

Ενότητα 3

Πιθανοί κίνδυνοι κατά τη χρήση των μέσων κοινωνικής δικτύωσης



PR.I.S.C.I.L.L.A
Preventing Incident of Sexual Cyberbullying
in Intellectual disability



Co-funded by
the European Union

Αριθ: 2023-2RO01-KA220-YOU-000174271

1

Πιθανοί κίνδυνοι κατά τη χρήση των μέσων κοινωνικής δικτύωσης



Περίληψη ενότητας

Σε αυτή την ενότητα, θα μάθετε για τους κινδύνους που μπορεί να προκύψουν κατά τη χρήση των μέσων κοινωνικής δικτύωσης. Αυτοί οι κίνδυνοι περιλαμβάνουν:



Εκφοβισμός στον κυβερνοχώρο



Καλλωπισμός



Phishing

Θα μάθετε επίσης πώς να εντοπίζετε αυτούς τους κινδύνους και πώς να παραμένετε ασφαλείς κατά τη χρήση των μέσων κοινωνικής δικτύωσης.



Μαθησιακά αποτελέσματα της ενότητας

Στο τέλος αυτής της ενότητας, θα είστε σε θέση να:

1. Κατανοήστε τι είναι ο διαδικτυακός εκφοβισμός, το grooming και το phishing.
2. Αναγνωρίστε τις καταστάσεις στις οποίες μπορεί να συμβούν αυτοί οι κίνδυνοι.
3. Μάθετε συμβουλές και βήματα για να προστατευτείτε από αυτούς τους κινδύνους.



Περίληψη ενότητας



Αυτή η ενότητα έχει σχεδιαστεί για να σας βοηθήσει:

- Πάρτε θετικά ρίσκα χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης με ασφάλεια
- Νιώστε ότι έχετε τον έλεγχο των ενεργειών σας στο διαδίκτυο
- Δημιουργήστε την ανεξαρτησία σας στη χρήση των κοινωνικών μέσων ενημέρωσης
- Κάντε ασφαλείς επιλογές με αυτοπεποίθηση



Εκφοβισμός στον κυβερνοχώρο

Συμβαίνει όταν οι άνθρωποι χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης ή τις διαδικτυακές πλατφόρμες για να στείλουν κακόβουλα μηνύματα, να δημοσιεύσουν επιζήμια σχόλια ή να διαδώσουν φήμες. Οι κυβερνοεκφοβιστές συχνά κρύβονται πίσω από ψεύτικους λογαριασμούς.



Συμβουλές για την αποφυγή του διαδικτυακού εκφοβισμού



1. **Μην απαντάτε.** Αν κάποιος σας στέλνει κακά μηνύματα, μην απαντάτε.
2. **Αποθηκεύστε τα αποδεικτικά στοιχεία.** Τραβήξτε στιγμιότυπα οθόνης των κακών μηνυμάτων ή σχολίων για να τα δείξετε σε έναν ενήλικα που εμπιστεύεστε.
3. **Αποκλεισμός και αναφορά.** Χρησιμοποιήστε τα εργαλεία της πλατφόρμας για να μπλοκάρετε τον εκφοβιστή και να αναφέρετε τη συμπεριφορά του.
4. **Μιλήστε σε κάποιον που εμπιστεύεστε.** Μοιραστείτε τα συναισθήματά σας με έναν γονέα, δάσκαλο ή φίλο.
5. **Να είστε ευγενικοί στο διαδίκτυο.** Αντιμετωπίστε τους άλλους με σεβασμό για να βοηθήσετε στη δημιουργία ενός θετικού διαδικτυακού περιβάλλοντος.



Grooming

Συμβαίνει όταν ένας ενήλικας χρησιμοποιεί το διαδίκτυο για να χειραγωγήσει και να εξαπατήσει ένα νεαρό άτομο ώστε να μοιραστεί προσωπικές πληροφορίες, να στείλει προσωπικές φωτογραφίες ή να εμπλακεί σε μη ασφαλείς συμπεριφορές.



