



ΕΝΟΤΗΤΑ 5

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΑΣΦΑΛΕΙΑ



erasmediah.eu



**Co-funded by
the European Union**



Μάθημα 5.6

Πρακτικά εργαλεία για την ασφάλεια 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 (ΕΑΕΕΑ). Η Ευρωπαϊκή Ένωση και ο ΕΑΕΕΑ δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Μάθημα 5.6

Πρακτικά εργαλεία για την ασφάλεια στο διαδίκτυο

Στόχοι:

- Να εξοπλίσει τους συμμετέχοντες με πρακτικά εργαλεία και τεχνικές για τον εντοπισμό και τον μετριασμό κοινών διαδικτυακών απειλών, συμπεριλαμβανομένου του ηλεκτρονικού "ψαρέματος" (phishing), του κακόβουλου λογισμικού και των απατήσεων.
- Να αναπτύξει την επάρκεια στην αξιοποίηση πόρων κυβερνοασφάλειας, όπως διαχειριστές κωδικών πρόσβασης, VPN και ασφαλή προγράμματα περιήγησης, ενώ παράλληλα θα ενισχύσουν την κατανόηση της διαχείρισης του διαδικτυακού απορρήτου.
- Να προωθήσει ασφαλείς και υπεύθυνες διαδικτυακές πρακτικές μέσω της κριτικής αξιολόγησης των ψηφιακών πλατφορμών, αναγνωρίζοντας προειδοποιητικά σημάδια απειλών στον κυβερνοχώρο και υιοθετώντας προστατευτικές συνήθειες, όπως η αναφορά ύποπτων δραστηριοτήτων.

Βασικά Μηνύματα:

- Η επίγνωση και η προετοιμασία είναι η πρώτη σας γραμμή άμυνας. Η κατανόηση των διαδικτυακών απειλών και η κατοχή των κατάλληλων εργαλείων σας δίνει τη δυνατότητα να πλοηγηθείτε στον ψηφιακό κόσμο με ασφάλεια.
- Η ασφάλειά σας είναι στα χέρια σας. Η αξιοποίηση πρακτικών εργαλείων όπως VPN, ασφαλή προγράμματα περιήγησης και ρυθμίσεις απορρήτου σας επιτρέπει να προστατεύετε τα προσωπικά σας δεδομένα και να διατηρείτε τον έλεγχο της διαδικτυακής σας παρουσίας.

**ΕΙΔΟΣ ΜΑΘΗΜΑΤΟΣ:**



Επισκόπηση μαθήματος

Η διαδικτυακή ασφάλεια εξαρτάται σε μεγάλο βαθμό από την ικανότητα αποτελεσματικής χρήσης εργαλείων που έχουν σχεδιαστεί για την προστασία των προσωπικών πληροφοριών και την πρόληψη ψηφιακών απειλών. Αυτό το μάθημα δίνει έμφαση στην πρακτική, πρακτική ενασχόληση με βασικά εργαλεία κυβερνοασφάλειας, όπως διαχειριστές κωδικών πρόσβασης, VPN και ρυθμίσεις απορρήτου. Οι συμμετέχοντες θα εξερευνήσουν ενεργά πώς λειτουργούν αυτά τα εργαλεία, θα δοκιμάσουν τις λειτουργίες τους και θα μάθουν στρατηγικές για να τα ενσωματώσουν στις καθημερινές ψηφιακές ρουτίνες. Μέσω καθοδηγούμενων δραστηριοτήτων, θα χτίσουν αυτοπεποίθηση στην εφαρμογή αυτών των εργαλείων για την προστασία της διαδικτυακής τους παρουσίας και την αντιμετώπιση κινδύνων με πρακτικές λύσεις.

Το εργαστήριο οργανώνεται σε 4 βήματα:

- 1: Εισαγωγή στα εργαλεία ασφάλειας στο διαδίκτυο (10 λεπτά)
- 2: Πρακτική εξερεύνηση εργαλείων (15 λεπτά)
- 3: Διαχείριση κινδύνου βάσει σεναρίων (10 λεπτά)
- 4: Τελικές σκέψεις (5 λεπτά)

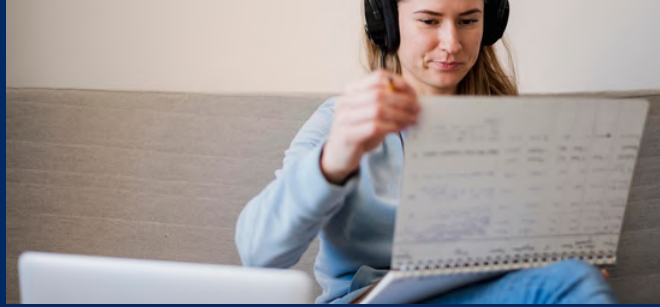


Βήμα 1

Εισαγωγή στα εργαλεία ασφάλειας στο διαδίκτυο

Έχετε ποτέ συναντήσει κάτι στο διαδίκτυο που σας φάνηκε ύποπτο; Ίσως ένα περίεργο email που σας ζητά να επαναφέρετε τον κωδικό πρόσβασής σας, ένα αναδυόμενο παράθυρο που προσφέρει ένα δωρεάν έπαθλο ή έναν ιστότοπο που ζητά πάρα πολλά προσωπικά στοιχεία; Αυτές οι καταστάσεις μπορεί να σας φαίνονται επικίνδυνες - και συχνά είναι.

