



ΕΝΟΤΗΤΑ 5

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ



erasmediah.eu



**Co-funded by
the European Union**



Μάθημα 5.2

Προστασία προσωπικών πληροφοριών και απορρήτου στο διαδίκτυο



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 (ΕΑΕΑ). Η Ευρωπαϊκή Ένωση και ο ΕΑΕΑ δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Μάθημα 5.2

Προστασία προσωπικών πληροφοριών και απορρήτου στο διαδίκτυο

Στόχοι:

- Να ευαισθητοποιήσει το κοινό σχετικά με τους κινδύνους που εγκυμονεί η κοινοποίηση προσωπικών πληροφοριών στο διαδίκτυο και τον τρόπο με τον οποίο μπορεί να γίνει κακή χρήση τους.
- Να εξοπλίσει τους μαθητές με πρακτικές στρατηγικές για τον έλεγχο του ψηφιακού τους αποτυπώματος, συμπεριλαμβανομένων των ρυθμίσεων απορρήτου δεδομένων, της ασφαλούς επικοινωνίας και της αποφυγής υπερβολικής κοινοποίησης.
- Να διερευνηθούν παραδείγματα παραβιάσεων της ιδιωτικής ζωής, καταδεικνύοντας τον αντίκτυπό τους στα άτομα και πώς θα μπορούσαν να είχαν αποτραπεί.
- Να εμπνεύσει προληπτική συμπεριφορά μέσω της οικοδόμησης συνηθειών όπως η αναθεώρηση των δικαιωμάτων εφαρμογών, η κατανόηση των όρων παροχής υπηρεσιών και η χρήση εργαλείων απορρήτου.

Βασικά Μηνύματα:

- Κάθε πληροφορία που κοινοποιείτε στο διαδίκτυο – από φωτογραφίες και likes μέχρι δεδομένα τοποθεσίας – μπορεί να γίνει αντικείμενο εκμετάλλευσης από κυβερνοεγκληματίες ή εταιρείες. Η γνώση του τρόπου περιορισμού της πρόσβασης είναι η πρώτη σας γραμμή άμυνας.
- Η προστασία του απορρήτου σας δεν έχει να κάνει με την αποφυγή του διαδικτύου. Έχει να κάνει με το να είστε έξυπνοι και συνειδητοί. Απλά εργαλεία και αποφάσεις μπορούν να διατηρήσουν τα δεδομένα σας ασφαλή χωρίς να θυσιάσουν την ψηφιακή σας ζωή.



ΕΙΔΟΣ ΜΑΘΗΜΑΤΟΣ:





Επισκόπηση μαθήματος

Με τόσο μεγάλο μέρος της ζωής μας να συμβαίνει στο διαδίκτυο, η διατήρηση της ασφάλειας των προσωπικών σας πληροφοριών δεν ήταν ποτέ πιο σημαντική. Αυτό το μάθημα υπογραμμίζει γιατί η προστασία του απορρήτου σας είναι σημαντική. Θα διερευνήσουμε πώς απλές συνήθειες, όπως η υπερβολική κοινοποίηση στα μέσα κοινωνικής δικτύωσης ή η αποδοχή δικαιωμάτων εφαρμογών χωρίς σκέψη, μπορούν να αφήσουν τα δεδομένα σας εκτεθειμένα. Αναγνωρίζοντας αυτούς τους κινδύνους και υιοθετώντας πρακτικές στρατηγικές, θα αποκτήσετε τα εργαλεία για να προστατεύσετε την ψηφιακή σας ταυτότητα και να αναλάβετε τον έλεγχο της διαδικτυακής σας ασφάλειας.

Το εργαστήριο οργανώνεται σε 4 βήματα:

- 1: Εισαγωγή στους κινδύνους για την ιδιωτικότητα στο διαδίκτυο (15 λεπτά)
- 2: Εξερεύνηση παραβιάσεων απορρήτου στον πραγματικό κόσμο (10 λεπτά)
- 3: Πρακτικές στρατηγικές για την προστασία των προσωπικών δεδομένων (10 λεπτά)
- 4: Τελικός αναστοχασμός και βασικά συμπεράσματα (5 λεπτά)



Βήμα 1

Εισαγωγή στους κινδύνους για την προστασία της ιδιωτικής ζωής στο διαδίκτυο

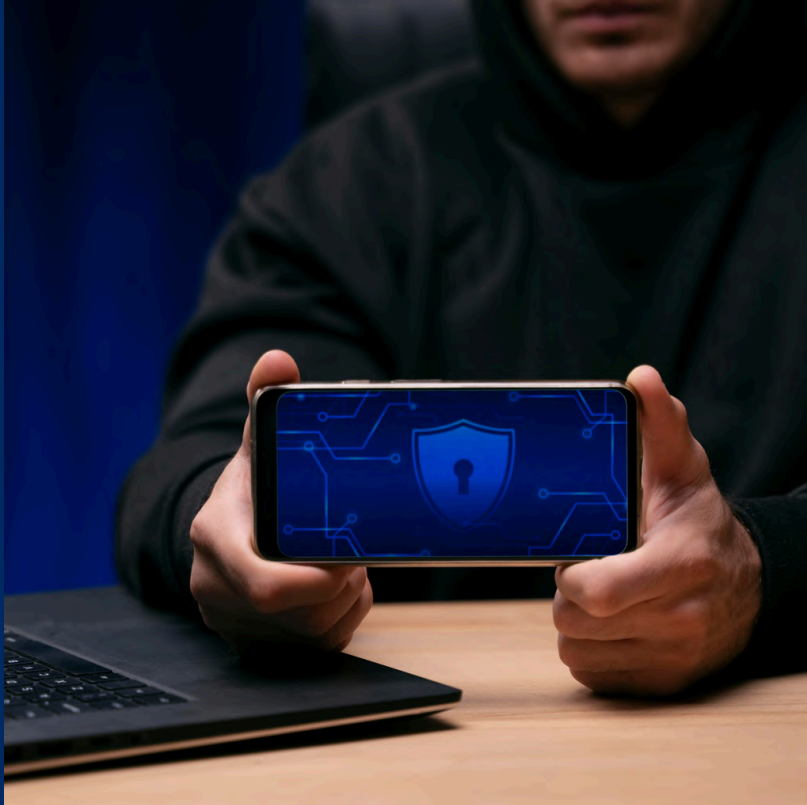
Σας έχει τύχει ποτέ να κατεβάσετε μια νέα εφαρμογή, να αποδεχτείτε τα δικαιώματά της και να μην έχετε σκεφτεί ποτέ τι πληροφορίες συλλέγει;