Συμβουλές για να αποφύγετε την περιποίηση



1. **Μην μοιράζεστε προσωπικές πληροφορίες.** Ποτέ μη δίνετε τη διεύθυνσή σας, τον αριθμό τηλεφώνου σας, το όνομα του σχολείου σας ή κωδικούς πρόσβασης.
1. **Να είστε προσεκτικοί με τις φωτογραφίες.** Μην στέλνετε τις φωτογραφίες σας σε άτομα που δεν γνωρίζετε.
1. **Εμπιστευτείτε τα συναισθήματά σας.** Αν κάποιος στο διαδίκτυο σας κάνει να αισθάνεστε άβολα, σταματήστε να του μιλάτε.
1. **Μιλήστε σε έναν έμπιστο ενήλικα.** Αν δεν αισθάνεστε σίγουροι για κάποιον στο διαδίκτυο, ενημερώστε έναν γονέα, δάσκαλο ή φροντιστή.
1. **Αποκλεισμός και αναφορά.** Χρησιμοποιήστε τις ρυθμίσεις της πλατφόρμας για να μπλοκάρετε το άτομο και να αναφέρετε τη συμπεριφορά του.



Phishing

Συμβαίνει όταν κάποιος προσποιείται ότι είναι ένα έμπιστο πρόσωπο ή εταιρεία για να κλέψει τις πληροφορίες σας, όπως κωδικούς πρόσβασης, στοιχεία λογαριασμών ή χρήματα. Συχνά χρησιμοποιούν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή ιστότοπους για να σας ξεγελάσουν.



Συμβουλές για να αποφύγετε το phishing



1. **Μην κάνετε κλικ σε άγνωστους συνδέσμους.** Εάν λάβετε ένα μήνυμα ή ηλεκτρονικό ταχυδρομείο από κάποιον που δεν εμπιστεύεστε, αγνοήστε το και μην κάνετε κλικ σε συνδέσμους που περιέχει το μήνυμα.
1. **Ελέγξτε τον αποστολέα.** Κοιτάξτε προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή το όνομα χρήστη του αποστολέα. Τα ψεύτικα μηνύματα έχουν συχνά μικρά ορθογραφικά λάθη.
1. **Διατηρήστε τους κωδικούς πρόσβασής σας ασφαλείς.** Ποτέ μην μοιράζεστε τους κωδικούς σας με κανέναν.
1. **Να είστε προσεκτικοί με τα βραβεία.** Αν κάποιος λέει ότι κερδίσατε κάτι καταπληκτικό, αλλά σας φαίνεται παράξενο ή πολύ εύκολο, μάλλον δεν είναι αληθινό.
1. **Χρησιμοποιήστε ασφαλείς ιστότοπους.** Βεβαιωθείτε ότι το όνομα ενός ιστότοπου αρχίζει με "https://" και εμφανίζει ένα σύμβολο λουκέτου.



2

Σενάρια περιπτώσεων



Τώρα θα διαβάσουμε τρεις on-line καταστάσεις που θα σας βοηθήσουν να κατανοήσετε ορισμένους από τους κινδύνους που μπορεί να αντιμετωπίσετε κατά τη χρήση των μέσων κοινωνικής δικτύωσης και του διαδικτύου.

Αφού διαβάσουμε κάθε ιστορία, θα σκεφτούμε την κατάσταση, θα εντοπίσουμε τους κινδύνους που ενέχει και θα σκεφτούμε τους καλύτερους τρόπους για να αντιδράσουμε με ασφάλεια.

Στόχος αυτής της δραστηριότητας είναι να σας βοηθήσει να αναγνωρίσετε τους διαδικτυακούς κινδύνους και να αναπτύξετε στρατηγικές για να προστατευτείτε.



