριλαμβανομένων των κυβερνοαπειλών και του ακατάλληλου περιεχομένου, και να τους εξοπλίσει με πρακτικές στρατηγικές για την ενίσχυση ασφαλέστερων διαδικτυακών αλληλεπιδράσεων. Αναλύοντας σενάρια πραγματικού κόσμου, οι συμμετέχοντες θα μάθουν να εντοπίζουν κινδύνους, να αναγνωρίζουν προειδοποιητικά σημάδια και να λαμβάνουν προληπτικά μέτρα.

Απαιτούμενα υλικά:

- Πίνακας παρουσιάσεων ή ψηφιακό εργαλείο παρουσίασης για την περιγραφή βασικών εννοιών
- Στυλό και μαρκαδόροι
- Λευκά φύλλα χαρτιού για σημειώσεις ή ολοκλήρωση δραστηριοτήτων
- Πρόσβαση σε εργαλεία όπως το CyberWise ή το Malwarebytes Browser Guard (σε περίπτωση παρουσίασής τους στους συμμετέχοντες)
- Πολύχρωμα σημειώματα post-it για καταιγισμό ιδεών

Βήμα 1: Βασικά στοιχεία για τις κυβερνοαπειλές και το ακατάλληλο περιεχόμενο (10 λεπτά)

1. Ξεκινήστε ρωτώντας τους συμμετέχοντες: «Έχετε συναντήσει ποτέ κάτι στο διαδίκτυο που σας φάνηκε μη ασφαλές ή ύποπτο;». Ενθαρρύνετε μερικούς να μοιραστούν τις εμπειρίες τους ή να δώσουν ένα σύντομο παράδειγμα, όπως η λήψη ενός ύποπτου email ή η προβολή ενός προσβλητικού σχολίου. Χρησιμοποιήστε αυτό για να τονίσετε τη σημασία της κατανόησης και της αντιμετώπισης των διαδικτυακών κινδύνων.
2. Μικρή διάλεξη - εξηγήστε τις βασικές κυβερνοαπειλές: ηλεκτρονικό ψάρεμα (phishing), grooming (προσβολή από ιούς) κ.λπ. Ορίστε το ακατάλληλο περιεχόμενο, όπως:
- Άσεμνο υλικό - Επιβλαβείς ή παραστατικές εικόνες και βίντεο.
- Αρπακτικά μηνύματα - Χειριστική ή επιβλαβής επικοινωνία.
- Περιεχόμενο ακατάλληλο για ηλικίες - Υλικό ακατάλληλο για ορισμένες ηλικιακές ομάδες.

3. Δραστηριότητα: Χωρίστε τους συμμετέχοντες σε ομάδες των 3-5 ατόμων και αναθέστε σε κάθε ομάδα ένα από τα τρία διαφορετικά σενάρια.

Οδηγίες για ομάδες:

1. Ανάλυση του κινδύνου: Συζητήστε τι καθιστά το σενάριο επικίνδυνο (π.χ. άγνωστος αποστολέας, επείγων τόνος ή ύποπτος σύνδεσμος).
2. Προτείνετε ασφαλείς ενέργειες: Κάντε καταιγισμό ιδεών για πρακτικές απαντήσεις:

- Για email: Αποφύγετε να κάνετε κλικ σε συνδέσμους, να επαληθεύετε τον αποστολέα μέσω επίσημων καναλιών ή να αναφέρετε τα ως ανεπιθύμητα.
- Για ακατάλληλα σχόλια: Αποκλείστε τον χρήστη, αναφέρετε το σχόλιο και αποφύγετε να απαντήσετε.
- Για ύποπτους συνδέσμους: Τοποθετήστε τον δείκτη του ποντικιού για να ελέγξετε τη διεύθυνση URL, μην κάνετε κλικ αν δεν είστε σίγουροι και συμβουλευτείτε μια αξιόπιστη πηγή.

3. Κοινοποίηση ευρημάτων: Οι ομάδες συνοψίζουν την ανάλυσή τους και τη μοιράζονται με την τάξη. Επισημαίνουν κοινές στρατηγικές και συζητούν την αποτελεσματικότητά τους.
4. 4. Ολοκληρώστε την δραστηριότητα ενισχύοντας τα βασικά σημεία, συνδέοντας τη δραστηριότητα με ευρύτερες στρατηγικές για την ασφάλεια στο διαδίκτυο, οι οποίες θα διερευνηθούν στα επόμενα βήματα.

