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 5.1

Εισαγωγή στις Βασικές Αρχές Κυβερνοασφάλειας

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 5.1

Εισαγωγή στις Βασικές Αρχές Κυβερνοασφάλειας

Στόχοι:

- Να αναπτύξετε μια σαφή κατανόηση των βασικών εννοιών της κυβερνοασφάλειας, συμπεριλαμβανομένων βασικών όρων όπως απειλές, τρωτά σημεία και κίνδυνοι.
- Να εντοπίσετε διαδεδομένες διαδικτυακές απειλές, όπως το ηλεκτρονικό ψάρεμα (phishing), το κακόβουλο λογισμικό, το ransomware και οι επιθέσεις κοινωνικής μηχανικής, και να κατανοήσετε τον αντίκτυπό τους.
- Να καλλιεργήσετε μια προληπτική νοοτροπία για τον εντοπισμό και την αντιμετώπιση πιθανών περιστατικών κυβερνοασφάλειας.

Βασικά Μηνύματα:

- Είτε είστε ιδιώτης, μικρή επιχείρηση είτε παγκόσμια επιχείρηση, η κατανόηση των βασικών πρακτικών κυβερνοασφάλειας είναι απαραίτητη για την προστασία του ψηφιακού σας αποτυπώματος.
- Η εφαρμογή απλών προληπτικών βημάτων μπορεί να εξοικονομήσει σημαντικό χρόνο, χρήματα και άγχος σε σύγκριση με την ανάκαμψη από μια κυβερνοεπίθεση.

ΕΙΔΟΣ ΜΑΘΗΜΑΤΟΣ:

Επισκόπηση μαθήματος

Στον σημερινό ψηφιακό κόσμο, η κατανόηση των βασικών αρχών της κυβερνοασφάλειας δεν είναι πλέον προαιρετική - είναι αναγκαιότητα. Αυτό το μάθημα σας εισάγει στις βασικές αρχές της κυβερνοασφάλειας, στις κοινές απειλές και στους πρακτικούς τρόπους ενίσχυσης της διαδικτυακής ασφάλειας. Μαζί, θα εξερευνήσουμε πώς να προστατεύσουμε τα προσωπικά και επαγγελματικά ψηφιακά περιουσιακά στοιχεία, καλλιεργώντας μια κουλτούρα κυβερνοεπίγνωσης και ανθεκτικότητας.

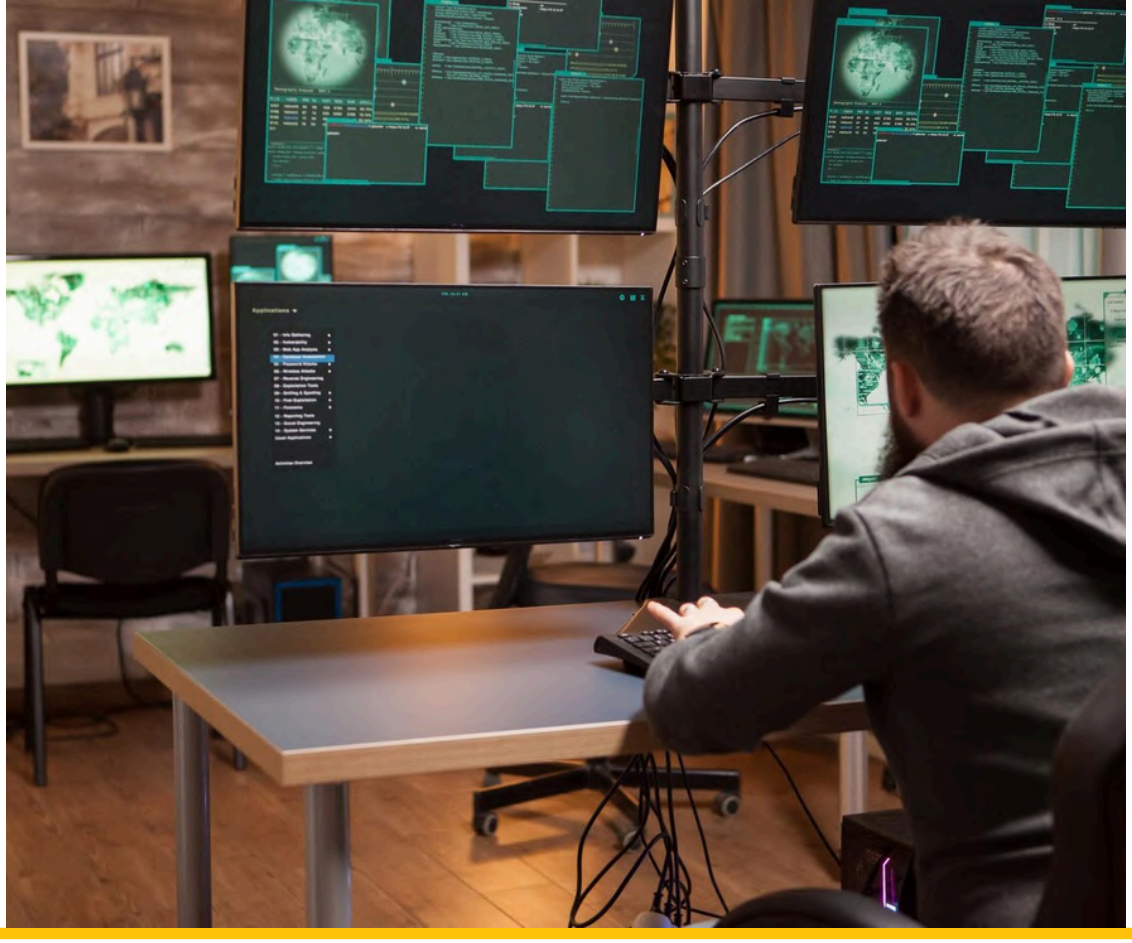
Το εργαστήριο οργανώνεται σε 4 βήματα:

1: Εισαγωγή στα βασικά της κυβερνοασφάλειας (15 λεπτά)

2: Εντοπισμός κοινών κυβερνοαπειλών (10 λεπτά)

3: Στρατηγικές για βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας (10 λεπτά)

4: Τελικός αναστοχασμός και βασικά συμπεράσματα (5 λεπτά)



Βήμα 1 Εισαγωγή στα βασικά στοιχεία της κυβερνοασφάλειας

Ας ξεκινήσουμε με ένα σύντομο βίντεο που παρουσιάζει την έννοια της κυβερνοασφάλειας. Στην καθημερινότητά μας, χρησιμοποιούμε συνεχώς ψηφιακά εργαλεία, αλλά πόσο συχνά σταματάμε να σκεφτόμαστε την ασφάλειά τους; Η κυβερνοασφάλεια είναι απαραίτητη για να διατηρούμε τον εαυτό μας και τα προσωπικά μας δεδομένα ασφαλή στον ψηφιακό κόσμο. Σήμερα, θα εμβαθύνουμε στις βασικές αρχές της κυβερνοασφάλειας και θα διερευνήσουμε γιατί είναι τόσο σημαντική.

Ας δούμε μαζί αυτό το βίντεο:
https://youtu.be/inWWhr5tnEA?si=Pxp1YyvjrFdLoo38

Τώρα που είδατε το βίντεο, ας συζητήσουμε:

1. Τι σας έκανε εντύπωση σχετικά με την κυβερνοασφάλεια από το βίντεο;
2. Γιατί πιστεύετε ότι η κυβερνοασφάλεια είναι σημαντική στην καθημερινότητά μας;

Βήμα 1

Εισαγωγή στα βασικά στοιχεία της κυβερνοασφάλειας

Η κυβερνοασφάλεια δεν αφορά μόνο την προστασία των συστημάτων. Πρόκειται επίσης για την κατανόηση της δικής μας συμπεριφοράς στο διαδίκτυο. Ο τρόπος με τον οποίο αλληλεπιδρούμε με τα ψηφιακά εργαλεία μπορεί είτε να ενισχύσει την ασφάλειά μας είτε να μας κάνει ευάλωτους σε απειλές.

Τώρα είναι η ώρα να αφιερώσετε λίγο χρόνο για να αναλογιστείτε την ψηφιακή σας ζωή.

Καταγράψτε τις απαντήσεις στις ακόλουθες ερωτήσεις:
Πόσο συχνά σκέφτεστε την ασφάλεια των διαδικτυακών σας δραστηριοτήτων;
Μπορείτε να εντοπίσετε τυχόν συνήθειες που θα μπορούσαν να θέσουν σε κίνδυνο τα προσωπικά σας δεδομένα;

Να είστε έτοιμοι να μοιραστείτε τις σκέψεις σας!

Βήμα 2

Εντοπισμός κοινών κυβερνοαπειλών

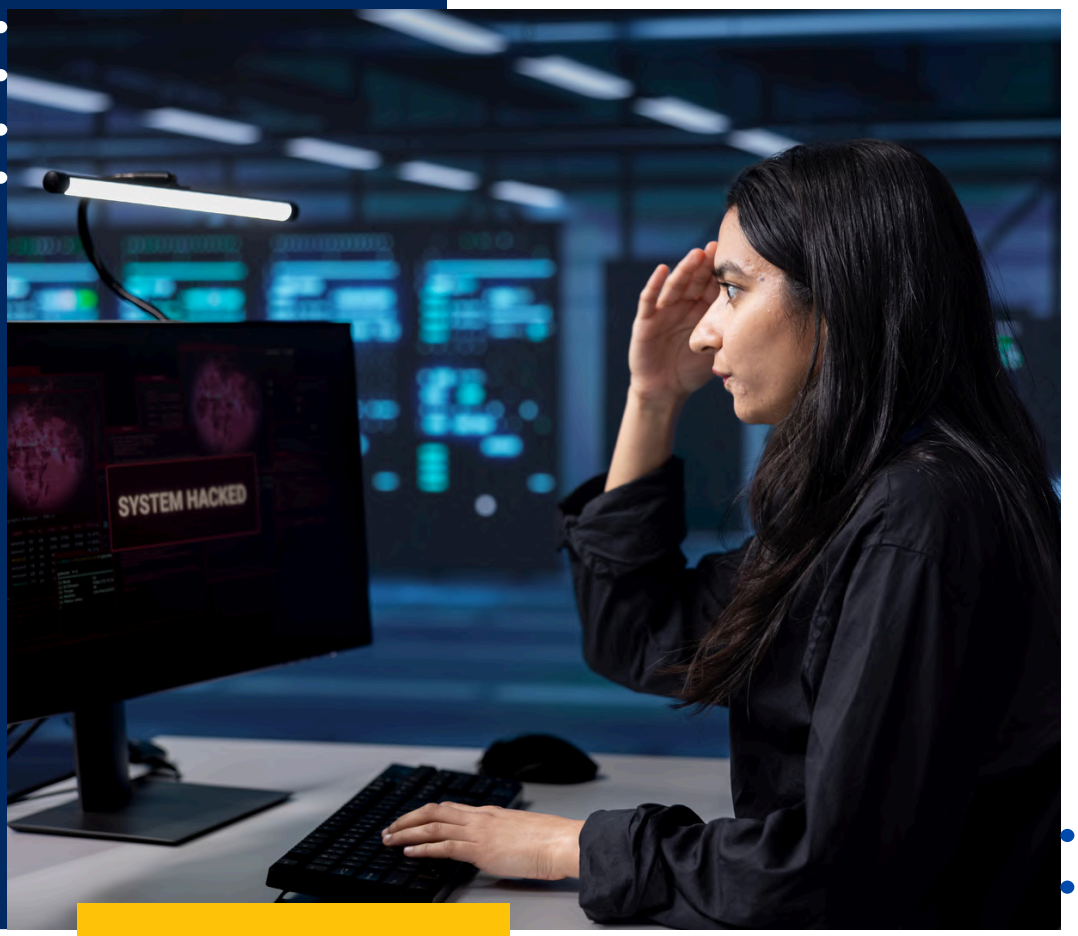
Ας ρίξουμε μια πιο προσεκτική ματιά στους τύπους κυβερνοαπειλών που ενδέχεται να αντιμετωπίσουμε.