Η περίπτωση της Lucia

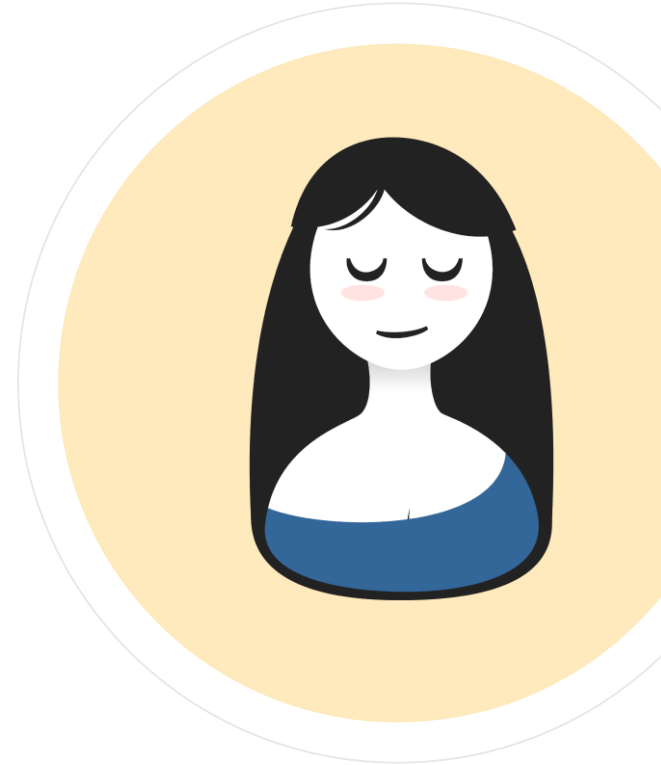
Η Lucia είναι 19 ετών και της αρέσει να ζωγραφίζει. Συχνά μοιράζεται τα έργα της στα μέσα κοινωνικής δικτύωσης.

Μια μέρα, κάποιος της στέλνει ένα μήνυμα λέγοντάς της: "Γεια σας! Λατρεύω τις ζωγραφιές σας. Είσαι τόσο ταλαντούχα! Μπορούμε να γίνουμε φίλοι;" Η Λουτσία αισθάνεται χαρούμενη και απαντά: "Ευχαριστώ! Βέβαια!" Μετά από λίγες μέρες, το άτομο αρχίζει να κάνει προσωπικές ερωτήσεις στη Λουτσία, όπως: "Πού μένεις;" και "Μπορείς να μου στείλεις μια φωτογραφία σου;". Λένε επίσης στη Λουτσία: "Μην πεις σε κανέναν για τη συνομιλία μας - είναι το μυστικό μας".



Η περίπτωση της Lucia - ας συζητήσουμε

- 1. Τι μπορεί να συμβεί αν η Λουκία μοιραστεί προσωπικές πληροφορίες με κάποιον που δεν γνωρίζει στο διαδίκτυο;
- 2. Τι πρέπει να κάνει η Λουκία όταν το άτομο ζητάει τη φωτογραφία της;
- 3. Αν η Λουκία αισθάνεται αβέβαιη για την κατάσταση αυτή, ποιο είναι το καλύτερο βήμα που πρέπει να κάνει;



Η περίπτωση του Luca

Ο Luca μοιράζεται μια αστεία φωτογραφία του στα μέσα κοινωνικής δικτύωσης. Κάποιος σχολιάζει: "Φαίνεσαι τόσο ηλίθιος!" και άλλοι άνθρωποι αρχίζουν να γελούν και να γράφουν άσχημα πράγματα γι' αυτόν. Ο Luca αισθάνεται αναστατωμένος και δεν ξέρει τι να κάνει. Αναρωτιέται αν πρέπει να διαγράψει τον λογαριασμό του ή να απαντήσει θυμωμένα στα σχόλια.