Τα καλά νέα είναι ότι υπάρχουν **πρακτικά εργαλεία** που μπορείτε να χρησιμοποιήσετε για να προστατευτείτε σε στιγμές σαν κι αυτές. Μέχρι το τέλος αυτής της δραστηριότητας, θα ξέρετε πώς να αναγνωρίζετε αυτούς τους κινδύνους και να χρησιμοποιείτε εργαλεία όπως διαχειριστές κωδικών πρόσβασης, VPN και ρυθμίσεις απορρήτου για να παραμένετε ασφαλείς στο διαδίκτυο. Ας εμβαθύνουμε και ας δούμε πώς αυτά τα εργαλεία μπορούν να σας βοηθήσουν!



Βήμα 1

Εισαγωγή στα εργαλεία ασφάλειας στο διαδίκτυο

Ακολουθούν τρία απλά εργαλεία που μπορούν να κάνουν την διαδικτυακή σας ζωή πολύ πιο ασφαλή:

- **Διαχειριστές κωδικών πρόσβασης:** Αυτά σας βοηθούν να δημιουργείτε και να αποθηκεύετε ισχυρούς, μοναδικούς κωδικούς πρόσβασης, ώστε να μην χρειάζεται να τους θυμάστε όλους.
- **VPN (Εικονικά Ιδιωτικά Δίκτυα):** Αυτά προστατεύουν την online δραστηριότητά σας, ειδικά σε δημόσια Wi-Fi, διατηρώντας την σύνδεσή σας ασφαλή.
- **Ρυθμίσεις απορρήτου προγράμματος περιήγησης:** Αυτές σας επιτρέπουν να ελέγχετε ποιες πληροφορίες μπορούν να συλλέξουν οι ιστότοποι για εσάς, όπως την τοποθεσία σας ή τις συνήθειες περιήγησής σας.

Θα επικεντρωθούμε σε αυτά τα εργαλεία σήμερα, επειδή μπορούν να κάνουν τεράστια διαφορά στην ασφάλεια στο διαδίκτυο.

Σκεφτείτε την τελευταία φορά που βρήκατε κάτι στο διαδίκτυο που σας φάνηκε παράξενο - ίσως έναν ιστότοπο που δεν σας φάνηκε αξιόπιστος. Πώς το χειριστήκατε; Το αγνοήσατε, το ερευνήσατε περαιτέρω ή ίσως κάνατε κλικ σε αυτό;

Ας κάνουμε καταιγισμό ιδεών μαζί:

- Τι είδους διαδικτυακές απειλές ή κινδύνους έχετε παρατηρήσει στο παρελθόν;
- Ποια εργαλεία ή στρατηγικές χρησιμοποιείτε ήδη για να παραμένετε ασφαλείς στο διαδίκτυο;

Θα αφιερώσουμε λίγα λεπτά για να μοιραστούμε ιδέες ως ομάδα. Μην ανησυχείτε αν δεν το έχετε βιώσει αυτό από πρώτο χέρι - οι ιστορίες των συνομηλίκων σας μπορεί να πυροδοτήσουν νέες σκέψεις.



Βήμα 2

Πρακτική εξερεύνηση εργαλείων

Τώρα είναι η ώρα να εμβαθύνετε και να εξερευνήσετε πώς απλά εργαλεία μπορούν να κάνουν την διαδικτυακή σας παρουσία ασφαλέστερη. Σε αυτήν τη δραστηριότητα, θα δοκιμάσετε τις ρυθμίσεις απορρήτου του προγράμματος περιήγησης και θα δοκιμάσετε τις δεξιότητές σας στη δημιουργία κωδικών πρόσβασης χρησιμοποιώντας το The Password Meter. Ας ξεκινήσουμε!

Μέρος 1: Ρυθμίσεις απορρήτου προγράμματος περιήγησης

Το πρόγραμμα περιήγησής σας μπορεί να ελέγξει πόσες πληροφορίες συλλέγουν οι ιστότοποι για εσάς. Ας ελέγξουμε και ας προσαρμόσουμε τις ρυθμίσεις απορρήτου σας:

1. Ανοίξτε τις ρυθμίσεις απορρήτου του προγράμματος περιήγησής σας (αναζητήστε «Ρυθμίσεις» ή «Προτιμήσεις» και, στη συνέχεια, μεταβείτε στο «Απόρρητο» ή «Ασφάλεια»).

2. Εξετάστε αυτούς τους βασικούς τομείς:

- **Πρόληψη παρακολούθησης:** Είναι ενεργοποιημένη;
- **Cookies:** Αποκλείονται τα cookies τρίτων μερών;
- **Δικαιώματα:** Ποιοι ιστότοποι μπορούν να έχουν πρόσβαση στην τοποθεσία, την κάμερα ή το μικρόφωνό σας;



Βήμα 2

Πρακτική εξερεύνηση εργαλείων

3. Κάντε προσαρμογές: Ενεργοποιήστε οποιεσδήποτε ρυθμίσεις απορρήτου πιστεύετε ότι θα βοηθήσουν στην προστασία των δεδομένων σας.

Για παράδειγμα:

- Αποκλεισμός cookie παρακολούθησης.
- Απενεργοποιήστε την κοινοποίηση τοποθεσίας για ιστότοπους που δεν εμπιστεύεστε.

Γρήγορη ανασκόπηση: Τι σας εξέπληξε στις τρέχουσες ρυθμίσεις σας; Κάνετε κάποιες αλλαγές;

Μέρος 2: Έλεγχος ισχύος κωδικού πρόσβασης με το The Password Meter

Η δημιουργία ενός ισχυρού κωδικού πρόσβασης είναι ένας από τους ευκολότερους τρόπους για να προστατεύσετε τους λογαριασμούς σας. Τώρα, ας δούμε πόσο ασφαλείς είναι οι κωδικοί πρόσβασής σας:

1. Μεταβείτε στο [Μετρητή Κωδικών Πρόσβασης](#).
2. Σκεφτείτε έναν νέο κωδικό πρόσβασης (μην χρησιμοποιήσετε έναν που ήδη έχετε!).