Όταν χρησιμοποιούμε το Διαδίκτυο, τα προσωπικά μας δεδομένα - όπως η τοποθεσία, οι κωδικοί πρόσβασης και οι συνήθειες περιήγησης - μπορούν εύκολα να εκτεθούν. Τώρα, θα διερευνήσουμε ποιοι κίνδυνοι απορρήτου υπάρχουν και πώς μπορεί να σας επηρεάσουν.

Ως πρώτο βήμα, **διαβάστε την ενότητα «Κοινές απειλές για την προστασία της ιδιωτικής ζωής στο διαδίκτυο» από αυτό το άρθρο: builtin.com/articles**

Ενώ διαβάζετε, γράψτε με λίγα λόγια σε ένα κομμάτι χαρτί:

- Η απειλή για την ιδιωτικότητα που θεωρείτε πιο ενοχλητική και γιατί αυτή η απειλή σας ξεχωρίζει ή σας φαίνεται επικίνδυνη.



Βήμα 1

Εισαγωγή στους κινδύνους για την προστασία της ιδιωτικής ζωής στο διαδίκτυο

Μόλις τελειώσετε την ανάγνωση, ας συζητήσουμε:

- Ποια απειλή απορρήτου σας εξέπληξε περισσότερο και γιατί;
- Πώς πιστεύετε ότι επηρεάζουν αυτές οι απειλές την καθημερινότητά μας;
- Τι θα μπορούσε να συμβεί αν τους αγνοήσουμε;

Μη διστάσετε να μοιραστείτε ένα σύντομο παράδειγμα από την εμπειρία σας - είτε πρόκειται για αδύναμους κωδικούς πρόσβασης, παρακολούθηση δεδομένων είτε για κάτι άλλο που έχετε δει ή ακούσει. Αν δεν είστε σίγουροι, απλώς ακούγοντας τους άλλους θα σας δοθούν ιδέες!



Βήμα 2

Εξερευνώντας παραβιάσεις απορρήτου στον πραγματικό κόσμο

Ας δούμε ένα πραγματικό παράδειγμα του τι συμβαίνει όταν δεν είμαστε προσεκτικοί με τα προσωπικά μας στοιχεία στο διαδίκτυο.

Φανταστείτε το εξής: Η Σάρα λατρεύει να μοιράζεται τη ζωή της στα μέσα κοινωνικής δικτύωσης. Δημοσιεύει φωτογραφίες από το νέο της διαμέρισμα, μιλάει για την καθημερινότητά της, ακόμη και μοιράζεται την τοποθεσία της όταν βρίσκεται στην αγαπημένη της καφετέρια. Μια μέρα, η Σάρα ανακαλύπτει ότι ο τραπεζικός της λογαριασμός έχει αδειάσει. Πώς; Ένας κυβερνοεγκληματίας συγκέντρωσε τα προσωπικά της στοιχεία από τις δημόσιες αναρτήσεις της - την τοποθεσία της, τις συνήθειες του τρόπου ζωής της, ακόμη και υποδείξεις για τους κωδικούς πρόσβασής της - για να αποκτήσει πρόσβαση στους λογαριασμούς της. Όλα αυτά εξαιτίας της υπερβολικής κοινοποίησης!

Τώρα, σκεφτείτε τις ακόλουθες ερωτήσεις:

Τι πήγε στραβά; Ποιες ενέργειες ή συνήθειες οδήγησαν στην παραβίαση της ιδιωτικότητας;

Πώς θα μπορούσε να είχε αποτραπεί αυτή η κατάσταση; Ποιες απλές αλλαγές θα έκαναν τη διαφορά;

Καταγράψτε τις απαντήσεις σας και να είστε έτοιμοι να τις μοιραστείτε με την ομάδα.



Βήμα 2

Εξερευνώντας παραβιάσεις απορρήτου στον πραγματικό κόσμο

Ας το συζητήσουμε μαζί:

- Τι πιστεύετε ότι πήγε στραβά στην περίπτωση της Σάρα;
- Γιατί πιστεύετε ότι τέτοιες παραβιάσεις απορρήτου συμβαίνουν τόσο εύκολα;

Στο τέλος, αφιερώστε λίγο χρόνο για να σκεφτείτε:

- Έχετε αντιμετωπίσει ποτέ εσείς ή κάποιος που γνωρίζετε κάποιο πρόβλημα απορρήτου στο διαδίκτυο; Θα μπορούσε να είναι ένα ύποπτο email, ένας παραβιασμένος λογαριασμός ή ένα περιστατικό υπερβολικής κοινοποίησης στα μέσα κοινωνικής δικτύωσης.
- Πώς συνέβη αυτό, και ποιο ήταν το αποτέλεσμα;

Αν νιώθετε άνετα, μοιραστείτε την ιστορία σας με την ομάδα. Αν όχι, δεν πειράζει - απλώς ακούγοντας θα πάρετε πολύτιμες πληροφορίες.