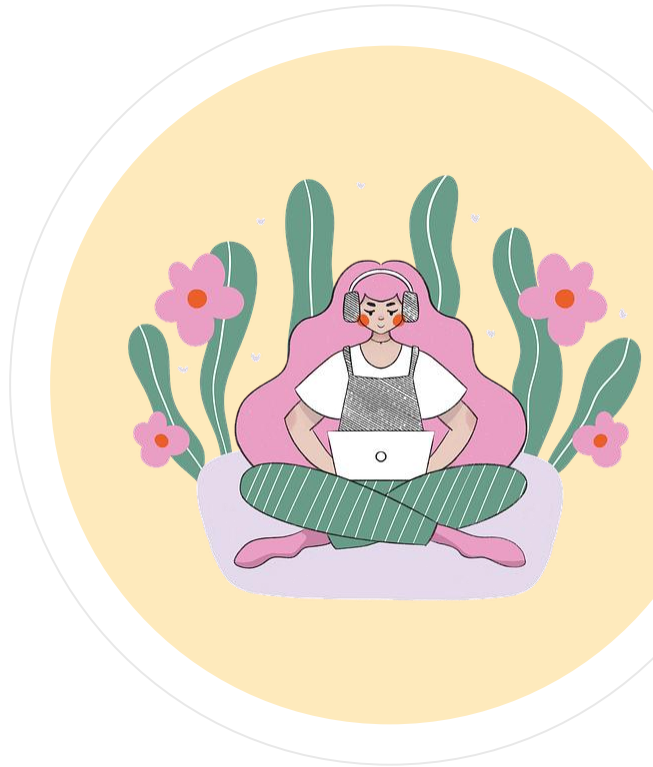
Η περίπτωση του Luca - ας συζητήσουμε

1. Ποιο είναι το πρώτο πράγμα που πρέπει να κάνει ο Luca για τα κακά σχόλια;
2. Σε ποιον πρέπει να μιλήσει ο Luca αν νιώθει πληγωμένος από τα σχόλια;
3. Ποιος θα ήταν ένας καλός τρόπος για τον Luca να χειριστεί τον διαδικτυακό εκφοβισμό στο μέλλον;



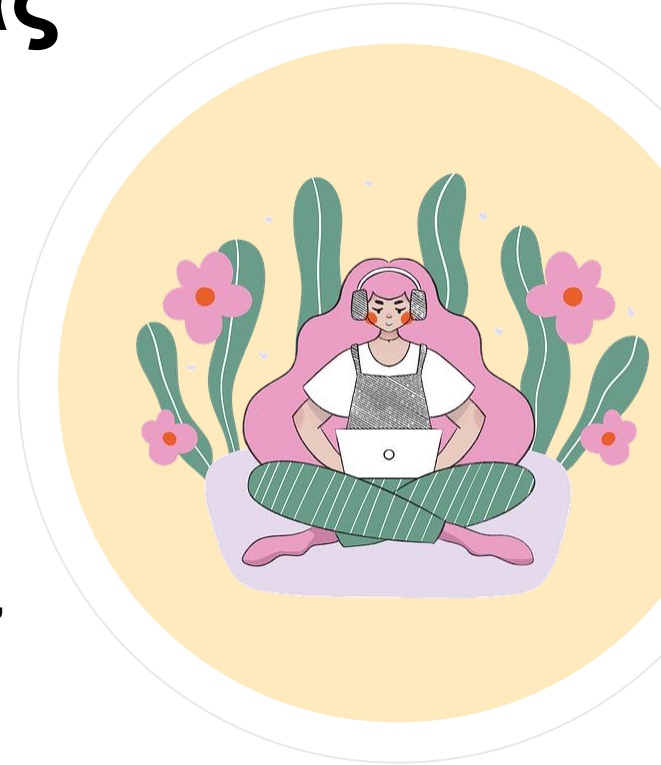
Η περίπτωση της Ana

Η Ana λαμβάνει ένα email που μοιάζει να προέρχεται από το αγαπημένο της ηλεκτρονικό κατάστημα. Το email λέει: "Συγχαρητήρια! Κερδίσατε μια δωροκάρτα αξίας 50 €! Κάντε κλικ εδώ για να παραλάβετε το βραβείο σας". Η Άνα είναι ενθουσιασμένη, αλλά δεν είναι σίγουρη αν είναι αληθινό. Παρατηρεί ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου μοιάζει παράξενη και ο σύνδεσμος δεν ταιριάζει με τον ιστότοπο του καταστήματος.