Βήμα 2: Αναγνώριση προειδοποιητικών σημαδιών και κινδύνων (15 λεπτά)

1. Παρουσιάστε στους συμμετέχοντες τα συνηθισμένα προειδοποιητικά σημάδια απειλών στον κυβερνοχώρο χρησιμοποιώντας σαφή παραδείγματα:
   - Ύποπτοι σύνδεσμοι ή άγνωστοι αποστολείς: Μηνύματα από άγνωστες επαφές με συνδέσμους ή συνημμένα (π.χ., "www.freeprizes.xyz").
   - Ορθογραφικά λάθη ή επείγουσες απαιτήσεις: Μηνύματα όπως «Ο λογαριασμός σας έχει αποκλειστεί! Επανενεργοποιήστε τώρα», συχνά κακογραμμένα για να δημιουργήσουν επείγον.
   - Προσφορές που είναι πολύ καλές για να είναι αληθινές: Υποσχέσεις για ανταμοιβές ή προσφορές, όπως «Κερδίσατε ένα δωρεάν iPhone!»

Μπορείτε επίσης να χρησιμοποιήσετε οπτικά στοιχεία, όπως στιγμιότυπα οθόνης από απόπειρες ηλεκτρονικού "ψαρέματος" (phishing), και να ενθαρρύνετε τους συμμετέχοντες να μοιράζονται παραδείγματα για καλύτερη αλληλεπίδραση.

2. Το επόμενο βήμα είναι η διεξαγωγή μιας ομαδικής άσκησης. Χωρίστε τους συμμετέχοντες σε μικρές ομάδες και αναθέστε σε κάθε ομάδα ένα συγκεκριμένο προειδοποιητικό σημάδι για ανάλυση (π.χ. επείγοντα μηνύματα ή ύποπτοι σύνδεσμοι). Παρέχετε τα εξής βήματα:
   1. Αναλύστε την προειδοποίηση: Συζητήστε τι κάνει την απειλή πειστική (π.χ. επείγον ή παραπλάνηση).
   2. Προτείνετε λύσεις: Σκεφτείτε καταιγισμό ιδεών για απαντήσεις, όπως επαλήθευση πηγών, αποφυγή ύποπτων συνδέσμων ή αναφορά απάτης.
   3. Συνοψίστε τα ευρήματα: Προετοιμάστε πρακτικές συμβουλές για την αποφυγή της απειλής που έχει ανατεθεί.

3. Στο τέλος, κάθε ομάδα παρουσιάζει τις ιδέες και τις στρατηγικές της. Συνοψίστε τες σε μια ενοποιημένη λίστα βέλτιστων πρακτικών σε έναν πίνακα ή σεμινάριο. Ολοκληρώστε τονίζοντας την αξία της προσοχής, της επαλήθευσης και της κριτικής σκέψης για την ασφαλή διαδικτυακή παραμονή.

Βήμα 3: Προσεγγίσεις για την πρόληψη και τον μετριασμό (10 λεπτά)

1. Ξεκινήστε τονίζοντας τη σημασία των προληπτικών βημάτων για την προστασία των προσωπικών δεδομένων και τη μείωση των κινδύνων στο διαδίκτυο. Παρουσιάστε μια λίστα με απλές ενέργειες που μπορούν να υιοθετήσουν άμεσα οι συμμετέχοντες, όπως:
Χρήση ισχυρών, μοναδικών κωδικών πρόσβασης και τακτική ενημέρωσή τους.

- Ενεργοποίηση πολυπαραγοντικής επαλήθευσης ταυτότητας (MFA) για κρίσιμους λογαριασμούς.
- Αποφυγή ύποπτων συνδέσμων και συνημμένων μέσω επαλήθευσης των πηγών τους.
- Έλεγχος των ρυθμίσεων απορρήτου στα μέσα κοινωνικής δικτύωσης και στις εφαρμογές.
- Διατήρηση της ενημέρωσης του λογισμικού για την αντιμετώπιση ευπαθειών ασφαλείας.