Βήμα 3

Πρακτικές στρατηγικές για την προστασία των προσωπικών δεδομένων

Τώρα που διερευνήσαμε τους κινδύνους για την ιδιωτικότητα και τα παραδείγματα από τον πραγματικό κόσμο, ας επικεντρωθούμε σε πρακτικά βήματα για να προστατεύσουμε τον εαυτό μας (τα δεδομένα μας) στο διαδίκτυο.

Θα ξεκινήσουμε με ένα σύντομο βίντεο: <https://youtu.be/6WQzMAd6mJs>

Δώστε προσοχή στις βασικές συμβουλές που κοινοποιούνται.

Αφού παρακολουθήσετε, γράψτε **τρεις συγκεκριμένες ενέργειες** που μπορείτε να κάνετε για να βελτιώσετε το διαδικτυακό σας απόρρητο. Σκεφτείτε:

- Την προσαρμογή των ρυθμίσεων απορρήτου στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης.
- Τον έλεγχο δικαιωμάτων εφαρμογών στο τηλέφωνό σας.
- Να είστε προσεκτικοί σχετικά με τα προσωπικά στοιχεία που κοινοποιείτε στο διαδίκτυο, ειδικά σε δημόσιες πλατφόρμες.



Βήμα 3

Πρακτικές στρατηγικές για την προστασία των προσωπικών δεδομένων

Τώρα, ας μοιραστούμε **μια στρατηγική** που σκοπεύετε να εφαρμόσετε. Για παράδειγμα:

- «Θα ελέγξω όλες τις εφαρμογές στο τηλέφωνό μου απόψε και θα αφαιρέσω όσες δεν χρησιμοποιώ»
- «Θα περιορίσω ποιος μπορεί να δει τις αναρτήσεις μου στο Facebook/Instagram και θα απενεργοποιήσω τη δημόσια ορατότητα για το προφίλ μου»

Ας συζητήσουμε:

1. Τι κάνει αυτές τις συνήθειες απορρήτου να φαίνονται εύκολες ή δύσκολες στην υιοθέτηση;
 - Μήπως νιώθουμε υπερβολικά άνετα να κοινοποιούμε πληροφορίες στο διαδίκτυο;
 - Πιστεύουμε ότι οι ρυθμίσεις απορρήτου και τα δικαιώματα είναι περίπλοκα ή χρονοβόρα;
2. Γιατί τόσοι πολλοί άνθρωποι αγνοούν απλές πρακτικές απορρήτου, ακόμη και όταν γνωρίζουν τους κινδύνους;
 - Μήπως επειδή δεν πιστεύουν ότι θα τους συμβεί κάποια παραβίαση;
 - Πιστεύετε ότι οφείλεται στο ότι οι άνθρωποι δεν γνωρίζουν τα εργαλεία ή τις συνήθειες που πρέπει να χρησιμοποιούν;
3. Πώς μπορείτε να παραμείνετε παρακινημένοι ώστε να τηρείτε αυτές τις συνήθειες;
 - Για παράδειγμα, ο ορισμός υπενθυμίσεων για την ενημέρωση των κωδικών πρόσβασης ή ο τακτικός έλεγχος των ρυθμίσεων των μέσων κοινωνικής δικτύωσης.

Βήμα 4

Τελικός αναστοχασμός και βασικά συμπεράσματα

Για να ολοκληρώσουμε αυτό το εργαστήριο, ας αφιερώσουμε λίγο χρόνο για να αναλογιστούμε όσα μάθαμε και πώς μπορούμε να τα εφαρμόσουμε στην καθημερινότητά μας.

Αναρωτηθείτε: Ποια είναι μια συνήθεια που μπορείτε να αλλάξετε σήμερα για να βελτιώσετε το απόρρητό σας στο διαδίκτυο; Θα μπορούσε να είναι κάτι απλό, όπως η απενεργοποίηση της κοινοποίησης τοποθεσίας, ο έλεγχος των ρυθμίσεων απορρήτου των μέσων κοινωνικής δικτύωσης ή η μεγαλύτερη προσοχή σε ό,τι δημοσιεύετε. Τώρα, σκεφτείτε πώς μπορείτε να βοηθήσετε τους άλλους: Πώς θα μοιραστείτε όσα μάθατε σήμερα με έναν φίλο, μέλος της οικογένειας ή συνάδελφο; Ακόμα και μικρές συμβουλές, όπως το να εξηγήσετε γιατί οι ισχυροί κωδικοί πρόσβασης είναι σημαντικοί ή να δείξετε σε κάποιον πώς να ελέγχει τα δικαιώματα εφαρμογών, μπορούν να κάνουν μεγάλη διαφορά.