Η περίπτωση της Άνα - ας συζητήσουμε

1. Τι πρέπει να κάνει η Άνα πριν κάνει κλικ στο σύνδεσμο;
2. Ποιο είναι ένα προειδοποιητικό σημάδι ότι αυτό το email μπορεί να είναι ψεύτικο;
3. Αν η Άννα πιστεύει ότι αυτό το email είναι ύποπτο, τι πρέπει να κάνει;



Δραστηριότητα: εντοπισμός κινδύνων

Σε αυτή τη δραστηριότητα, θα δείτε εικόνες ή θα ακούσετε σύντομες ιστορίες για πράγματα που μπορεί να συμβούν στο διαδίκτυο. Η δουλειά σας είναι να:

- ✓ Αποφασίστε αν η κατάσταση είναι επικίνδυνη ή ασφαλής.
- ✓ Πείτε γιατί πιστεύετε ότι είναι επικίνδυνο.
- Εξηγήστε τι θα κάνατε για να παραμείνετε ασφαλείς.

Παράδειγμα

Ένας άγνωστος σας στέλνει ένα μήνυμα που λέει: "Είσαι τόσο γαμάτος! Μπορούμε να συναντηθούμε;"

Ρωτήστε τον εαυτό σας:

- Είναι επικίνδυνο αυτό;
- Γιατί μπορεί να είναι επικίνδυνο;
- Τι πρέπει να κάνετε σε αυτή την περίπτωση;



Εντοπισμός κινδύνων Σενάρια

Σενάριο 1:

Μπορώ να σε βοηθήσω να αποκτήσεις πολλούς οπαδούς αν μου στείλεις τον κωδικό πρόσβασής σου".

Σενάριο 2:

Ένας φίλος δημοσιεύει μια αστεία φωτογραφία σας χωρίς να σας ρωτήσει πρώτα.

Σενάριο 3:

Κάποιος σχολιάζει στην ανάρτησή σας: "Είσαι τόσο άσχημη, που όλοι σε μισούν".

Σενάριο 4:

Συγχαρητήρια! Κερδίσατε 1.000 €! Κάντε κλικ εδώ για να διεκδικήσετε το βραβείο σας".

Σενάριο 5:

Βρίσκεστε σε μια διαδικτυακή ομαδική συνομιλία για το αγαπημένο σας βιντεοπαιχνίδι. Κάποιος στη συνομιλία ρωτάει: "Ποια είναι τα γενέθλιά σου; Θέλουμε να τα γιορτάσουμε μαζί σας!"

Σενάριο 6:

Λαμβάνετε ένα μήνυμα από κάποιον που λέει: "Ψάχνουμε άτομα για εργασία από το σπίτι. Απλά στείλτε το όνομά σας, τη διεύθυνσή σας και τα τραπεζικά σας στοιχεία για να ξεκινήσετε!"

Σενάριο 7:

Βγάζετε μια ομαδική φωτογραφία με τους φίλους σας σε ένα πάρκο και θέλετε να τη δημοσιεύσετε στα μέσα κοινωνικής δικτύωσης. Ένας από τους φίλους σας λέει ότι δεν θέλει τη φωτογραφία του στο διαδίκτυο.