Βήμα 2

Πρακτική εξερεύνηση εργαλείων

3. Εισαγάγετε το στο *The Password Meter* και δείτε τα σχόλια:

- Πόσο ισχυρός είναι ο κωδικός πρόσβασής σας;
- Τι προτάσεις δίνει για να το ενισχύσει;

4. Πειραματιστείτε αλλάζοντας τον κωδικό πρόσβασής σας με βάση τα σχόλια (π.χ., προσθέστε σύμβολα, κάντε τον μεγαλύτερο ή συνδυάστε πεζά και κεφαλαία γράμματα). Δείτε πώς βελτιώνεται η βαθμολογία!

Γρήγορη ανασκόπηση: Πόσο εύκολο ή δύσκολο ήταν να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης; Ποιο είναι ένα πράγμα που θα κάνετε διαφορετικά όταν ορίζετε κωδικούς πρόσβασης στο μέλλον;

Μέχρι το τέλος αυτής της δραστηριότητας, θα έχετε βελτιώσει τις ρυθμίσεις απορρήτου του προγράμματος περιήγησής σας και θα έχετε μάθει να δημιουργείτε ισχυρότερους κωδικούς πρόσβασης!



Βήμα 3

Διαχείριση κινδύνου βάσει σεναρίων

Αφού εξετάσουμε ορισμένα πρακτικά εργαλεία, ας δούμε πώς μπορούν να εφαρμοστούν σε πραγματικές καταστάσεις. Θα εργαστείτε σε μικρές ομάδες για να αναλύσετε σενάρια, να εντοπίσετε κινδύνους και να αποφασίσετε πώς να τους αντιμετωπίσετε χρησιμοποιώντας τα εργαλεία που συζητήθηκαν. Διαβάστε το σενάριο που δίνεται στην ομάδα σας. Ακολουθούν μερικά παραδείγματα:

1. *Λαμβάνετε ένα email που σας ενημερώνει ότι κερδίσατε ένα βραβείο, αλλά ο σύνδεσμος φαίνεται ύποπτος. Τι κάνετε;*
2. *Μια εφαρμογή κοινωνικής δικτύωσης ζητά πρόσβαση στην τοποθεσία, την κάμερα και το μικρόφωνό σας όταν την εγκαθιστάτε. Πρέπει να την επιτρέψετε;*
3. *Χρησιμοποιείτε δημόσιο Wi-Fi σε μια καφετέρια και σας ζητείται να συνδεθείτε σε έναν άγνωστο ιστότοπο. Πώς παραμένετε ασφαλείς;*

Συζητήστε με την ομάδα σας σχετικά με τους κινδύνους στο σενάριό σας. Αναρωτηθείτε:

- Τι μπορεί να πάει στραβά αν δεν ενεργήσετε προσεκτικά;
- Γιατί αυτή η κατάσταση σας δίνει την αίσθηση ότι δεν είστε ασφαλείς;

Αποφασίστε πώς θα μπορούσατε να χρησιμοποιήσετε πρακτικά εργαλεία για την αντιμετώπιση του κινδύνου. Για παράδειγμα:

- Χρησιμοποιήστε τις ρυθμίσεις απορρήτου του προγράμματος περιήγησης για να αποκλείσετε τα περιττά δικαιώματα.
- Αποφύγετε να κάνετε κλικ σε ύποπτους συνδέσμους και ελέγξτε τα email σας για ενδείξεις ηλεκτρονικού "ψαρέματος" (phishing).
- Ενεργοποιήστε ένα VPN για να ασφαλίσετε τη σύνδεσή σας σε δημόσιο Wi-Fi.



Βήμα 3

Διαχείριση κινδύνου βάσει σεναρίων

1. Μετά από λίγα λεπτά, κάθε ομάδα θα μοιραστεί:

- Ποιους κινδύνους εντοπίσατε στο σενάριο
- Ποια εργαλεία ή βήματα χρησιμοποιήσατε για να παραμείνετε ασφαλείς

Σκεφτείτε το: Πώς θα μπορούσαν αυτά τα εργαλεία να σας βοηθήσουν στις δικές σας διαδικτυακές δραστηριότητες;

Πρακτικά εργαλεία όπως οι ρυθμίσεις απορρήτου του προγράμματος περιήγησης, τα VPN και η ανίχνευση ηλεκτρονικού "ψαρέματος" (phishing) μπορούν να μετατρέψουν τις επικίνδυνες καταστάσεις σε διαχειρίσιμες. Η τακτική χρήση τους κάνει την παραμονή σας ασφαλή στο διαδίκτυο πολύ πιο εύκολη!

Ας αναλογιστούμε τι μάθατε και πώς θα το χρησιμοποιήσετε για να παραμείνετε ασφαλείς στο διαδίκτυο.

Βήμα 1: Αναλογιστείτε

Σκεφτείτε αυτά τα ερωτήματα:

- Ποιο εργαλείο (π.χ. ρυθμίσεις απορρήτου προγράμματος περιήγησης, VPN, διαχειριστές κωδικών πρόσβασης) ήταν το πιο χρήσιμο για εσάς; Γιατί;
- Πώς έχει αλλάξει η άποψή σας για την ασφάλεια στο διαδίκτυο μετά τη χρήση αυτών των εργαλείων;

Βήμα 2: Σχεδιάστε το επόμενο βήμα σας

Καταγράψτε μία ενέργεια που θα κάνετε για να βελτιώσετε την ασφάλειά σας στο διαδίκτυο.