Σύνοψη των βασικών συμπερασμάτων

- Να είστε προσεκτικοί με το τι κοινοποιείτε στο διαδίκτυο: Μικρές λεπτομέρειες, όπως τοποθεσίες ή συνήθειες, μπορούν να χρησιμοποιηθούν λανθασμένα αν πέσουν σε λάθος χέρια.
- Ελέγξτε και προσαρμόστε τις ρυθμίσεις απορρήτου: Ελέγχετε τακτικά τα μέσα κοινωνικής δικτύωσης, τα δικαιώματα εφαρμογών και τις ρυθμίσεις του λογαριασμού σας για να περιορίσετε την περιττή κοινοποίηση δεδομένων.
- Περιορίστε τα προσωπικά στοιχεία που δημοσιεύετε δημόσια: Αποφύγετε την κοινοποίηση ευαίσθητων λεπτομερειών, όπως διευθύνσεις, ρουτίνες ή προσωπικά αναγνωριστικά στοιχεία, στα μέσα κοινωνικής δικτύωσης ή σε άλλες πλατφόρμες.
- Να είστε προσεκτικοί με εφαρμογές και συνδέσμους: Σκεφτείτε πριν κάνετε κλικ σε συνδέσμους, κατεβάσετε εφαρμογές ή παραχωρήσετε δικαιώματα - εμπιστευτείτε μόνο επαληθευμένες πηγές.
- Ξεκινήστε με μικρά βήματα: Απλές συνήθειες, όπως η απενεργοποίηση της παρακολούθησης τοποθεσίας ή ο περιορισμός των δημόσιων αναρτήσεων, μπορούν να έχουν μεγάλο αντίκτυπο στην προστασία του απορρήτου σας.



Οδηγίες για εργαζόμενους στον τομέα της νεολαίας, εκπαιδευτικούς και δασκάλους

Σκοπός:

Στόχος αυτού του μαθήματος είναι να παρέχει στους συμμετέχοντες πρακτικές δεξιότητες και γνώσεις για την προστασία των προσωπικών τους πληροφοριών και τη διατήρηση του διαδικτυακού απορρήτου. Μέσω διαδραστικών δραστηριοτήτων, παραδειγμάτων από την πραγματική ζωή και στοχαστικών συζητήσεων, οι συμμετέχοντες θα εντοπίσουν κοινούς κινδύνους για το διαδικτυακό απόρρητο, θα αποκτήσουν εικόνα για τον αντίκτυπο των παραβιάσεων του απορρήτου και θα αναπτύξουν εφαρμόσιμες στρατηγικές για την προστασία των δεδομένων τους. Μέχρι το τέλος της συνεδρίας, οι μαθητές θα αισθάνονται πιο συνειδητοποιημένοι, προετοιμασμένοι και αφοσιωμένοι στην υιοθέτηση συνηθειών που ενισχύουν την ψηφιακή τους ασφάλεια.

Απαιτούμενα υλικά:

- Σύνδεση στο Διαδίκτυο για αναπαραγωγή βίντεο ή άρθρου
- Προβολέας και οθόνη
- Ομιλητές
- Πρόσβαση σε προτεινόμενα εργαλεία κυβερνοασφάλειας
- Χαρτί γραφικών παραστάσεων ή μαρκαδόροι λευκού πίνακα
- Στυλό, μολύβια και φύλλα σημειώσεων





Βήμα 1: Εισαγωγή στους κινδύνους για την ιδιωτικότητα στο διαδίκτυο (15 λεπτά)

1. Ξεκινήστε με μια σχετική ερώτηση: «Πότε ήταν η τελευταία φορά που κατεβάσατε μια εφαρμογή, αποδεχτήκατε τα δικαιώματά της ή κοινοποιήσατε μια ανάρτηση στο διαδίκτυο; Σκεφτήκατε ποιες προσωπικές πληροφορίες μπορεί να δίνετε;». Εξηγήστε ότι αυτές οι μικρές, καθημερινές ενέργειες μπορούν να εκθέσουν ακούσια ιδιωτικά στοιχεία όπως η τοποθεσία, οι συνήθειες περιήγησης ή οι προσωπικές σας ρουτίνες σε τρίτους ή κυβερνοεγκληματίες.

2. Τονίστε ότι η προστασία των προσωπικών δεδομένων είναι απαραίτητη στον σημερινό ψηφιακό κόσμο. Επισημάνετε ότι φαινομενικά ακίνδυνες συμπεριφορές - όπως η κοινοποίηση μιας φωτογραφίας ή η παροχή πρόσβασης σε εφαρμογές στις επαφές σας - μπορεί να έχουν ακούσιες συνέπειες. Χρησιμοποιήστε μια απλή αναλογία: «Οι προσωπικές σας πληροφορίες είναι σαν κομμάτια ενός παζλ. Ένα κομμάτι από μόνο του μπορεί να φαίνεται ακίνδυνο, αλλά όταν συνδυάζεται με άλλα, μπορεί να αποκαλύψει πολλά για εσάς».

3. Δραστηριότητα – ανάγνωση άρθρων και αναστοχασμός

Διανείμετε ή κοινοποιήστε την ενότητα «Κοινές απειλές για την προστασία της ιδιωτικής ζωής στο διαδίκτυο» από το άρθρο: Τι είναι η προστασία της ιδιωτικής ζωής στο διαδίκτυο;.

Ζητήστε από τους συμμετέχοντες να:

- Προσδιορίστε την απειλή για την ιδιωτικότητα που τους ανησυχεί περισσότερο.
- Σκεφτείτε γιατί αυτή η απειλή σας φαίνεται ιδιαίτερα επικίνδυνη ή εκπληκτική.

Ενθαρρύνετε τους να καταγράψουν σύντομες σκέψεις για να προετοιμαστούν για την ομαδική συζήτηση.





Βήμα 1: Εισαγωγή στους κινδύνους για την ιδιωτικότητα στο διαδίκτυο (15 λεπτά)

4. Διευκολύνετε μια σύντομη συζήτηση χρησιμοποιώντας αυτές τις προτροπές:

- «Ποια απειλή για την ιδιωτικότητα σας έκανε εντύπωση περισσότερο και γιατί;»
- «Πώς επηρεάζουν αυτοί οι κίνδυνοι τη διαδικτυακή σας συμπεριφορά ή τις συνήθειές σας;»

Προσκαλέστε μερικούς συμμετέχοντες να μοιραστούν τις σκέψεις τους, ενισχύοντας ότι η επίγνωση αυτών των κινδύνων είναι το πρώτο βήμα για την καλύτερη προστασία των προσωπικών δεδομένων.