Σενάριο 8:

Ένας άγνωστος σας στέλνει ένα μήνυμα που λέει: "Είσαι τόσο ωραία και όμορφη! Θα ήθελα πολύ να μιλήσουμε περισσότερο. Μπορείς να μου πεις περισσότερα για σένα;"



Σκέψεις και συμπεράσματα

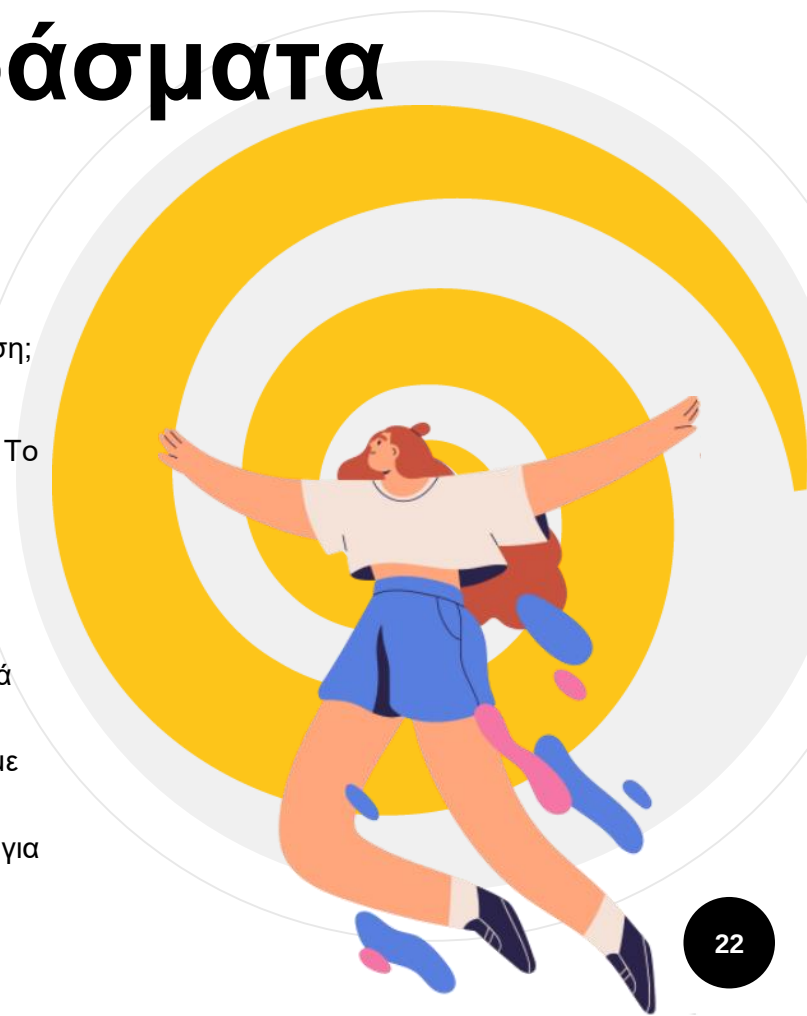
Αφού ολοκληρώσετε τα σενάρια, αφιερώστε λίγο χρόνο για να σκεφτείτε τι μάθατε.

Ρωτήστε τον εαυτό σας:

- ✓ Ποιος κίνδυνος σας εξέπληξε περισσότερο;
- ✓ Πώς αισθανθήκατε όταν αποφασίσατε τι να κάνετε σε κάθε περίπτωση;
- ✓ Τι θα κάνετε διαφορετικά την επόμενη φορά που θα είστε online;
- ✓ Συζητήστε με την ομάδα ή τον καθηγητή σας για τις απαντήσεις σας. Το να μοιραστείτε τις σκέψεις σας μπορεί να σας βοηθήσει να νιώσετε μεγαλύτερη αυτοπεποίθηση σχετικά με την ασφάλεια στο διαδίκτυο.

Θυμηθείτε το

- Αν κάτι σας φαίνεται λάθος στο διαδίκτυο, εμπιστευτείτε τα αισθήματά σας.
- Μην μοιράζετε προσωπικές πληροφορίες ή κωδικούς πρόσβασης με άτομα που δεν γνωρίζετε.
- Πάντα να μιλάτε σε κάποιον που εμπιστεύεστε αν δεν είστε σίγουροι για μια κατάσταση.