- Τι θα κάνετε; (π.χ., «Θα χρησιμοποιήσω έναν διαχειριστή κωδικών πρόσβασης για να δημιουργήσω ισχυρούς κωδικούς πρόσβασης.»)
- Πότε θα το κάνετε; (π.χ., «Μέχρι το τέλος της εβδομάδας.»).

Τα πρακτικά εργαλεία είναι το πρώτο σας βήμα - μείνετε συνεπείς για να διατηρήσετε ισχυρή την ασφάλειά σας στο διαδίκτυο!





Σύνοψη των βασικών συμπερασμάτων

- Οι ρυθμίσεις απορρήτου του προγράμματος περιήγησης, οι διαχειριστές κωδικών πρόσβασης και τα VPN είναι απλά αλλά ισχυρά εργαλεία για να βελτιώσετε την ασφάλειά σας στο διαδίκτυο.
- Διαχειριστείτε ενεργά τις πληροφορίες που κοινοποιείτε στο διαδίκτυο προσαρμόζοντας τις ρυθμίσεις απορρήτου και περιορίζοντας τα περιττά δικαιώματα.
- Ενημερώνετε τακτικά τις ρυθμίσεις απορρήτου, δημιουργείτε ασφαλείς κωδικούς πρόσβασης και ελέγχετε τα δικαιώματα των εφαρμογών για να κάνετε την ασφάλεια στο διαδίκτυο μέρος της ψηφιακής σας ζωής.
- Παραμείνετε προνοητικοί - ο συνδυασμός εργαλείων με κριτική σκέψη και η ενημέρωση διασφαλίζει ότι είστε προετοιμασμένοι για τις εξελισσόμενες διαδικτυακές απειλές.
- Προσπαθήστε επίσης να δοκιμάσετε άλλα πρακτικά διαδικτυακά εργαλεία για να κατανοήσετε και να βελτιώσετε την ψηφιακή σας ασφάλεια - όσο περισσότερα εργαλεία γνωρίζετε πώς να χρησιμοποιείτε, τόσο περισσότερο θα αυξήσετε την ασφάλειά σας!



Οδηγίες για εργαζόμενους στον τομέα της νεολαίας, εκπαιδευτικούς και δασκάλους

Σκοπός:

Αυτό το μάθημα επικεντρώνεται στον εξοπλισμό των συμμετεχόντων με τις πρακτικές δεξιότητες για τη χρήση βασικών εργαλείων διαδικτυακής ασφάλειας. Μέσω ατομικών και ομαδικών ασκήσεων και συζητήσεων, θα αποκτήσουν την ικανότητα να εντοπίζουν και να αντιμετωπίζουν κοινές διαδικτυακές απειλές, να ενισχύουν την ψηφιακή τους προστασία με πόρους όπως διαχειριστές κωδικών πρόσβασης, VPN και ρυθμίσεις απορρήτου, και να ενσωματώνουν ασφαλέστερες συνήθειες στις καθημερινές διαδικτυακές τους δραστηριότητες.

Απαιτούμενα υλικά:

- Πρόσβαση στο Διαδίκτυο για εργαλεία δοκιμών (π.χ. VPN, διαχειριστές κωδικών πρόσβασης)
- Φορητοί υπολογιστές, tablet ή smartphone για πρακτικές ασκήσεις
- Λευκός πίνακας ή πίνακας παρουσιάσεων για καταιγισμό ιδεών και σύνοψη συζητήσεων
- Λευκά φύλλα χαρτιού για σημειώσεις
- Στυλό, μολύβια ή χρωματιστοί μαρκαδόροι





Βήμα 1: Εισαγωγή στα εργαλεία ασφάλειας στο διαδίκτυο (10 λεπτά)