Το διαδίκτυο είναι ένας απέραντος χώρος γεμάτος ευκαιρίες, αλλά συνοδεύεται και από κινδύνους. Οι κυβερνοαπειλές μπορούν να στοχεύσουν οποιονδήποτε, οπουδήποτε, γεγονός που καθιστά κρίσιμη την κατανόηση της φύσης και του αντίκτυπού τους. Σε αυτό το βήμα, θα εξερευνήσουμε διάφορους τύπους απειλών και πώς μπορούν να μας επηρεάσουν.

Διαβάστε το άρθρο: IBM: Είδη κυβερνοαπειλών

Το άρθρο τονίζει:

- Τους διαφορετικούς τύπους κυβερνοαπειλών, συμπεριλαμβανομένου του ηλεκτρονικού "ψαρέματος" (phishing), του ransomware και του κακόβουλου λογισμικού.
- Πώς λειτουργούν αυτές οι απειλές και ποιους στοχεύουν.
- Παραδείγματα της ζημιάς που μπορούν να προκαλέσουν.



Βήμα 2

Εντοπισμός κοινών κυβερνοαπειλών

Αφού διαβάσετε το άρθρο, σκεφτείτε τα εξής:

1. Ποιο είδος κυβερνοαπειλής θεωρήσατε πιο ανησυχητικό και γιατί;
2. Έχετε εσείς ή κάποιος που γνωρίζετε βιώσει κάποια από αυτές τις απειλές;
3. Πώς πιστεύετε ότι η κατανόηση αυτών των απειλών μπορεί να βοηθήσει στην πρόληψή τους;

Στη συνέχεια, καταγράψτε ένα πραγματικό παράδειγμα ή σενάριο (μπορεί να είναι υποθετικό) όπου θα μπορούσε να συμβεί μία από αυτές τις κυβερνοαπειλές που αναφέρονται στο άρθρο.
Να είστε έτοιμοι να μοιραστείτε το παράδειγμά σας και να το συζητήσετε με την ομάδα!

Βήμα 3

Στρατηγικές για βέλτιστες πρακτικές κυβερνοασφάλειας

Τώρα, ας επικεντρωθούμε στην προστασία του εαυτού μας στο διαδίκτυο.

Ενώ οι κυβερνοαπειλές εξελίσσονται συνεχώς, υπάρχουν απλά και αποτελεσματικά βήματα που μπορούμε να κάνουμε για να προστατεύσουμε τις πληροφορίες μας και να διατηρήσουμε την ασφάλειά τους. Υιοθετώντας βέλτιστες πρακτικές κυβερνοασφάλειας, μπορούμε να ελαχιστοποιήσουμε τους κινδύνους και να παραμείνουμε ασφαλέστεροι στην ψηφιακή μας ζωή.

Η κυβερνοασφάλεια δεν απαιτεί προηγμένες τεχνικές δεξιότητες - μικρές, σκόπιμες ενέργειες μπορούν να κάνουν μεγάλη διαφορά στην προστασία του εαυτού σας και των δεδομένων σας.

Βήμα 3

Στρατηγικές για βέλτιστες πρακτικές κυβερνοασφάλειας

Ακολουθούν μερικές βασικές πρακτικές που πρέπει να λάβετε υπόψη:

- Δημιουργήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης και αλλάξτε τους τακτικά.
- Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) για πρόσθετη ασφάλεια.
- Να είστε προσεκτικοί με συνδέσμους και συνημμένα, ειδικά από άγνωστες πηγές.
- Διατηρείστε το λογισμικό και τις συσκευές ενημερωμένες για την επιδιόρθωση ευπαθειών.
- Χρησιμοποιήστε ασφαλείς συνδέσεις Wi-Fi, αποφεύγοντας τα δημόσια δίκτυα όποτε είναι δυνατόν.

Δραστηριότητα: Λίστα ελέγχου βέλτιστων πρακτικών κυβερνοασφάλειας - Λίστα ελέγχου βέλτιστων πρακτικών κυβερνοασφάλειας

Βήμα 1: Αξιολογήστε τις τρέχουσες συνήθειές σας

- Σκεφτείτε τις τρέχουσες διαδικτυακές σας συμπεριφορές και συνήθειες. Υπάρχουν τομείς στους οποίους ενδέχεται να θέτετε τον εαυτό σας σε κίνδυνο;

Παράδειγμα: «Χρησιμοποιώ τον ίδιο κωδικό πρόσβασης σε πολλούς λογαριασμούς»

Βήμα 2: Δημιουργήστε ένα σχέδιο

- Καταγράψτε ένα εφαρμόσιμο βήμα για κάθε βασική έννοια που αναφέρεται παραπάνω. Για παράδειγμα:

Ισχυροί κωδικοί πρόσβασης: «Θα εγκαταστήσω έναν διαχειριστή κωδικών πρόσβασης για τη δημιουργία και την αποθήκευση ασφαλών κωδικών πρόσβασης» κ.λπ.