Παιχνίδι ρόλων

Σε αυτή τη δραστηριότητα θα εξασκηθείτε στον τρόπο αντίδρασης σε διάφορους διαδικτυακούς κινδύνους, παίζοντας καταστάσεις σε μικρές ομάδες. Θα σας βοηθήσει να νιώσετε μεγαλύτερη αυτοπεποίθηση για το τι πρέπει να κάνετε αν αντιμετωπίσετε αυτούς τους κινδύνους στην πραγματική ζωή.

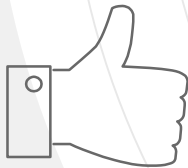
Οδηγίες

Θα εργαστείτε σε μικρές ομάδες για να υποδυθείτε διάφορες καταστάσεις. Κάθε ομάδα θα λάβει ένα σενάριο σχετικά με έναν διαδικτυακό κίνδυνο. Ένα άτομο θα υποδυθεί το άτομο που αντιμετωπίζει το πρόβλημα και οι υπόλοιποι θα υποδυθούν διαφορετικούς ρόλους, όπως ένας φίλος, το άτομο που διατρέχει κίνδυνο ή ένας ενήλικας που εμπιστεύεστε. Αφού παίξουμε το σενάριο, θα συζητήσουμε για το τι συνέβη και πώς να το χειριστούμε.





Σενάριο 1



- **Κατάσταση:** Κάποιος στο διαδίκτυο λέει, "Είσαι τόσο ταλαντούχος! Μπορώ να δω περισσότερες φωτογραφίες σου; Υπόσχομαι ότι δεν θα τις μοιραστώ με κανέναν".
- **Ρόλοι:**
 - Πρόσωπο από το οποίο ζητούνται φωτογραφίες.
 - Ο ξένος.
 - Ένας έμπιστος ενήλικας ή φίλος στον οποίο το άτομο απευθύνεται για συμβουλές.
- **Βήματα δράσης:**
 - Αρνούνται να στείλουν φωτογραφίες.
 - Αποκλείστε τον ξένο.
 - Μιλήστε σε έναν έμπιστο ενήλικα για το τι συνέβη.



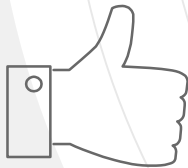
Σενάριο 2



- **Κατάσταση:** Κάποιος σχολιάζει την ανάρτησή σας: "Αυτό είναι τόσο χαζό. Γιατί κάνεις τον κόπο;" Άλλοι άνθρωποι αρχίζουν να κάνουν like στο σχόλιο και να γράφουν κι αυτοί κακά πράγματα.
- **Ρόλοι:**
 - Το άτομο που εκφοβίζεται.
 - Ο νταής.
 - Ένας έμπιστος ενήλικας ή φίλος με τον οποίο το άτομο μιλάει.
- **Βήματα δράσης:**
 - Μην απαντάτε στα κακά σχόλια.
 - Πάρτε στιγμιότυπα οθόνης ως αποδεικτικά στοιχεία.
 - Αποκλείστε και αναφέρετε τον νταή.



Σενάριο 3



- **Κατάσταση:** Συγχαρητήρια! Κερδίσατε ένα νέο τηλέφωνο! Κάντε κλικ σε αυτόν τον σύνδεσμο για να διεκδικήσετε το βραβείο σας".
- **Ρόλοι:**
 - Το άτομο που λαμβάνει το email.
 - Ο απατεώνας που έστειλε αυτό το e-mail.
 - Ένας φίλος ή έμπιστος ενήλικας που δίνει συμβουλές.
- **Βήματα δράσης:**
 - Μην κάνετε κλικ στον σύνδεσμο.
 - Διαγράψτε το email και αναφέρετέ το ως spam.
 - Μιλήστε σε έναν έμπιστο ενήλικα αν δεν είστε σίγουροι.