1. Ξεκινήστε επικοινωνώντας τους συμμετέχοντες με μια σχετική ερώτηση: «Έχετε συναντήσει ποτέ κάτι στο διαδίκτυο που σας φάνηκε ύποπτο, όπως ένα παράξενο email, ένα αναδυόμενο παράθυρο που προσφέρει ένα έπαθλο ή έναν ιστότοπο που ζητά πάρα πολλά προσωπικά στοιχεία;» Εξηγήστε σύντομα ότι αυτές οι καταστάσεις μπορεί να φαίνονται επικίνδυνες και συχνά είναι, αλλά υπάρχουν πρακτικά εργαλεία για την αντιμετώπισή τους.
2. Παρουσιάστε την εστίαση της συνεδρίας σε τρία βασικά εργαλεία: τους διαχειριστές κωδικών πρόσβασης, τα VPN και τις ρυθμίσεις απορρήτου του προγράμματος περιήγησης. Επισημάνετε τη σημασία τους εξηγώντας ότι οι διαχειριστές κωδικών πρόσβασης βοηθούν στη δημιουργία και αποθήκευση ισχυρών, μοναδικών κωδικών πρόσβασης, τα VPN ασφαλίζουν την online δραστηριότητα σε δημόσια Wi-Fi και οι ρυθμίσεις απορρήτου του προγράμματος περιήγησης ελέγχουν ποιες πληροφορίες μπορούν να συλλέξουν οι ιστότοποι, όπως η τοποθεσία ή οι συνήθειες περιήγησης.
3. Ενθαρρύνετε τους συμμετέχοντες να αναλογιστούν τις δικές τους εμπειρίες με τους διαδικτυακούς κινδύνους ρωτώντας: «Σκεφτείτε την τελευταία φορά που αντιμετωπίσατε κάτι ύποπτο στο διαδίκτυο. Πώς το χειριστήκατε;»
4. Διευκολύνετε μια σύντομη συζήτηση με ερωτήσεις όπως «Τι είδους διαδικτυακές απειλές έχετε παρατηρήσει;» και «Ποια εργαλεία ή στρατηγικές χρησιμοποιείτε ήδη για να παραμείνετε ασφαλείς;» Προσκαλέστε τους συμμετέχοντες να μοιραστούν τις ιστορίες ή τις ιδέες τους, τονίζοντας ότι η μάθηση ο ένας από τον άλλον μπορεί να πυροδοτήσει νέες γνώσεις.
5. Ολοκληρώστε τονίζοντας τη σημασία αυτών των εργαλείων στη διαχείριση των διαδικτυακών κινδύνων, δηλώνοντας: «Χρησιμοποιώντας εργαλεία όπως διαχειριστές κωδικών πρόσβασης, VPN και ρυθμίσεις απορρήτου, μπορείτε να πλοηγηθείτε με σιγουριά στον ψηφιακό κόσμο προστατεύοντας παράλληλα τα προσωπικά σας στοιχεία». Διατηρήστε τη συζήτηση διαδραστική και υποστηρικτική, διασφαλίζοντας ότι οι συμμετέχοντες αισθάνονται ότι ενθαρρύνονται να μοιραστούν τις σκέψεις τους και να μάθουν από την ομάδα.





Βήμα 2: Πρακτική εξερεύνηση εργαλείων (15 λεπτά)

1. Ξεκινήστε εξηγώντας τον στόχο αυτής της δραστηριότητας: να εξερευνήσετε πρακτικά εργαλεία που ενισχύουν την ασφάλεια στο διαδίκτυο μέσω των ρυθμίσεων απορρήτου του προγράμματος περιήγησης και των δοκιμών ισχύος του κωδικού πρόσβασης.
2. Χωρίστε τη δραστηριότητα σε δύο μέρη για να εξασφαλίσετε μια δομημένη προσέγγιση.

Μέρος 1: Ρυθμίσεις απορρήτου προγράμματος περιήγησης (8 λεπτά)

1. Καθοδηγήστε τους συμμετέχοντες να ανοίξουν τις ρυθμίσεις απορρήτου του προγράμματος περιήγησης τους (πλοηγηθείτε στις «Ρυθμίσεις» ή στις «Προτιμήσεις» και, στη συνέχεια, βρείτε τις επιλογές «Απόρρητο» ή «Ασφάλεια»). Ζητήστε τους να εξετάσουν βασικούς τομείς:
 - Πρόληψη παρακολούθησης: Βεβαιωθείτε ότι είναι ενεργοποιημένη.
 - Cookies: Ελέγξτε αν τα cookies τρίτων έχουν αποκλειστεί.
 - Δικαιώματα: Ελέγξτε ποιοι ιστότοποι έχουν πρόσβαση στην τοποθεσία, την κάμερα ή το μικρόφωνό τους.
2. Ενθαρρύνετε τους συμμετέχοντες να κάνουν προσαρμογές, όπως να αποκλείουν τα cookies παρακολούθησης ή να απενεργοποιούν την περιττή κοινοποίηση τοποθεσίας.
3. Στη συνέχεια, παρακινήστε τους συμμετέχοντες σε μια γρήγορη ανασκόπηση: «Τι σας εξέπληξε στις τρέχουσες ρυθμίσεις σας; Κάνετε κάποιες αλλαγές;» Αυτό βοηθά τους συμμετέχοντες να συνδέσουν τις ανακαλύψεις τους με την αξία αυτών των εργαλείων.

Μέρος 2: Δοκιμή ισχύος κωδικού πρόσβασης (5 λεπτά)

1. Κατευθύνετε τους συμμετέχοντες στην πρόσβαση στο The Password Meter. Ζητήστε τους να δημιουργήσουν έναν νέο κωδικό πρόσβασης (όχι έναν που χρησιμοποιούν αυτήν τη στιγμή) και να ελέγξουν την ισχύ του.
2. Ενθαρρύνετε τους να αναλύσουν τα σχόλια και να πειραματιστούν με αλλαγές, όπως η προσθήκη συμβόλων, η ανάμειξη πεζών-κεφαλαίων ή η αύξηση του μήκους, για να δουν πώς βελτιώνεται η βαθμολογία.
3. Ολοκληρώστε με μια ανασκόπηση: «Πόσο εύκολο ή δύσκολο ήταν να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης; Ποιο είναι ένα πράγμα που θα κάνετε διαφορετικά όταν ορίζετε κωδικούς πρόσβασης στο μέλλον;»
4. Ολοκληρώστε τη δραστηριότητα ενισχύοντας την πρακτική της αξία.
5. Διατηρήστε τη συνεδρία διαδραστική και ενδιαφέρουσα, προσφέροντας καθοδήγηση όποτε χρειάζεται, ενώ οι συμμετέχοντες εξερευνούν και εφαρμόζουν αυτά τα εργαλεία.