Βήμα 3

Στρατηγικές για βέλτιστες πρακτικές κυβερνοασφάλειας

Βήμα 3: Κοινή χρήση ομάδας

- Μοιραστείτε μία από τις προγραμματισμένες ενέργειές σας με έναν συνεργάτη ή την ομάδα.
- Συζητήστε πώς αυτά τα βήματα θα μπορούσαν να σας βοηθήσουν να βελτιώσετε την ψηφιακή σας ασφάλεια.
- Προσφέρετε συμβουλές ή προτάσεις για πρόσθετα μέτρα που μπορούν να λάβουν άλλοι.

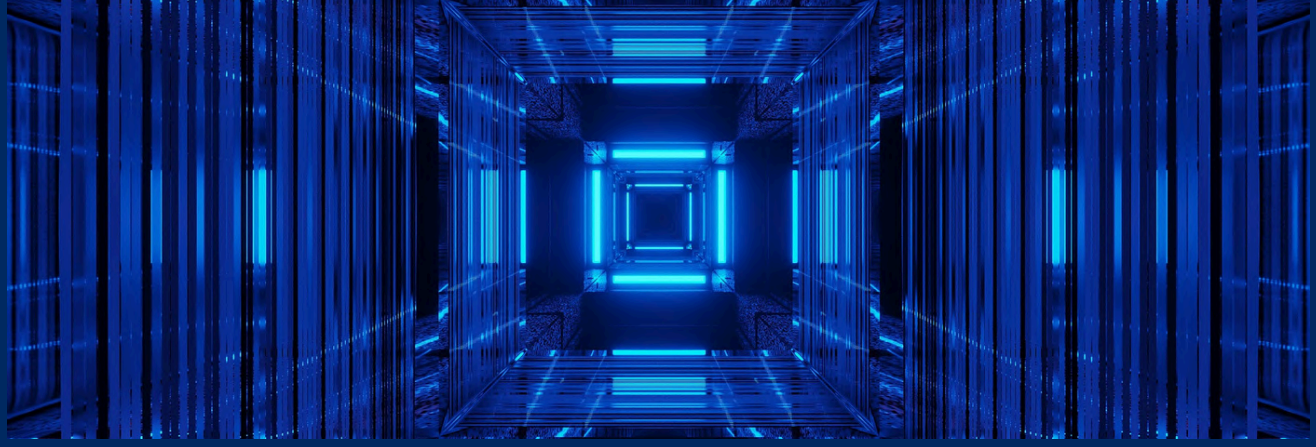
Στο τέλος, απαντήστε στοχαστικά στο μυαλό σας την **βασική ερώτηση αναστοχασμού:**
Ποια είναι μια συνήθεια ή στρατηγική που μπορείτε να αρχίσετε να εφαρμόζετε σήμερα για να βελτιώσετε άμεσα την ασφάλειά σας στο διαδίκτυο;

Βήμα 4 Τελικός αναστοχασμός και βασικά συμπεράσματα

Καθώς ολοκληρώνουμε, ας αφιερώσουμε λίγο χρόνο για να αναλογιστούμε όλα όσα καλύψαμε σε αυτό το μάθημα και πώς μπορούμε να χρησιμοποιήσουμε αυτή τη γνώση στο μέλλον.

Σκεφτείτε τις διαδικτυακές σας συνήθειες - υπάρχουν αλλαγές που σας εμπνέουν να κάνετε μετά τη σημερινή συζήτηση; Αν ναι, ποιο είναι ένα βήμα που θα κάνετε πρώτα για να βελτιώσετε την κυβερνοασφάλειά σας; Τώρα σκεφτείτε πώς μπορούμε να βοηθήσουμε τους άλλους. Ποια είναι μια απλή συμβουλή ή συνήθεια από αυτό το εργαστήριο που θα μπορούσατε να μοιραστείτε με έναν φίλο ή συνάδελφο για να τους βοηθήσετε να παραμείνουν ασφαλείς στο διαδίκτυο;

Σας ευχαριστούμε όλους για την ενεργό συμμετοχή και τις χρήσιμες συνεισφορές σας σήμερα!



Σύνοψη των βασικών συμπερασμάτων

- **Η κυβερνοασφάλεια είναι για όλους. Η κατανόηση των απειλών και η υιοθέτηση βέλτιστων πρακτικών μας βοηθά να παραμένουμε ασφαλείς στο διαδίκτυο.**
- **Τα μικρά βήματα κάνουν μεγάλη διαφορά. Εργαλεία όπως οι διαχειριστές κωδικών πρόσβασης και οι τακτικές ενημερώσεις μπορούν να βελτιώσουν σημαντικά την ασφάλειά σας.**
- **Μείνετε ενημερωμένοι. Οι κυβερνοαπειλές εξελίσσονται συνεχώς, επομένως η ενημέρωση για τις πιο πρόσφατες συμβουλές και εργαλεία είναι απαραίτητη για τη μακροπρόθεσμη ασφάλεια.**
- **Να είστε προνοητικοί. Όσο περισσότερο υιοθετείτε ασφαλείς συνήθειες, τόσο πιο ασφαλείς θα είστε εσείς - και οι γύρω σας.**