Εξηγήστε πώς αυτές οι ενέργειες μπορούν να μετριάσουν αποτελεσματικά τους κοινούς διαδικτυακούς κινδύνους.

2. Διατηρήστε τους συμμετέχοντες στις υπάρχουσες ομάδες τους και δώστε τους τη λίστα ενεργειών. Ζητήστε τους να συζητήσουν και να ολοκληρώσουν τις ακόλουθες εργασίες:

1. Ομαδική συζήτηση:

- Προσδιορίστε ποιες ενέργειες εφαρμόζουν ήδη και ποιες θεωρούν δύσκολες.
- Συζητήστε γιατί ορισμένες στρατηγικές μπορεί να είναι πιο δύσκολο να εφαρμοστούν και σκεφτείτε τρόπους για να ξεπεράσετε αυτές τις προκλήσεις.

2. Απαντήστε σε βασικές ερωτήσεις:

- «Ποια στρατηγική πιστεύετε ότι είναι η πιο αποτελεσματική για να παραμείνετε ασφαλείς στο διαδίκτυο;»
- «Πώς μπορείτε να υπενθυμίσετε στον εαυτό σας να αναπτύξει καλύτερες συνήθειες, όπως τον τακτικό έλεγχο των ρυθμίσεων απορρήτου ή την αποφυγή επικίνδυνων συνδέσμων;»

3. Κοινοποιήστε νέες στρατηγικές:

- Κάθε ομάδα επιλέγει μια νέα στρατηγική που σκοπεύει να υιοθετήσει, εξηγεί γιατί είναι σημαντική και τη μοιράζεται με άλλους.

Βήμα 3: Προσεγγίσεις για την πρόληψη και τον μετριασμό (10 λεπτά)

3. Ολοκληρώστε τη δραστηριότητα ζητώντας από κάθε συμμετέχοντα να σκεφτεί ατομικά μια συνήθεια ή ένα εργαλείο που θα δεσμευτεί να χρησιμοποιήσει αμέσως για να βελτιώσει την ασφάλειά του στο διαδίκτυο. Ζητήστε του να το γράψει σε ένα αυτοκόλλητο χαρτί. Ενθαρρύνετε τους συμμετέχοντες να σκεφτούν πώς μπορούν να μοιραστούν αυτή τη συνήθεια με φίλους, συγγενείς ή συναδέλφους για να προωθήσουν συλλογικά ένα ασφαλέστερο διαδικτυακό περιβάλλον.

Βήμα 4: Στοχασμός και εφαρμογή (5 λεπτά)

1. Ατομικός αναστοχασμός:
   - Ρωτήστε τους μαθητές: «Ποια είναι μια διαδικτυακή συνήθεια που μπορείτε να αλλάξετε για να βελτιώσετε την ασφάλειά σας;»
   - Οι συμμετέχοντες γράφουν τις απαντήσεις τους σε αυτοκόλλητα σημειώματα.
2. Συζήτηση μεταξύ συνομηλίκων:
   - Χωρίστε τους συμμετέχοντες σε ζεύγη για να μοιραστούν τους στόχους τους και να προτείνουν εφαρμόσιμα βήματα.
3. Σύνοψη:
   - Ολοκληρώστε με ένα ενθαρρυντικό συμπέρασμα. Θα μπορούσε να είναι, για παράδειγμα: «Οι μικρές αλλαγές στη διαδικτυακή σας συμπεριφορά μπορούν να κάνουν μεγάλη διαφορά στην ασφάλειά σας και στην ασφάλεια της κοινότητάς σας».

Βασικά σημεία:
Οι συμμετέχοντες θα πρέπει να ολοκληρώσουν τη συνεδρία έχοντας κατανοήσει πλήρως τον τρόπο αναγνώρισης των κυβερνοαπειλών και του ακατάλληλου περιεχομένου, όπως απόπειρες ηλεκτρονικού "ψαρέματος" (phishing), χειριστικά μηνύματα ή ύποπτους συνδέσμους. Να επισημάνουν τη σημασία των πρακτικών στρατηγικών ασφαλείας, όπως η χρήση ισχυρών κωδικών πρόσβασης, η ενεργοποίηση της πολυπαραγοντικής επαλήθευσης ταυτότητας και η προσαρμογή των ρυθμίσεων απορρήτου για την προστασία των προσωπικών πληροφοριών.
Προσκαλέστε τους συμμετέχοντες να υιοθετήσουν μια προληπτική νοοτροπία, καλλιεργώντας την κριτική σκέψη και διατηρώντας ανοιχτές συζητήσεις σχετικά με τους διαδικτυακούς κινδύνους. Ενισχύστε αυτές τις αρχές μέσω τακτικής εξάσκησης και ανταλλαγής γνώσεων με άλλους, δημιουργώντας ένα κυματιστικό αποτέλεσμα που προωθεί ασφαλέστερες διαδικτυακές συνήθειες στις κοινότητές τους.