Βήμα 3: Διαχείριση κινδύνου βάσει σεναρίων (10 λεπτά)

1. Αυτή η δραστηριότητα βοηθά τους συμμετέχοντες να εφαρμόσουν εργαλεία διαδικτυακής ασφάλειας σε σενάρια πραγματικής ζωής. Χωρίστε τους συμμετέχοντες σε μικρές ομάδες και αναθέστε σε κάθε ομάδα ένα σενάριο, όπως:

- Ένα ύποπτο email με σύνδεσμο για έπαθλο.
- Μια εφαρμογή κοινωνικής δικτύωσης που ζητά υπερβολικά δικαιώματα.
- Χρησιμοποιώ δημόσιο Wi-Fi και αντιμετωπίζω μια άγνωστη προτροπή σύνδεσης.

2. Δώστε οδηγίες στις ομάδες να συζητήσουν τους κινδύνους, λαμβάνοντας υπόψη:

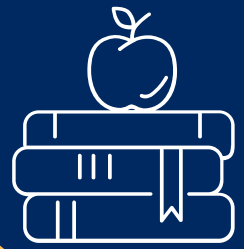
- «Τι θα μπορούσε να πάει στραβά αν δεν ενεργήσεις προσεκτικά;»
- «Γιατί αυτή η κατάσταση μου δίνει την αίσθηση ότι δεν είμαι ασφαλής;»

3. Ζητήστε τους να προσδιορίσουν πώς να χειριστούν τον κίνδυνο χρησιμοποιώντας εργαλεία όπως οι ρυθμίσεις απορρήτου του προγράμματος περιήγησης, η αποφυγή συνδέσμων ηλεκτρονικού "ψαρέματος" (phishing) ή η ενεργοποίηση ενός VPN.

4. Στη συνέχεια, κάθε ομάδα παρουσιάζει τους κινδύνους που εντόπισε και τα εργαλεία που χρησιμοποίησε για την αντιμετώπισή τους.

5. Ολοκληρώστε επισημαίνοντας: «Εργαλεία όπως οι ρυθμίσεις απορρήτου, τα VPN και η ανίχνευση ηλεκτρονικού «ψαρέματος» (phishing) διευκολύνουν τη διαχείριση των διαδικτυακών κινδύνων. Η τακτική χρήση αυτών των εργαλείων ενισχύει την ασφάλεια στο διαδίκτυο». Διατηρήστε την ενότητα στοχευμένη και ενθαρρύνετε πρακτικές, εφαρμόσιμες γνώσεις.





Βήμα 4: Τελικές σκέψεις (5 λεπτά)

1. Ολοκληρώστε τη συνεδρία καθοδηγώντας τους συμμετέχοντες σε μια αναστοχαστική άσκηση για να εμπεδώσουν τη μάθησή τους. Ξεκινήστε ζητώντας τους να σκεφτούν:

- «Ποιο εργαλείο (π.χ. ρυθμίσεις απορρήτου προγράμματος περιήγησης, VPN, διαχειριστές κωδικών πρόσβασης) ήταν το πιο χρήσιμο για εσάς; Γιατί;»
- «Πώς έχει αλλάξει η άποψή σας για την ασφάλεια στο διαδίκτυο μετά τη χρήση αυτών των εργαλείων;»

2. Ενθαρρύνετε τους συμμετέχοντες να μοιραστούν σύντομα τις σκέψεις τους, καλλιεργώντας ένα υποστηρικτικό περιβάλλον για συζήτηση.

3. Στη συνέχεια, παροτρύνετέ τους να σχεδιάσουν μια συγκεκριμένη δράση για την ενίσχυση της διαδικτυακής τους ασφάλειας, όπως:

- «Τι θα κάνεις;» (π.χ., «Θα χρησιμοποιήσω έναν διαχειριστή κωδικών πρόσβασης για να δημιουργήσω ισχυρούς κωδικούς πρόσβασης.»)
- «Πότε θα το κάνεις;» (π.χ., «Μέχρι το τέλος της εβδομάδας.»)

4. Ολοκληρώστε τονίζοντας τη σημασία της συνέπειας, υπενθυμίζοντας στους συμμετέχοντες: «Τα πρακτικά εργαλεία είναι το πρώτο σας βήμα - μείνετε συνεπείς για να διατηρήσετε ισχυρή την ασφάλειά σας στο διαδίκτυο!» Διατηρήστε τον τόνο παρακινητικό και επικεντρωμένο στην εφαρμογή των διδαγμάτων που αντλήσατε στις καθημερινές διαδικτυακές πρακτικές.

Βασικά σημεία:

Μετά την ολοκλήρωση του μαθήματος, οι συμμετέχοντες θα αποκτήσουν μια σαφή κατανόηση του τρόπου χρήσης βασικών εργαλείων, όπως διαχειριστές κωδικών πρόσβασης, VPN και ρυθμίσεις απορρήτου του προγράμματος περιήγησης, για την ενίσχυση της διαδικτυακής τους ασφάλειας. Θα μάθουν να εντοπίζουν κοινές απειλές, όπως η παρακολούθηση δεδομένων, και να λαμβάνουν προληπτικά μέτρα για την προστασία των προσωπικών τους πληροφοριών. Ενσωματώνοντας αυτά τα εργαλεία και τις στρατηγικές στην καθημερινή τους ρουτίνα, θα είναι σε θέση να πλοηγούνται στον ψηφιακό κόσμο με σιγουριά, ελαχιστοποιώντας τις πιθανές απειλές. Για να επικοινωνήσετε αποτελεσματικά αυτά τα συμπεράσματα, θα πρέπει να χρησιμοποιήσετε σχετικά σενάρια και σαφή παραδείγματα για να δείξετε τον πραγματικό αντίκτυπο αυτών των εργαλείων στην καθημερινή διαδικτυακή ασφάλεια.