Οδηγίες για εργαζόμενους στον τομέα της νεολαίας, εκπαιδευτικούς και δασκάλους

Σκοπός:
Αυτό το μάθημα στοχεύει να βοηθήσει τους εργαζόμενους για νέους, τους εκπαιδευτικούς και τους δασκάλους να εξοπλίσουν τους νέους με βασικές γνώσεις κυβερνοασφάλειας. Μέσω ενδιαφέρουσας συζήτησης, δραστηριοτήτων και προβληματισμού, οι συμμετέχοντες θα κατανοήσουν κοινές κυβερνοαπειλές, θα μάθουν βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο και θα δημιουργήσουν εφαρμόσιμα σχέδια για να προστατευτούν στον ψηφιακό κόσμο.

Απαιτούμενα υλικά:

- Σύνδεση στο Διαδίκτυο για αναπαραγωγή βίντεο ή άρθρων
- Προβολέας και οθόνη
- Ομιλητές
- Πρόσβαση σε προτεινόμενα εργαλεία κυβερνοασφάλειας
- Χαρτί γραφικών παραστάσεων ή μαρκαδόροι λευκού πίνακα
- Στυλό ή μολύβια
- Φύλλα χαρτιού

Βήμα 1: Εισαγωγή στα βασικά της κυβερνοασφάλειας (15 λεπτά)

1. Ξεκινήστε εμπλέγοντας τους συμμετέχοντες με ένα σχετικό παράδειγμα: «Σκεφτείτε την τελευταία φορά που χρησιμοποιήσατε μια νέα εφαρμογή ή επισκεφτήκατε έναν ιστότοπο. Σταματήσατε να σκεφτείτε πόσο ασφαλή είναι τα δεδομένα σας;»

2. Επισημάνετε τη σημασία της κυβερνοασφάλειας: Εξηγήστε ότι η κυβερνοασφάλεια δεν αφορά μόνο τους επαγγελματίες πληροφορικής. Είναι μια κρίσιμη δεξιότητα για όλους στη σημερινή ψηφιακή εποχή. Τονίστε πώς η κυβερνοασφάλεια βοηθά στην προστασία των προσωπικών, επαγγελματικών και οργανωτικών πληροφοριών.

3. Περιγράψτε με σαφήνεια τους στόχους της συνεδρίας.

4. Δραστηριότητα: Προβολή βίντεο και συζήτηση:
- Δείτε το βίντεο: «Τι είναι η κυβερνοασφάλεια;» (δείτε εδώ).
- Δώστε στους συμμετέχοντες καθοδηγητικές ερωτήσεις μετά την παρακολούθηση.

5. Μετά το βίντεο, ξεκινήστε μια συζήτηση:
- «Τι σας εξέπληξε περισσότερο στην κυβερνοασφάλεια;»
- «Πιστεύετε ότι η κυβερνοασφάλεια είναι σημαντική για όλους; Γιατί ή γιατί όχι;»
- «Ποιοι είναι οι κίνδυνοι αν δεν δίνουμε προσοχή στην ασφάλεια στο διαδίκτυο;»

Βήμα 1: Εισαγωγή στα βασικά της κυβερνοασφάλειας (15 λεπτά)

6. Προσωπικός αναστοχασμός: Ζητήστε από τους συμμετέχοντες να αφιερώσουν λίγα λεπτά για να καταγράψουν τις σκέψεις τους:

- «Πόσο συχνά σκέφτεστε την ασφάλεια των διαδικτυακών σας δραστηριοτήτων;»
- «Μπορείτε να εντοπίσετε μία ή δύο συνήθειες που θα μπορούσαν να θέσουν σε κίνδυνο τα προσωπικά σας στοιχεία;»
- «Ποιες αλλαγές πιστεύετε ότι θα μπορούσατε να κάνετε για να βελτιώσετε την ασφάλειά σας στο διαδίκτυο;»

7. Ενθαρρύνετε την ανταλλαγή σε ζευγάρια ή μικρές ομάδες:

- Επιλογή 1: Μοιραστείτε μια συνήθεια που θεωρείτε επικίνδυνη και ζητήστε συμβουλές από την ομάδα σας για το πώς να τη βελτιώσετε.
- Επιλογή 2: Συζητήστε αν έχετε βιώσει ή ακούσει ποτέ για κάποια κυβερνοαπειλή και πώς αντιμετωπίστηκε.

8. Εάν οι συμμετέχοντες προτιμούν να μην μοιράζονται τις απόψεις τους σε ομάδες, επιτρέψτε τους να γράψουν μια αλλαγή που δεσμεύονται να κάνουν και να την υποβάλουν ανώνυμα στον συντονιστή για συζήτηση αργότερα.

Βήμα 2: Εντοπισμός κοινών κυβερνοαπειλών (10 λεπτά)

1. Κοινοποιήστε το άρθρο IBM: Είδη κυβερνοαπειλών ή μια έντυπη περίληψη των βασικών σημείων του.
2. Δώστε στους συμμετέχοντες 5 λεπτά για να διαβάσουν και να σημειώσουν τις απειλές που τους ανησυχούν περισσότερο, εστιάζοντας στη λειτουργία τους και στις πιθανές επιπτώσεις.
3. Συζήτηση:

Διευκολύνετε μια ομαδική συζήτηση:

- «Ποια κυβερνοαπειλή θεωρείτε πιο ανησυχητική και γιατί;»
- «Έχετε εσείς ή κάποιος που γνωρίζετε βιώσει κάποια από αυτές τις απειλές; Τι συνέβη;»

4. Προσθέστε πληροφορίες, εάν χρειάζεται:

Επισημάνετε στατιστικά στοιχεία ή παραδείγματα για να εμπλουτίσετε τη συζήτηση, όπως email ηλεκτρονικού "ψαρέματος" (phishing) ή επιθέσεις ransomware.