5. Σύνοψη - συνοψίστε το βασικό σημείο της συζήτησης (για παράδειγμα: Αναγνωρίζοντας αυτούς τους κινδύνους για την ιδιωτικότητα, αναλαμβάνετε τον έλεγχο της διαδικτυακής σας παρουσίας. Η επίγνωση σας επιτρέπει να λαμβάνετε πιο έξυπνες αποφάσεις σχετικά με το τι κοινοποιείτε και τον τρόπο με τον οποίο αλληλεπιδράτε στο διαδίκτυο).





Βήμα 2: Διερεύνηση παραβιάσεων απορρήτου στον πραγματικό κόσμο (10 λεπτά)

1. Ξεκινήστε κοινοποιώντας ένα σχετικό και επηρεαστικό σενάριο για να δείξετε πώς η υπερβολική κοινοποίηση στο διαδίκτυο μπορεί να οδηγήσει σε σοβαρές παραβιάσεις της ιδιωτικότητας. Εξηγήστε στους συμμετέχοντες ότι αυτή η ιστορία δεν είναι μοναδική. Πολλοί άνθρωποι μοιράζονται εν αγνοία τους προσωπικά στοιχεία που οι κυβερνοεγκληματίες ή κακόβουλα άτομα μπορούν να χρησιμοποιήσουν για να τους παρακολουθήσουν, να παραβιάσουν τους λογαριασμούς τους ή ακόμα και να κλέψουν την ταυτότητά τους. Τονίστε ότι οι παραβιάσεις της ιδιωτικότητας συχνά ξεκινούν με μικρά, φαινομενικά ακίνδυνα κομμάτια πληροφοριών.

2. Δείξτε ένα σύντομο γραπτό σενάριο στους συμμετέχοντες, είτε βασισμένο στην ιστορία της Σάρα είτε σε μια παρόμοια υποθετική κατάσταση:

Παράδειγμα ενός άλλου σεναρίου:

«Ο Άλεξ κατέβασε μια δωρεάν εφαρμογή για κινητά χωρίς να διαβάσει τα δικαιώματα. Η εφαρμογή είχε πρόσβαση στην τοποθεσία, τις επαφές και τα αρχεία πολυμέσων του. Λίγο αργότερα, παρατήρησε ότι στέλνονταν παράξενα μηνύματα στους φίλους του. Αποδείχθηκε ότι η εφαρμογή συνέλεγε τα δεδομένα του και έστελνε ανεπιθύμητα μηνύματα χρησιμοποιώντας τον λογαριασμό του».





Βήμα 2: Διερεύνηση παραβιάσεων απορρήτου στον πραγματικό κόσμο (10 λεπτά)

3. Δώστε στους συμμετέχοντες οδηγίες:

Εργαστείτε ατομικά ή σε μικρές ομάδες για να αναλύσετε την κατάσταση.

- Τι πήγε στραβά; Ποιες ενέργειες ή συμπεριφορές προκάλεσαν την παραβίαση;
- Πώς θα μπορούσε να είχε αποτραπεί αυτό; Προσδιορίστε απλά βήματα ή συνήθειες για την προστασία των προσωπικών πληροφοριών.

Καταγράψτε σύντομα τις σκέψεις σας.

4. Αφήστε τους συμμετέχοντες να μοιραστούν τις σκέψεις τους, ως εξής:

- «Έχετε εσείς ή κάποιος που γνωρίζετε αντιμετωπίσει παρόμοιο πρόβλημα, όπως ηλεκτρονικό ψάρεμα (phishing), hacking ή υπερβολική κοινοποίηση;»
- «Γιατί οι άνθρωποι μοιράζονται τόσες πολλές προσωπικές πληροφορίες χωρίς να λαμβάνουν υπόψη τους κινδύνους;»
- Πιθανοί λόγοι:
 - Αξιόπιστες εφαρμογές ή πλατφόρμες.
 - Μη συνειδητοποιώντας τις συνέπειες.
 - Μπερδεμένες ρυθμίσεις απορρήτου.

Ενθαρρύνετε την ανοιχτή, υποστηρικτική ανταλλαγή εμπειριών ή ιδεών.





Βήμα 3: Πρακτικές στρατηγικές για την προστασία των προσωπικών πληροφοριών (10 λεπτά)

1. Προβολή βίντεο

Προβολή του βίντεο με τίτλο «Πώς να προστατεύσετε τα προσωπικά σας δεδομένα στο διαδίκτυο». Ενθαρρύνετε τους συμμετέχοντες να δώσουν ιδιαίτερη προσοχή στις πρακτικές, εφαρμόσιμες στρατηγικές που παρουσιάζονται στο βίντεο. Τονίστε ότι αυτές οι συμβουλές είναι εύκολες στην εφαρμογή, αλλά μπορούν να βελτιώσουν σημαντικά το διαδικτυακό απόρρητο.

2. Δραστηριότητα – «Προσωπικό σχέδιο απορρήτου»

Ζητήστε από τους συμμετέχοντες να γράψουν τρεις ενέργειες που θα αναλάβουν για να προστατεύσουν το απόρρητό τους στο διαδίκτυο.