Δραστηριότητες παρακολούθησης και δραστηριότητες στο σπίτι:

Εμπνεύστε τους συμμετέχοντες να εξετάσουν πιο προσεκτικά τις τρέχουσες πρακτικές τους στο διαδίκτυο, εξετάζοντας και προσαρμόζοντας τις ρυθμίσεις απορρήτου του προγράμματος περιήγησης, δοκιμάζοντας την ισχύ των κωδικών πρόσβασής τους με εργαλεία όπως το The Password Meter και εξερευνώντας τη λειτουργικότητα του VPN. Αναθέστε τους να αξιολογήσουν τα δικαιώματα εφαρμογών που χρησιμοποιούνται συχνά, σημειώνοντας πιθανούς κινδύνους και εφαρμόζοντας ασφαλέστερες εναλλακτικές λύσεις. Τέλος, ζητήστε από τους συμμετέχοντες να μοιραστούν μια νέα συμβουλή ασφαλείας με έναν φίλο ή μέλος της οικογένειάς τους, ενισχύοντας τις γνώσεις τους και ευαισθητοποιώντας τους σχετικά με την ψηφιακή ασφάλεια.

Συμβουλές για εκπαιδευτικούς:

Μπορείτε να χρησιμοποιήσετε πρακτικά παραδείγματα από τον πραγματικό κόσμο και άλλες διαδραστικές ασκήσεις για να δείξετε πώς εργαλεία όπως οι διαχειριστές κωδικών πρόσβασης, τα VPN και οι ρυθμίσεις απορρήτου μπορούν να χρησιμοποιηθούν αποτελεσματικά για την ενίσχυση της ασφάλειας στο διαδίκτυο. Δείξτε στους συμμετέχοντες βήμα προς βήμα πώς να πλοηγούνται και να διαμορφώνουν αυτά τα εργαλεία, καθιστώντας τη συνεδρία πρακτική και εφαρμόσιμη. Δημιουργήστε ένα ανοιχτό και υποστηρικτικό περιβάλλον όπου οι συμμετέχοντες αισθάνονται άνετα να συζητούν τις εμπειρίες τους με τις διαδικτυακές απειλές και να θέτουν ερωτήσεις. Επισημάνετε τη σημασία της τακτικής χρήσης αυτών των εργαλείων και της ενσωμάτωσής τους στις καθημερινές διαδικτυακές ρουτίνες για να διασφαλίσετε συνεπή και προληπτική ψηφιακή προστασία.





Εργαλεία

Get Safe Online



Ένας ολοκληρωμένος ιστότοπος που προσφέρει δωρεάν, απλές συμβουλές για ένα ευρύ φάσμα θεμάτων ασφάλειας στο διαδίκτυο. Περιλαμβάνει πρακτικούς οδηγούς για την προστασία των προσωπικών πληροφοριών, την αποφυγή απάτης και την ασφαλή διαδικτυακή επικοινωνία. Το περιεχόμενο είναι φιλικό προς το χρήστη και έχει σχεδιαστεί για άτομα με ελάχιστες τεχνικές γνώσεις.

www.getsafeonline.org

The Password Meter



Ένα δωρεάν εργαλείο που αξιολογεί την ισχύ των κωδικών πρόσβασης και παρέχει συμβουλές για τη βελτίωσή τους. Οι μαθητές μπορούν να πειραματιστούν με τη δημιουργία κωδικών πρόσβασης και να λάβουν άμεσα σχόλια σχετικά με το επίπεδο ασφαλείας τους, καθιστώντας το έναν διαδραστικό τρόπο για να κατανοήσουν τη σημασία των ισχυρών κωδικών πρόσβασης.

passwordmeter.com



Παραπομπές

- Alice. (2022, October 3). 5 Tools That Help Keep People Safe Online. Ryadel. Retrieved from <https://www.ryadel.com/en/5-privacy-data-protection-security-tools>
- Get Safe Online. (n.d.). Retrieved from <https://www.getsafeonline.org>
- Goodwall Team. (2022, March 24). 7 Best Online Safety Tools and Privacy Settings to Keep Yourself Protected. Retrieved from <https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings>
- 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>
- The Password Meter. (n.d.). Retrieved from <https://passwordmeter.com>
- Vodafone. (n.d.). Using online safety and wellbeing tools. Retrieved from <https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools>





ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Ποια είναι η κύρια λειτουργία ενός Εικονικού Ιδιωτικού Δικτύου (VPN);
 - A. Παροχή αυτόματης προστασίας από ιούς
 - B. Αύξηση της ταχύτητας του Διαδικτύου
 - Γ. Αποτροπή εμφάνισης αναδυόμενων διαφημίσεων σε όλους τους ιστότοπους
 - Δ. Κρυπτογράφηση της διαδικτυακής δραστηριότητας, ειδικά σε δημόσια Wi-Fi

2. Ποια συμπεριφορά θα μπορούσε να θέσει σε κίνδυνο την ασφάλειά σας στο διαδίκτυο;
 - A. Χρήση ισχυρών, μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό
 - B. Τακτική προσαρμογή των ρυθμίσεων απορρήτου στο πρόγραμμα περιήγησής σας
 - Γ. Χρήση ενός διαχειριστή κωδικών πρόσβασης για την αποθήκευση των διαπιστευτηρίων σύνδεσης
 - Δ. Κλικ σε κάθε σύνδεσμο σε ανεπιθύμητα email