Δραστηριότητες παρακολούθησης και δραστηριότητες στο σπίτι:
Ζητήστε από τους συμμετέχοντες να:

- Ελέγξουν τις προσωπικές τους ρυθμίσεις στα μέσα κοινωνικής δικτύωσης.
- Δοκιμάσουν εργαλεία όπως το Malwarebytes Browser Guard ή φίλτρα περιεχομένου.
- Μοιραστούν μια στρατηγική που έμαθαν με έναν φίλο ή ένα μέλος της οικογένειάς τους.

Συμβουλές για εκπαιδευτικούς:
Κάντε τα μαθήματα ενδιαφέροντα χρησιμοποιώντας παραδείγματα από τον πραγματικό κόσμο και σαφή γραφικά για να εξηγήσετε τους κινδύνους στο διαδίκτυο και τις πρακτικές στρατηγικές ασφάλειας. Ενθαρρύνετε τις διαδραστικές συζητήσεις για να βοηθήσετε τους συμμετέχοντες να συνδεθούν με το υλικό. Οι πρακτικές δραστηριότητες, όπως η δημιουργία οδηγών ασφάλειας, βοηθούν στην εδραίωση των εννοιών. Διατηρήστε ένα υποστηρικτικό και ανοιχτό περιβάλλον όπου οι ερωτήσεις είναι ευπρόσδεκτες και δώστε έμφαση στα μακροπρόθεσμα οφέλη των ασφαλών διαδικτυακών συνηθειών. Ενισχύστε τα βασικά μαθήματα μέσω επακόλουθων εργασιών ή ομαδικών αναστοχασμών για να διασφαλίσετε ότι οι συμμετέχοντες διατηρούν και εφαρμόζουν όσα έχουν μάθει.

Δραστηριότητες παρακολούθησης και δραστηριότητες στο σπίτι:

Ζητήστε από τους συμμετέχοντες να:

- Ελέγξουν τις προσωπικές τους ρυθμίσεις στα μέσα κοινωνικής δικτύωσης.
- Δοκιμάσουν εργαλεία όπως το Malwarebytes Browser Guard ή φίλτρα περιεχομένου.
- Μοιραστούν μια στρατηγική που έμαθαν με έναν φίλο ή ένα μέλος της οικογένειάς τους.

Συμβουλές για εκπαιδευτικούς:

Κάντε τα μαθήματα ενδιαφέροντα χρησιμοποιώντας παραδείγματα από τον πραγματικό κόσμο και σαφή γραφικά για να εξηγήσετε τους κινδύνους στο διαδίκτυο και τις πρακτικές στρατηγικές ασφάλειας. Ενθαρρύνετε τις διαδραστικές συζητήσεις για να βοηθήσετε τους συμμετέχοντες να συνδεθούν με το υλικό. Οι πρακτικές δραστηριότητες, όπως η δημιουργία οδηγών ασφάλειας, βοηθούν στην εδραίωση των εννοιών. Διατηρήστε ένα υποστηρικτικό και ανοιχτό περιβάλλον όπου οι ερωτήσεις είναι ευπρόσδεκτες και δώστε έμφαση στα μακροπρόθεσμα οφέλη των ασφαλών διαδικτυακών συνηθειών. Ενισχύστε τα βασικά μαθήματα μέσω επακόλουθων εργασιών ή ομαδικών αναστοχασμών για να διασφαλίσετε ότι οι συμμετέχοντες διατηρούν και εφαρμόζουν όσα έχουν μάθει.