Ενθαρρύνετε τους να σκεφτούν:

- Προσαρμογή των ρυθμίσεων απορρήτου των μέσων κοινωνικής δικτύωσης.
- Έλεγχος δικαιωμάτων εφαρμογών στις συσκευές τους.
- Να έχουν επίγνωση των όσων δημοσιεύουν δημόσια.

3. Κοινή χρήση εντός της ομάδας.

Προσκαλέστε τους συμμετέχοντες να μοιραστούν μια ενέργεια που σκοπεύουν να εφαρμόσουν με την ομάδα. Χρησιμοποιήστε τις ακόλουθες υποδείξεις για να καθοδηγήσετε τη συζήτηση:

- «Ποια στρατηγική σας φαίνεται πιο εύκολη να ξεκινήσετε σήμερα και γιατί;»
- «Ποιες προκλήσεις μπορεί να αντιμετωπίσετε προσπαθώντας να υιοθετήσετε αυτές τις συνήθειες;»
- «Πώς μπορούμε να ξεπεράσουμε συνηθισμένα εμπόδια, όπως το να ξεχνάμε να προσαρμόσουμε τις ρυθμίσεις ή να μας μπερδεύουν τα εργαλεία απορρήτου;»

Ενθαρρύνετε την ομάδα να παρέχει πρακτικές συμβουλές ή να μοιραστεί προσωπικές εμπειρίες για το πώς ξεπέρασαν παρόμοιες προκλήσεις. Τονίστε ότι η συνεπής λήψη μικρών βημάτων μπορεί να οδηγήσει σε σημαντικές βελτιώσεις στην προστασία της ιδιωτικής ζωής στο διαδίκτυο.

4. Επιπλέον, μπορείτε να ζητήσετε από τους συμμετέχοντες να σκεφτούν πώς μπορούν να μοιραστούν αυτές τις στρατηγικές με φίλους ή συγγενείς.





Βήμα 4: Τελικός στοχασμός και βασικά συμπεράσματα:

1. Ζητήστε από τους συμμετέχοντες να αναλογιστούν:

- «Ποια είναι μια συνήθεια που θα αλλάξετε για να βελτιώσετε το διαδικτυακό σας απόρρητο ξεκινώντας από σήμερα;»
- «Πώς θα μοιραστείτε αυτά που έχετε μάθει με φίλους ή συγγενείς;»

2. Ενισχύστε τα κύρια σημεία του μαθήματος:

- Μικρές αλλαγές, όπως η προσαρμογή των ρυθμίσεων ή ο περιορισμός του περιεχομένου που κοινοποιείτε, έχουν μεγάλο αντίκτυπο.
- Η προστασία των δεδομένων σας σας δίνει τον έλεγχο της ψηφιακής σας ταυτότητας.

3. Ολοκληρώστε τη συνεδρία με μια καταληκτική πρόταση. Για παράδειγμα: «Τα προσωπικά σας στοιχεία είναι πολύτιμα. Κάντε μικρά, έξυπνα βήματα για να τα προστατεύσετε και θα παραμείνετε ασφαλέστεροι στο διαδίκτυο».

Βασικά σημεία:

Στο τέλος του μαθήματος, οι συμμετέχοντες θα πρέπει να κατανοήσουν σαφώς ότι το διαδικτυακό απόρρητο ξεκινά με την επίγνωση και μικρά, εφαρμόσιμα βήματα. Απλές αλλαγές, όπως η προσαρμογή των δικαιωμάτων εφαρμογών, ο έλεγχος των ρυθμίσεων απορρήτου στα μέσα κοινωνικής δικτύωσης και η επίγνωση του τι κοινοποιείται δημόσια, μπορούν να μειώσουν σημαντικά τους κινδύνους. Ενθαρρύνετε τους συμμετέχοντες να αναλάβουν τον έλεγχο της ψηφιακής τους συμπεριφοράς αναπτύσσοντας συνήθειες όπως ο έλεγχος του ποιος έχει πρόσβαση στα δεδομένα τους και η επιφύλαξη ύποπτων συνδέσμων ή μηνυμάτων. Ενισχύστε την ιδέα ότι η προστασία των προσωπικών πληροφοριών δίνει τη δυνατότητα στα άτομα να διατηρούν τον έλεγχο της ψηφιακής τους ταυτότητας και της ασφάλειάς τους.





Παρακολούθηση και δραστηριότητες στο σπίτι

Ζητήστε από τους συμμετέχοντες να αφιερώσουν τις επόμενες ημέρες στην εφαρμογή τουλάχιστον μίας ενέργειας απορρήτου που εντόπισαν κατά τη διάρκεια της συνεδρίας. Αυτό θα μπορούσε να περιλαμβάνει τον έλεγχο των ρυθμίσεων απορρήτου σε μια πλατφόρμα κοινωνικής δικτύωσης, τη διαγραφή αχρησιμοποίητων εφαρμογών ή την κοινοποίηση συμβουλών απορρήτου με φίλους ή μέλη της οικογένειάς τους. Προτείνετε να καταγράψουν την πρόοδό τους και να σκεφτούν πώς αυτές οι αλλαγές τους κάνουν να αισθάνονται πιο ασφαλείς στο διαδίκτυο. Επιπλέον, ενθαρρύνετε τους συμμετέχοντες να εξερευνήσουν εργαλεία όπως το DuckDuckGo (μια ιδιωτική μηχανή αναζήτησης) ή το Google Privacy Checkup για να δουν πόσο εύκολα μπορούν να βελτιώσουν την ασφάλειά τους στο διαδίκτυο. Εξετάστε το ενδεχόμενο να οργανώσετε μια συνεδρία παρακολούθησης όπου οι συμμετέχοντες μπορούν να μοιραστούν τις εμπειρίες τους και να συζητήσουν τις προκλήσεις που αντιμετώπισαν.