Συζήτηση και Συμπέρασμα

Συζήτηση

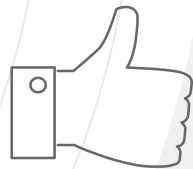
Αφού Παίξουμε το σενάριο, ας συζητήσουμε:

- ✓ Τι έκανε την κατάσταση επικίνδυνη;
- ✓ Τι έκανε το άτομο για να Παραμείνει ασφαλές;
- ✓ Πώς αισθάνεστε όταν εξασκείστε σε αυτή την κατάσταση;
- ✓ Τι θα κάνατε αν σας συνέβαινε αυτό στην Πραγματική ζωή;

Συμπέρασμα

Έχετε κάνει εξαιρετική δουλειά στην εξάσκηση του τρόπου χειρισμού των διαδικτυακών κινδύνων! **Να θυμάστε:**

- ✓ Πάντα να εμπιστεύεστε το ένστικτό σας - αν κάτι σας φαίνεται λάθος, μάλλον είναι.
- ✓ Αποκλείστε και αναφέρετε άτομα που σας κάνουν να νιώθετε άβολα.
- ✓ Μιλήστε σε έναν ενήλικα που εμπιστεύεστε αν δεν είστε σίγουροι για το τι πρέπει να κάνετε.



Ταξινόμηση κινδύνου Παιχνίδι



Θα εξασκηθούμε στον εντοπισμό ασφαλών και επικίνδυνων διαδικτυακών συμπεριφορών, ταξινομώντας παραδείγματα σε κατηγορίες "Ασφαλών" ή "Επικίνδυνων".

Σε αυτή τη δραστηριότητα, θα δείτε παραδείγματα πραγμάτων που μπορεί να κάνουν οι άνθρωποι στο διαδίκτυο. Ο στόχος σας είναι να αποφασίσετε αν κάθε παράδειγμα είναι "ασφαλές" ή "επικίνδυνο".

Θα εργαστούμε σε ζευγάρια ή μικρές ομάδες. Κάθε ομάδα θα λάβει κάρτες με παραδείγματα διαδικτυακών ενεργειών. Η δουλειά σας είναι να τοποθετήσετε κάθε κάρτα στην κατηγορία "Ασφαλής" ή "Επικίνδυνη" στον πίνακα ή στο τραπέζι.

Αφού ταξινομήσουμε τις κάρτες, θα συζητήσουμε τις επιλογές μας ως ομάδα.

Ταξινόμηση κινδύνου Παιχνίδι

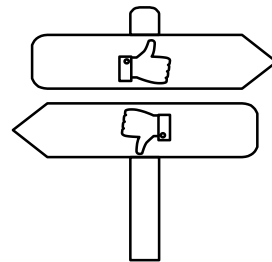


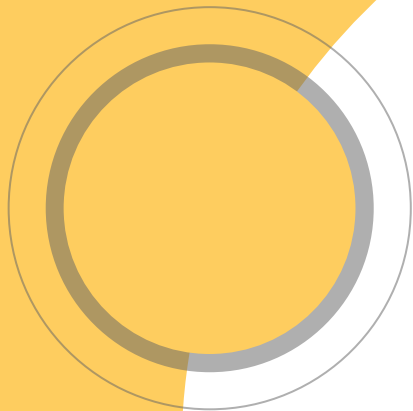
Παράδειγμα κάρτας:

"Κοινοποίηση του πλήρους ονόματος και της διεύθυνσής σας στο προφίλ σας".
Είναι ασφαλές ή επικίνδυνο;

Απαντήστε: Κινδύνου: Επικίνδυνο. Η κοινοποίηση προσωπικών πληροφοριών
μπορεί να σας κάνει ευάλωτους.

Τώρα είναι η σειρά σας!





Ευχαριστώ!



Co-funded by
the European Union

Χρηματοδοτείται από την Ευρωπαϊκή Ένωση. Ωστόσο, οι απόψεις και οι γνώμες που εκφράζονται είναι αποκλειστικά του/των συγγραφέα/ων και δεν αντανακλούν κατ' ανάγκη τις απόψεις και τις γνώμες της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Ούτε η Ευρωπαϊκή Ένωση ούτε ο EACEA μπορούν να θεωρηθούν υπεύθυνοι γι' αυτές.