Εργαλεία

CyberWise

Το CyberWise είναι μια εκπαιδευτική πλατφόρμα που προσφέρει εργαλεία, πόρους και οδηγούς για να βοηθήσει άτομα, ιδιαίτερα γονείς, εκπαιδευτικούς και μαθητές, να κατανοήσουν την ασφάλεια στο διαδίκτυο. Παρέχει ενότητες για την αναγνώριση απειλών στον κυβερνοχώρο, όπως το ηλεκτρονικό ψάρεμα (phishing), ο διαδικτυακός εκφοβισμός (cyberbullying) και το ακατάλληλο περιεχόμενο, μαζί με στρατηγικές για τον μετριασμό των κινδύνων.

www.cyberwise.org

Malwarebytes Browser Guard

Πρόκειται για μια δωρεάν επέκταση προγράμματος περιήγησης που προστατεύει τους χρήστες από ηλεκτρονικό ψάρεμα (phishing), απάτες, κακόβουλο λογισμικό και ακατάλληλο περιεχόμενο. Αποκλείει ενεργά επιβλαβείς ιστότοπους και διαφημίσεις, διασφαλίζοντας ασφαλέστερη περιήγηση για όλους τους χρήστες, όχι μόνο για τα παιδιά.

www.malwarebytes.com

Παραπομπές

- CyberWise. (n.d.). Retrieved from https://www.cyberwise.org
- Dalby, J. (2021, January 15). How to Avoid Inappropriate Content. Gabb Now. Retrieved from https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (2023, September 25). Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. Retrieved from https://figshare.com/ndownloader/files/42443952
- Lynch, M. (2024, April 5). 19 simple ways to block inappropriate content. The Tech Edvocate. Retrieved from https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (2024, February 21). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Retrieved from https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Retrieved from https://www.malwarebytes.com/browserguard
- Roy, R. (2021, August 23). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Retrieved from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 Types of Cyber Security Threats and Solutions. Retrieved from https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Ποιο είναι ένα βασικό σημάδι μιας απόπειρας ηλεκτρονικού "ψαρέματος" (phishing);

Α. Λήψη μηνύματος από έναν προηγουμένως άγνωστο αλλά επαληθευμένο λογαριασμό

Β. Ένα email χωρίς συνδέσμους, εικόνες ή συνημμένα

Γ. Ένα email που σας προτρέπει να ενεργήσετε αμέσως, συχνά με κακή γραμματική

Δ. Ένα μήνυμα από έναν γνωστό αποστολέα που ζητά πληροφορίες ρουτίνας

2. Ποια συμπεριφορά θα μπορούσε να αυξήσει τον κίνδυνο κυβερνοαπειλών;

Α. Τακτική ενημέρωση των συσκευών και των εφαρμογών σας

Β. Κλικ σε συνδέσμους σε email χωρίς επαλήθευση του αποστολέα

Γ. Χρήση ελέγχου ταυτότητας δύο παραγόντων για διαδικτυακούς λογαριασμούς

Δ. Έλεγχος των ρυθμίσεων απορρήτου στα μέσα κοινωνικής δικτύωσης μία φορά το μήνα

3. Ποια συνήθεια βοηθά στην αποφυγή απειλών στον κυβερνοχώρο;

Α. Χρήση ενός διαχειριστή κωδικών πρόσβασης για τη δημιουργία και αποθήκευση μοναδικών κωδικών πρόσβασης

Β. Αποδοχή όλων των δικαιωμάτων κατά την εγκατάσταση εφαρμογών για λόγους ευκολίας

Γ. Κοινοποίηση κωδικών πρόσβασης σε έμπιστους φίλους ή μέλη της οικογένειάς σας για να έχετε ένα εφεδρικό σύστημα σε περίπτωση που τους ξεχάσετε