Συμβουλές για εκπαιδευτικούς:

Συνιστάται να συμπεριληφθούν παραδείγματα από την πραγματική ζωή στη συζήτηση, ώστε να καταστεί κατανοητή η έννοια του διαδικτυακού απορρήτου. Χρησιμοποιήστε σενάρια που περιλαμβάνουν υπερβολική κοινοποίηση στα μέσα κοινωνικής δικτύωσης, παραβιάσεις δεδομένων ή δικαιώματα χρήσης εφαρμογών για να δείξετε πώς οι μικρές συνήθειες μπορούν να έχουν μεγάλες συνέπειες. Δημιουργήστε έναν υποστηρικτικό χώρο για τους συμμετέχοντες, ώστε να μοιράζονται τις εμπειρίες τους χωρίς κριτική. Για να διασφαλίσετε τη συνεχή εμπλοκή, ενσωματώστε σύντομες, πρακτικές εργασίες στα μαθήματα, όπως η επίδειξη του τρόπου προσαρμογής των ρυθμίσεων απορρήτου ή η αναγνώριση ύποπτων συνδέσμων. Επανεξετάζετε τακτικά το θέμα για να διατηρείτε την ευαισθητοποίησή σας σχετικά με το απόρρητο και ενθαρρύνετε τους μαθητές να βλέπουν την προστασία των πληροφοριών τους ως μια συνήθεια ζωής.





Εργαλεία

DuckDuckGo



Το DuckDuckGo είναι μια μηχανή αναζήτησης που εστιάζει στην προστασία της ιδιωτικής ζωής και δεν παρακολουθεί το ιστορικό αναζήτησής σας ούτε συλλέγει προσωπικά δεδομένα. Διασφαλίζει ότι οι αναζητήσεις σας παραμένουν ιδιωτικές και βοηθά στην ελαχιστοποίηση του ψηφιακού αποτυπώματος που αφήνετε κατά την περιήγηση.

duckduckgo.com

Έλεγχος απορρήτου Google



Το Google Privacy Checkup είναι ένα ενσωματωμένο εργαλείο που σας βοηθά να διαχειρίζεστε τις ρυθμίσεις του Λογαριασμού σας Google. Σας επιτρέπει να ελέγχετε και να προσαρμόζετε τα προσωπικά δεδομένα που συλλέγονται, ποιος μπορεί να δει τη δραστηριότητά σας και ποιες εφαρμογές έχουν πρόσβαση στις πληροφορίες σας.

myaccount.google.com/privacycheckup



Παραπομπές

- DuckDuckGo (n.d.). Retrieved from <https://duckduckgo.com>
- Farrier, E. (2024, August 21). A guide to protecting your personal information. Retrieved from <https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online>
- Glover, E. (2024, January 24). What Is Online Privacy?. Built In. Retrieved from <https://builtin.com/articles/what-is-online-privacy>
- Google Privacy Checkup (n.d.). Retrieved from <https://myaccount.google.com/privacycheckup>
- Negrean, R. (n.d.). 10 Tips for Protecting Online Privacy: Strategies for Digital Security. Privacy Tutor. Retrieved from <https://privacytutor.net/10-tips-for-protecting-online-privacy>
- Tech Implement Infra Pvt Ltd. (2024, December 8). Essential Tips on Protecting Personal and Professional Data Online. [Video]. YouTube. <https://youtu.be/6WQzMAd6mJs?si=cq1NFnjxu7i8NRk5>
- Webb, M. (2023, November 26). How to Protect Your Online Privacy: 7 Best Practices to Implement Today. Techopedia. Retrieved from <https://www.techopedia.com/how-to/how-to-protect-your-privacy-online>





ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Ποια είναι μια απλή ενέργεια που μπορείτε να κάνετε για να περιορίσετε την κακή χρήση προσωπικών δεδομένων στο διαδίκτυο;

- A. Αποφύγετε εντελώς τη δημιουργία λογαριασμών κοινωνικής δικτύωσης
- B. Απενεργοποιήστε όλες τις ειδοποιήσεις στις συσκευές σας
- Γ. Αποδεχτείτε τα δικαιώματα εφαρμογών χωρίς να τα ελέγξετε
- Δ. Προσαρμόζετε τακτικά τις ρυθμίσεις απορρήτου των μέσων κοινωνικής δικτύωσης

2. Ποιο από τα παρακάτω αποτελεί παράδειγμα υπερβολικής κοινοποίησης που θα μπορούσε να οδηγήσει σε κλοπή ταυτότητας;

- A. Κοινοποίηση φωτογραφίας από διακοπές μόνο με στενούς φίλους
- B. Δημοσίευση της τοποθεσίας και της καθημερινής σας ρουτίνας δημόσια
- Γ. Αποστολή φωτογραφιών των κατοικίδιων ζώων σας μέσω προσωπικού μηνύματος
- Δ. Χρήση emoji για να περιγράψετε τη διάθεσή σας στο διαδίκτυο

3. Πώς μπορεί ο έλεγχος των δικαιωμάτων εφαρμογών να βελτιώσει το απόρρητό σας στο διαδίκτυο;

- A. Σας επιτρέπει να περιορίσετε την πρόσβαση εφαρμογών σε περιττά προσωπικά δεδομένα
- B. Σας βοηθά να κατεβάζετε εφαρμογές πιο γρήγορα παρακάμπτοντας τους ελέγχους δικαιωμάτων
- Γ. Διασφαλίζει ότι όλες οι εφαρμογές στη συσκευή σας ενημερώνονται αυτόματα
- Δ. Επιτρέπει στις εφαρμογές να εκτελούνται πιο ομαλά στη συσκευή σας





ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

4. Γιατί πολλοί άνθρωποι δεν προστατεύουν τα προσωπικά τους στοιχεία στο διαδίκτυο;

A. Τα εργαλεία απορρήτου δεν είναι διαθέσιμα για τους τακτικούς χρήστες

B. Οι άνθρωποι εμπιστεύονται τις εταιρείες για την ασφάλεια των δεδομένων τους

Γ. Οι ρυθμίσεις και τα εργαλεία απορρήτου συχνά παραβλέπονται ή θεωρούνται περίπλοκα

Δ. Οι περισσότεροι άνθρωποι πιστεύουν ότι δεν έχουν προσωπικά δεδομένα που αξίζουν να προστατευτούν

5. Ποια είναι μια καλή συνήθεια που πρέπει να αναπτύξετε για την προστασία των προσωπικών σας πληροφοριών;

A. Χρήση του ίδιου κωδικού πρόσβασης για ευκολία

B. Επιτρέποντας σε εφαρμογές να παρακολουθούν την τοποθεσία σας ανά πάσα στιγμή

Γ. Αγνόηση των όρων παροχής υπηρεσιών

Δ. Να είστε προσεκτικοί σχετικά με την κοινοποίηση ευαίσθητων πληροφοριών σε δημόσιες πλατφόρμες





Λύσεις

Ερώτηση 1: Δ

Ερώτηση 2: Β

Ερώτηση 3: Α

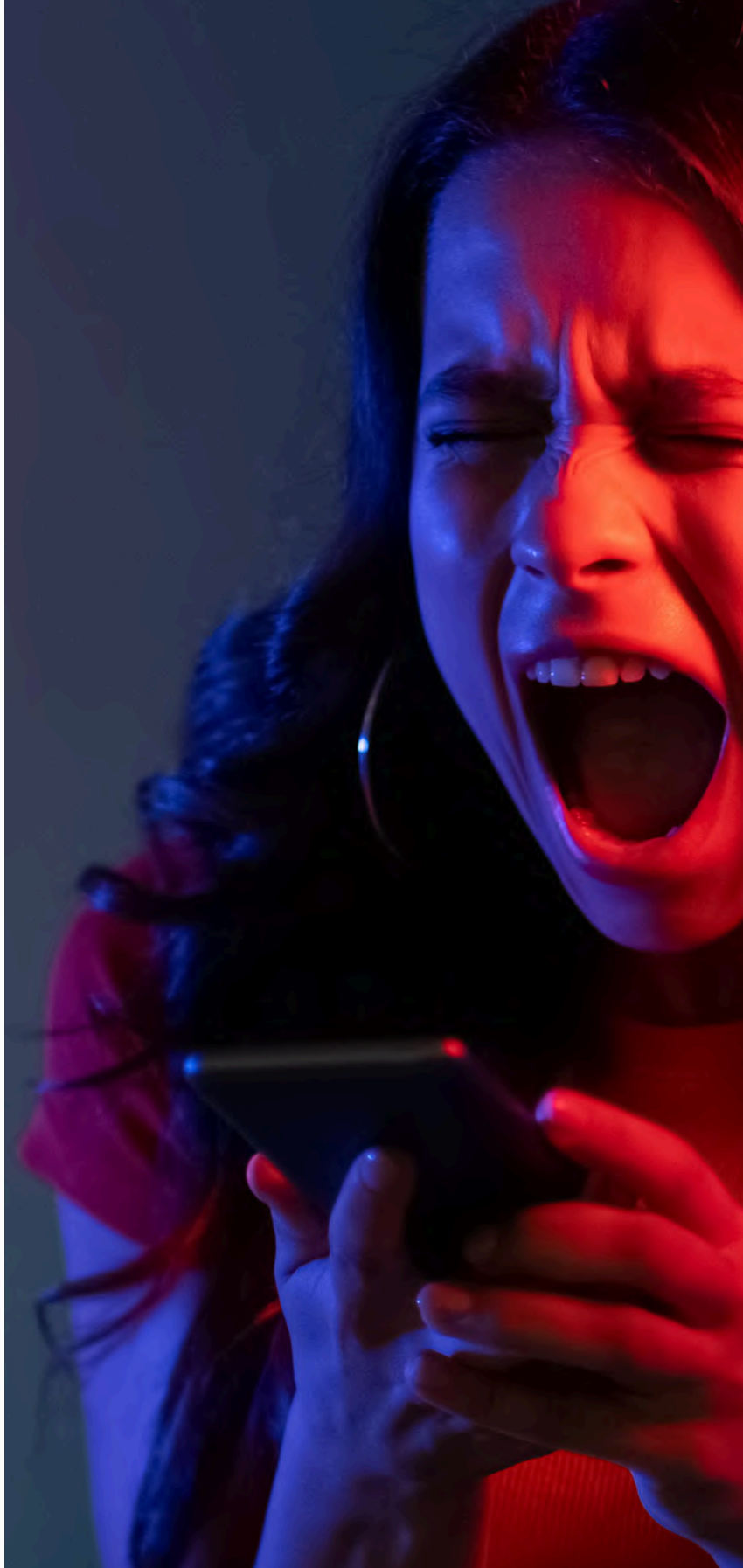
Ερώτηση 4: Γ

Ερώτηση 5: Δ





Centrum Wspierania
Edukacji
i Przedsiębiorczości



**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 (ΕΑΕΑ). Η Ευρωπαϊκή Ένωση και ο ΕΑΕΑ δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.