5. Δραστηριότητα σεναρίου:

Ζητήστε από τους συμμετέχοντες να γράψουν ένα σύντομο παράδειγμα, πραγματικό ή υποθετικό, που να αφορά μια κυβερνοαπειλή, όπως:

- Ηλεκτρονικό "ψάρεμα" (phishing): «Ένα δόλιο email ξεγέλασε κάποιον ώστε να κοινοποιήσει τα στοιχεία σύνδεσης του λογαριασμού του»
- Κακόβουλο λογισμικό: «Κάνοντας κλικ σε έναν ύποπτο σύνδεσμο, κατεβάστηκε ένας ιός, κλειδώνοντας τα αρχεία τους»

6. Μοιραστείτε σενάρια στην ομάδα και διευκολύνετε μια συζήτηση γύρω από:

- «Τι πήγε στραβά στο σενάριο;»
- «Πώς θα μπορούσε να είχε αποφευχθεί η κατάσταση;»
- «Ποια προληπτικά μέτρα θα βοηθούσαν;»

7. Προαιρετικά, μπορείτε να συμβάλετε στη συζήτηση επισημαίνοντας στρατηγικές πρόληψης από τον πραγματικό κόσμο για κάθε τύπο απειλής.

Βήμα 3: Στρατηγικές για βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας (10 λεπτά)

1. Επισκόπηση βέλτιστων πρακτικών:
    - Παρουσιάστε απλές, αποτελεσματικές στρατηγικές:
    - Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης.
    - Ενεργοποίείστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA).
    - Αποφύγετε ύποπτους συνδέσμους και συνημμένα.
    - Διατηρείστε το λογισμικό και τις συσκευές ενημερωμένες.
    - Χρησιμοποιήστε ασφαλές Wi-Fi ή VPN.
- Χρησιμοποιήστε παραδείγματα από την πραγματική ζωή ή σύντομες επιδείξεις για να δείξετε τον αντίκτυπο κάθε στρατηγικής.

2. Εάν είναι δυνατόν, δείξτε ή εξηγήστε τη ρύθμιση ενός εργαλείου (που περιλαμβάνεται στην ενότητα «Εργαλεία») για να το κάνετε πιο σχετικό.
3. Δραστηριότητα: λίστα ελέγχου κυβερνοασφάλειας:
- Μοιράστε ένα απλό πρότυπο λίστας ελέγχου με τις στρατηγικές που αναφέρονται.
- Ζητήστε από τους συμμετέχοντες να γράψουν ένα εφαρμόσιμο βήμα για τον καθένα.
- Παράδειγμα: «Θα ενεργοποιήσω το MFA στο email μου».
- Ενθαρρύνετε τους συμμετέχοντες να επικεντρωθούν σε απλές, άμεσες ενέργειες και βοηθήστε στην αποσαφήνιση των βημάτων, εάν χρειάζεται.
4. Κοινή χρήση σε ομάδες:
- Οι συμμετέχοντες μοιράζονται ένα βήμα που σκοπεύουν να κάνουν.
- Προσφέρετε γρήγορη ανατροφοδότηση και ενθαρρύνετε τη συζήτηση σχετικά με τα οφέλη αυτών των αλλαγών.
- Ενθαρρύνετε τους συμμετέχοντες να επανεξετάζουν τακτικά τη λίστα ελέγχου τους για να ενημερώνουν τις συνήθειές τους.

Βήμα 4 Τελική αναστοχασμός και βασικά συμπεράσματα (5 λεπτά)

1. Ενισχύστε τη μάθηση και παρακινήστε τους συμμετέχοντες να εφαρμόσουν όσα έχουν μάθει.
2. Ρωτήστε τους συμμετέχοντες:
   - «Ποια είναι μια συνήθεια που σκοπεύεις να αλλάξεις ή να υιοθετήσεις ξεκινώντας από σήμερα;»
   - «Πώς θα μοιραστείς αυτά που έχεις μάθει με άλλους;»
3. Κοινή χρήση σε ομάδες:
   - Προσκαλέστε εθελοντές να μοιραστούν τις σκέψεις τους ή ένα βασικό συμπέρασμα.
4. Κλείσιμο μηνύματος:
   - Υπενθυμίστε στους συμμετέχοντες: «Η κυβερνοασφάλεια είναι ευθύνη όλων. Μικρά, σκόπιμα βήματα μπορούν να κάνουν μεγάλη διαφορά στην ασφάλεια στο διαδίκτυο».
   - Ευχαριστούμε όλους για την ενεργή συμμετοχή τους και τους ενθαρρύνουμε να αναλάβουν άμεσα δράση.