Δ. Αγνόηση των προειδοποιήσεων ασφαλείας από το πρόγραμμα περιήγησής σας

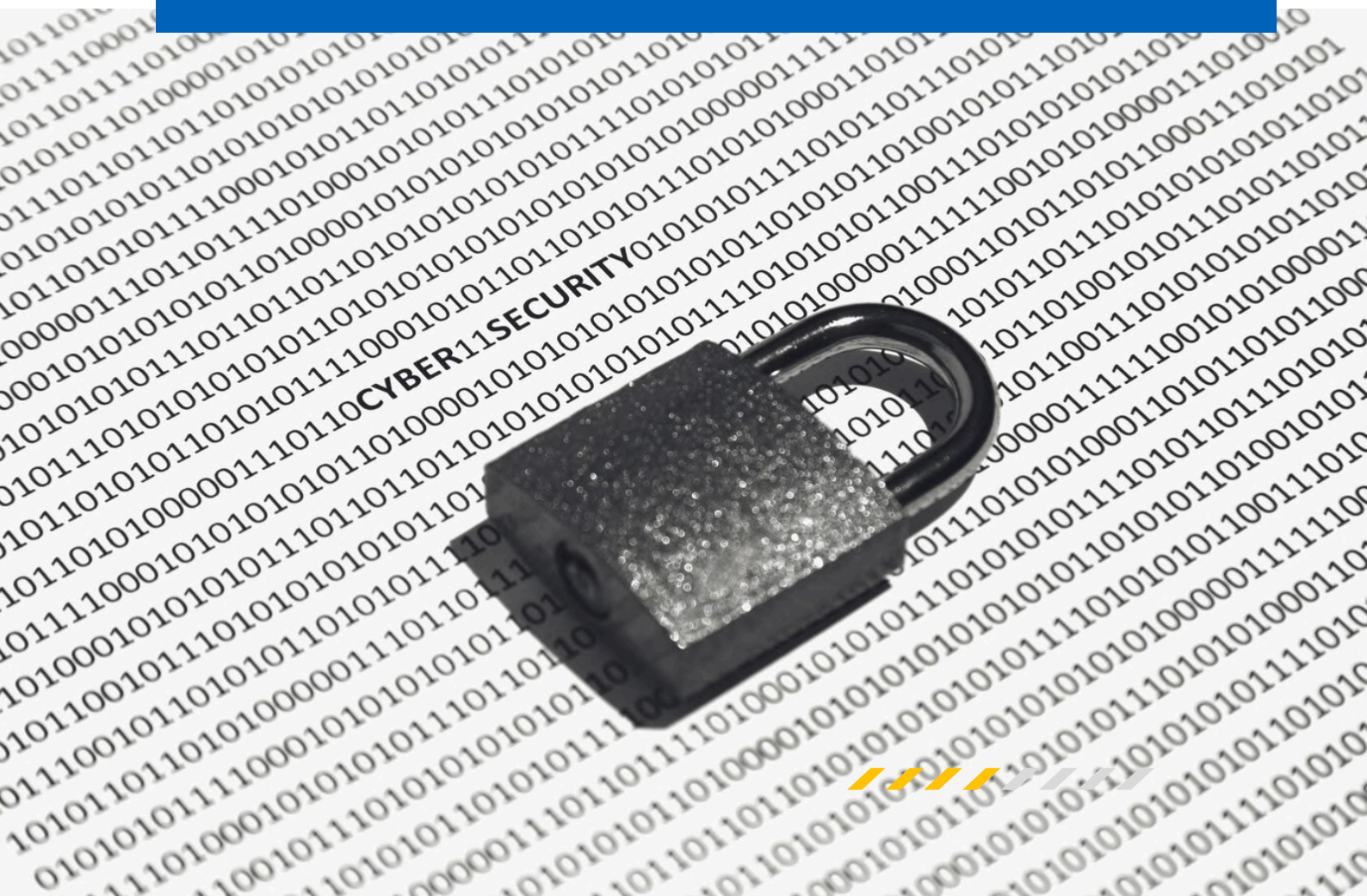
ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

4. Τι καθιστά έναν σύνδεσμο ύποπτο και ενδεχομένως επιβλαβή;
Α. Χρησιμοποιεί κρυπτογράφηση HTTPS
Β. Ανακατευθύνει σε άλλον ιστότοπο
Γ. Περιέχει ασυνήθιστους χαρακτήρες ή τομείς
Δ. Κοινοποιείται από έναν φίλο σε άμεσο μήνυμα

5. Ποια στρατηγική είναι η πιο αποτελεσματική για την αποτροπή της έκθεσης σε ακατάλληλο περιεχόμενο;
Α. Ελάχιστη χρήση οποιουδήποτε ηλεκτρονικού τσιγάρου
Β. Απενεργοποίηση όλων των ειδοποιήσεων στις συσκευές σας
Γ. Βασίζεστε αποκλειστικά σε λογισμικό προστασίας από ιούς
Δ. Χρήση φίλτρων περιεχομένου και προσαρμογή των ρυθμίσεων απορρήτου