3. Ποιο είναι ένα συνιστώμενο βήμα για τη βελτίωση των ρυθμίσεων απορρήτου του προγράμματος περιήγησής σας;
 - A. Χρήση προεπιλεγμένων ρυθμίσεων χωρίς τροποποιήσεις
 - B. Αποκλεισμός cookie παρακολούθησης και απενεργοποίηση περιττών δικαιωμάτων
 - Γ. Απενεργοποίηση cookie για όλους τους ιστότοπους
 - Δ. Επιτρέποντας σε όλους τους ιστότοπους να έχουν πρόσβαση στην τοποθεσία σας





ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

4. Ποιος είναι ο σκοπός των ρυθμίσεων απορρήτου του προγράμματος περιήγησης;
- A. Η επιτάχυνση της εμπειρίας περιήγησης του χρήστη
 - B. Η ασφαλής αποθήκευση των κωδικών πρόσβασης των χρηστών
 - Γ. Ο έλεγχος των πληροφοριών που μπορούν να συλλέξουν οι ιστότοποι σχετικά με τον χρήστη
 - Δ. Η αποτροπή αναδυόμενων διαφημίσεων σε όλους τους ιστότοπους
5. Πώς μπορείτε να βελτιώσετε την ισχύ του κωδικού πρόσβασής σας;
- A. Συμπεριλαμβάνοντας σύμβολα, αναμειγνύοντας πεζά-κεφαλαία και αυξάνοντας το μήκος
 - B. Χρησιμοποιώντας κοινές φράσεις που είναι εύκολο να θυμάστε
 - Γ. Αποφεύγοντας τη χρήση αριθμών και ειδικών χαρακτήρων
 - Δ. Δοκιμάζοντας τον ίδιο κωδικό πρόσβασης επανειλημμένα





Λύσεις

Ερώτηση 1: Δ

Ερώτηση 2: Δ

Ερώτηση 3: Β

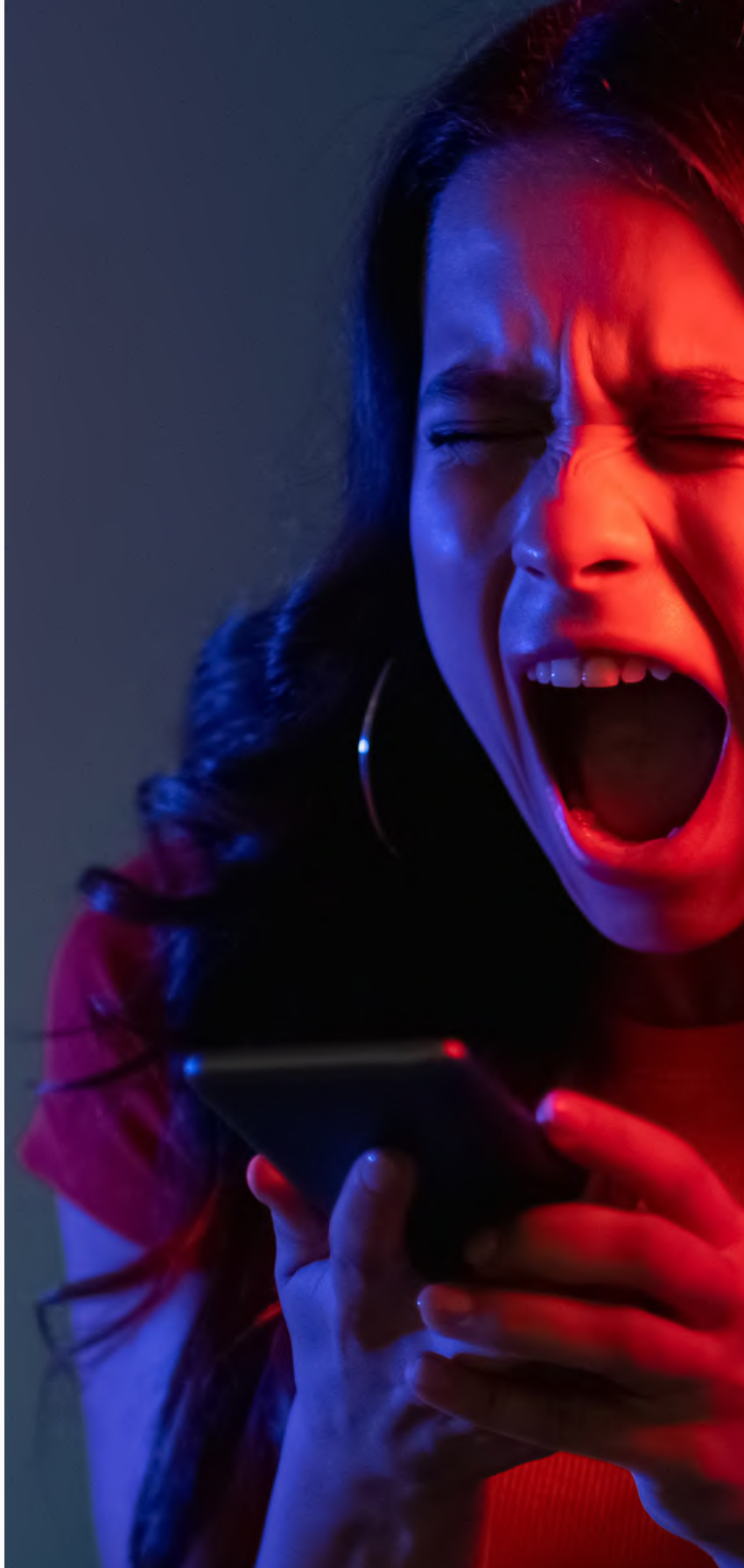
Ερώτηση 4: Γ

Ερώτηση 5: Α





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.