Βασικά σημεία:

Τονίστε στους συμμετέχοντες ότι η κυβερνοασφάλεια είναι μια δεξιότητα που χρειάζεται ο καθένας, ανεξάρτητα από την τεχνική του εξειδίκευση. Χρησιμοποιήστε τα βασικά σημεία του μαθήματος για να επισημάνετε πώς η κατανόηση κοινών απειλών και η υιοθέτηση προληπτικών μέτρων, όπως η χρήση ισχυρών κωδικών πρόσβασης ή η ενεργοποίηση του MFA, μπορούν να μειώσουν δραματικά τους διαδικτυακούς κινδύνους. Ενθαρρύνετε τους συμμετέχοντες να υιοθετήσουν μια προληπτική νοοτροπία θέτοντας απλούς, εφικτούς στόχους για τη βελτίωση των διαδικτυακών τους συνηθειών. Ενισχύστε αυτά τα συμπεράσματα μέσω επακόλουθων συζητήσεων ή δραστηριοτήτων που επανεξετάζουν αυτές τις έννοιες, διασφαλίζοντας ότι οι συμμετέχοντες παραμένουν σε εγρήγορση και παρακινημένοι να διατηρούν ισχυρές πρακτικές κυβερνοασφάλειας.

Παρακολούθηση και δραστηριότητες στο σπίτι

Ενθαρρύνετε τους συμμετέχοντες να εξασκήσουν όσα έμαθαν παρακολουθώντας τις διαδικτυακές τους δραστηριότητες την επόμενη εβδομάδα. Μπορούν να εντοπίσουν τομείς όπου αισθάνονται πιο ευάλωτοι και να εφαρμόσουν μία νέα στρατηγική κυβερνοασφάλειας κάθε μέρα. Επιπλέον, προτείνετε να δοκιμάσουν εργαλεία όπως το LastPass ή το Bitdefender στο σπίτι και να μοιραστούν τις εμπειρίες τους με την ομάδα σε μια συνεδρία παρακολούθησης.

Συμβουλές για εκπαιδευτικούς:

Ενσωματώστε θέματα κυβερνοασφάλειας σε καθημερινές συζητήσεις ή μαθήματα χρησιμοποιώντας παραδείγματα από την πραγματική ζωή που σχετίζονται με τις εμπειρίες των μαθητών, όπως η ασφάλεια στα μέσα κοινωνικής δικτύωσης ή οι συνήθεις απάτες. Χρησιμοποιήστε διαδραστικές μεθόδους όπως ομαδικές συζητήσεις ή σενάρια ρόλων για να κάνετε το θέμα ενδιαφέρον και πρακτικό. Ελέγχετε τακτικά την πρόοδο και παρέχετε υποστήριξη για να ενισχύσετε τη σημασία της οικοδόμησης ισχυρών συνηθειών κυβερνοασφάλειας.

Εργαλεία

LastPass

Το LastPass είναι ένα ισχυρό εργαλείο διαχείρισης κωδικών πρόσβασης που έχει σχεδιαστεί για να ενισχύει την κυβερνοασφάλεια, δημιουργώντας και αποθηκεύοντας με ασφάλεια ισχυρούς, μοναδικούς κωδικούς πρόσβασης για όλους τους διαδικτυακούς λογαριασμούς. Εξαλείφει την ανάγκη να απομνημονεύετε πολλούς σύνθετους κωδικούς πρόσβασης, αποθηκεύοντάς τους σε ένα κρυπτογραφημένο ψηφιακό θησαυροφυλάκιο, προσβάσιμο μόνο με έναν κύριο κωδικό πρόσβασης.

www.lastpass.com

Bitdefender

Το Bitdefender είναι ένα προηγμένο εργαλείο κυβερνοασφάλειας που προσφέρει ολοκληρωμένη προστασία από κακόβουλο λογισμικό, ηλεκτρονικό ψάρεμα (phishing), ransomware και άλλες διαδικτυακές απειλές. Συνδυάζει ισχυρό λογισμικό προστασίας από ιούς με έξυπνα μέτρα κατά του ηλεκτρονικού "ψαρέματος" (phishing) για να παρέχει πολυεπίπεδη ασφάλεια για προσωπική και επαγγελματική χρήση.

www.bitdefender.com

Παραπομπές

- Bitdefender. (n.d.). Retrieved from https://www.bitdefender.com
- Cisco Networking Academy. (n.d.). Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More. Retrieved from https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US
- IBM. (2024, March 25). Types of cyberthreats. Retrieved from https://www.ibm.com/think/topics/cyberthreats-types
- Lakhwani, S. (2024, June 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Retrieved from https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- LastPass. (n.d.). Retrieved from https://www.lastpass.com
- Simplilearn. (2020, June 10). What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn. [Video]. YouTube. https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Ποιος είναι ένας από τους κύριους στόχους της κυβερνοασφάλειας;

Α. Διασφαλίζει ότι κανείς δεν μπορεί να έχει πρόσβαση στο διαδίκτυο χωρίς άδεια

Β. Επιτρέπει στις επιχειρήσεις να παρακολουθούν τη δραστηριότητα των χρηστών

Γ. Προστατεύει ψηφιακά περιουσιακά στοιχεία μέσω της διαχείρισης κινδύνων και τρωτών σημείων

Δ. Αποκλείει όλα τα email από άγνωστους αποστολείς

2. Ποιο από τα παρακάτω καταδεικνύει τη χρήση πολυπαραγοντικής επαλήθευσης ταυτότητας (MFA);

Α. Σύνδεση απαντώντας σε μια ερώτηση ασφαλείας

Β. Χρήση του κωδικού πρόσβασης email σας και ενός εφεδρικού email για ανάκτηση

Γ. Συνδυασμός κωδικού πρόσβασης με έναν προσωρινό κωδικό που αποστέλλεται στο τηλέφωνό σας

Δ. Αποθήκευση κωδικών πρόσβασης σε κρυπτογραφημένο αρχείο στον υπολογιστή σας

3. Τι κάνει το ηλεκτρονικό ψάρεμα (phishing) να διαφέρει από άλλες διαδικτυακές απειλές;