Λύσεις

Ερώτηση 1: Γ
Ερώτηση 2: Β
Ερώτηση 3: Α
Ερώτηση 4: Γ
Ερώτηση 5: Δ



ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

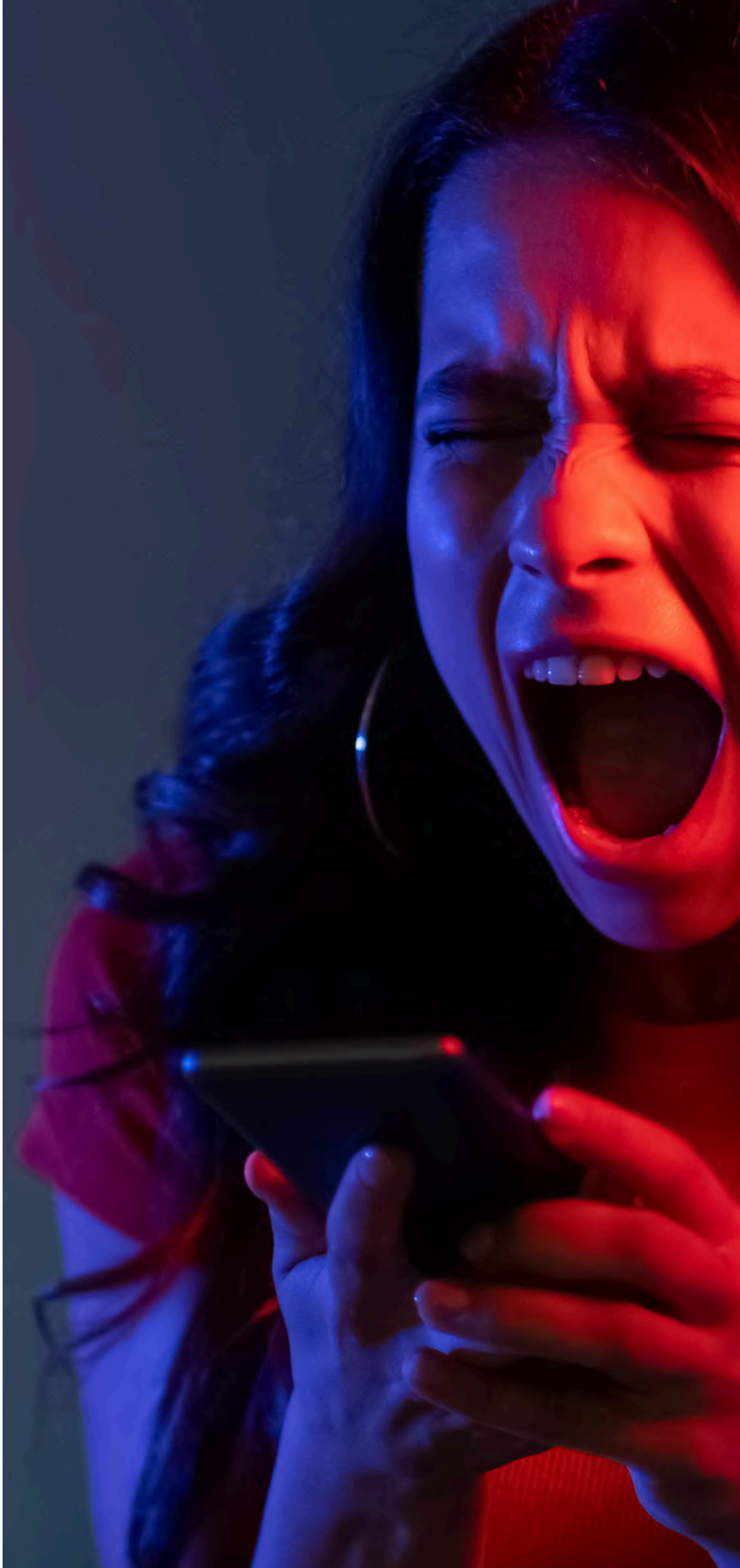
LABC

CWEP Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.