Α. Περιλαμβάνει άμεση εισβολή σε συστήματα χωρίς την παρέμβαση του χρήστη

Β. Χρησιμοποιεί παραπλανητικές τακτικές για να ξεγελάσει τους χρήστες ώστε να κοινοποιήσουν ευαίσθητες πληροφορίες

Γ. Εξαπλώνεται μέσω φυσικών συσκευών, όπως μονάδες USB

Δ. Λειτουργεί αποκλειστικά εγκαθιστώντας κακόβουλο λογισμικό σε έναν υπολογιστή

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

4. Πώς βελτιώνει η ενημέρωση του λογισμικού σας την κυβερνοασφάλεια;

Α. Βελτιώνει τον σχεδιασμό και τη χρηστικότητα των εφαρμογών σας

Β. Μειώνει τις πιθανότητες εμφάνισης σφαλμάτων που επηρεάζουν τις εργασίες σας

Γ. Κλείνει τα κενά ασφαλείας που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς

Δ. Επιτρέπει καλύτερη συμβατότητα με παλαιότερο υλικό

5. Γιατί είναι ωφέλιμη η χρήση ενός διαχειριστή κωδικών πρόσβασης;

Α. Διασφαλίζει ότι όλοι οι κωδικοί πρόσβασής σας έχουν αντίγραφα ασφαλείας σε έναν κοινόχρηστο διακομιστή

Β. Σας αποσυνδέει αυτόματα από τους λογαριασμούς μετά από ένα καθορισμένο χρονικό διάστημα

Γ. Δημιουργεί και αποθηκεύει με ασφάλεια σύνθετους κωδικούς πρόσβασης για κάθε λογαριασμό

Δ. Σας ειδοποιεί όταν κάποιος αποκτά πρόσβαση στο email σας χωρίς άδεια

Λύσεις

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

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

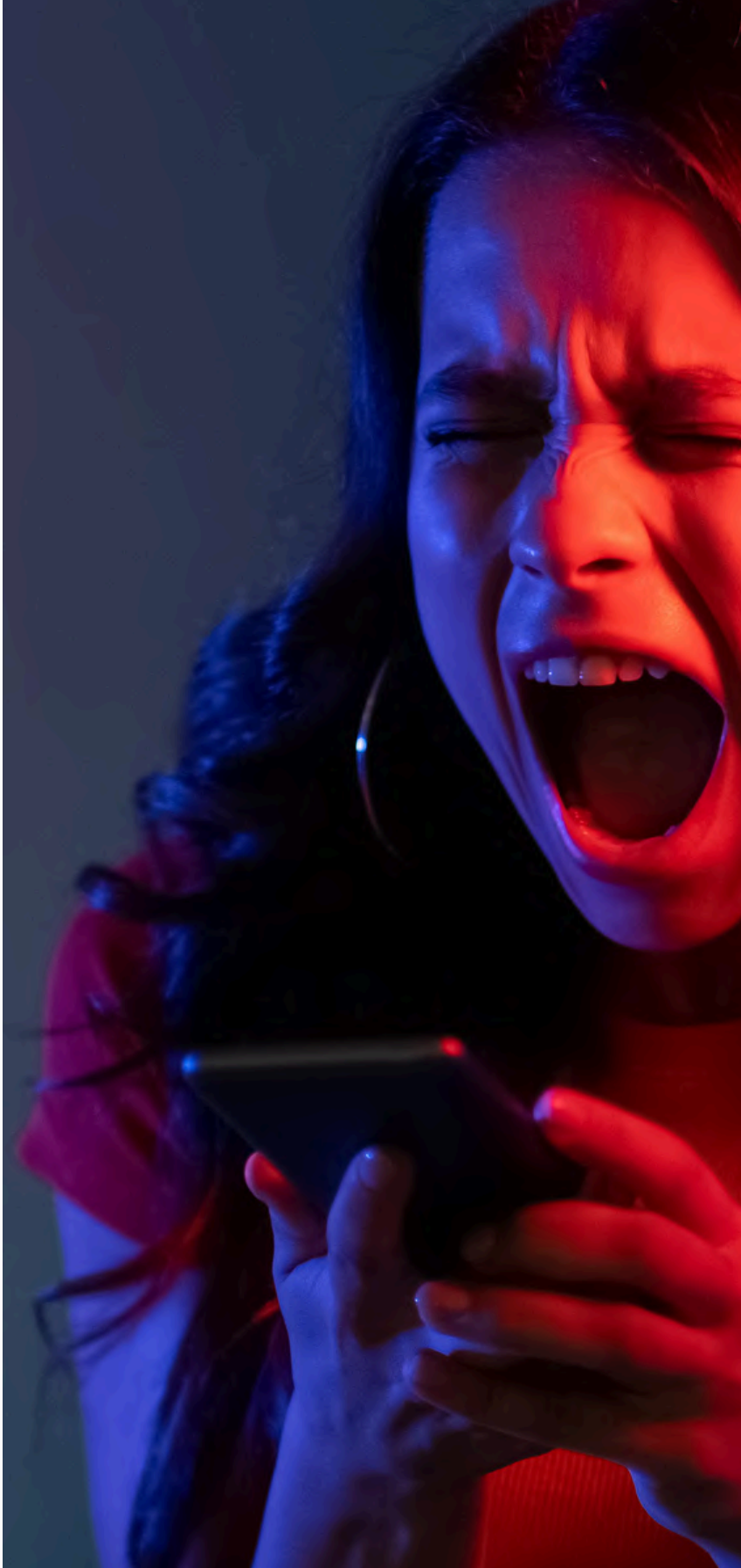
LABC

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.