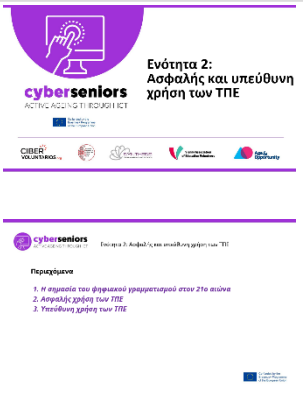
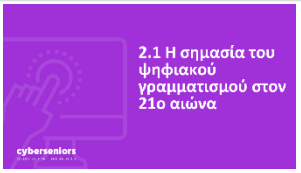
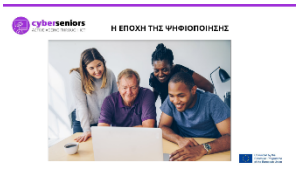
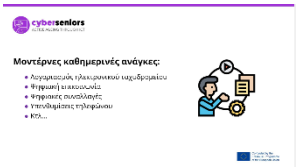
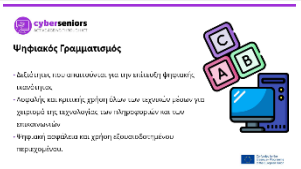
ΟΔΗΓΟΣ ΚΑΤΑΡΤΙΣΗΣ

Ενότητα 2/ Ασφαλής και υπεύθυνη χρήση των ΤΠΕ

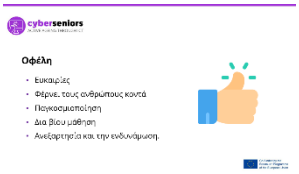
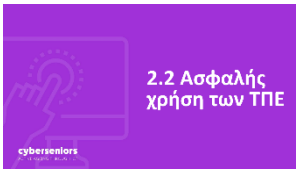
Πριν ξεκινήσετε την εκπαίδευση	
Βεβαιωθείτε ότι έχετε ετοιμάσει τα εξής:	• Ηλεκτρονικός υπολογιστής • Παρουσίαση • USB • Κατεβάσατε τις απαραίτητες εφαρμογές
Ο εκπαιδευτής	Προετοιμάστε καλά την παρουσίασή σας
	Έχετε μια θετική και παρακινητική στάση
	Να είστε ακριβείς στην ώρα σας

Κατά τη διάρκεια της εκπαίδευσης		
Διάρκεια	**Κυρίως μέρος**	Σχετική διαφάνεια παρουσίασης
2 λεπτά	Πριν ξεκινήσετε κάθε συνεδρία: • Καλωσορίστε τους συμμετέχοντες και συστηθείτε για να δημιουργήσετε μια καλή ατμόσφαιρα. • Να λαμβάνετε υπόψη για το χρόνο ανά πάσα στιγμή, ώστε να μπορέσετε να καλύψετε όλο το υλικό. • Αφήστε λίγο χρόνο στο τέλος για να απαντήσετε σε ερωτήσεις. • Ενεργήστε με ενσυναίσθηση, υπομονή και εγγύτητα. • Προσπαθήστε να βεβαιώνεστε κατά καιρούς ότι οι συμμετέχοντες σας ακολουθούν τις επεξηγήσεις σας.	
3 λεπτά	Θα εξηγήσουμε ότι το Cyberseniors είναι ένα έργο που συγχρηματοδοτείται από την Ευρωπαϊκή Επιτροπή μέσω του προγράμματος Erasmus+, με κύριο στόχο τη δημιουργία εκπαιδευτικών πόρων για άτομα άνω των 55 ετών, σχετικά με τον τρόπο διαχείρισης ενός smartphone, καθώς και χρήσιμων εφαρμογών για μια ενεργή γήρανση και μεγαλύτερη αυτονομία. Υπενθυμίζουμε ότι όλες οι πληροφορίες, καθώς και αυτοί οι πόροι, είναι διαθέσιμοι στη διεύθυνση www.ciberseniors.org	

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή του παρόντος εγγράφου δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει μόνο τις απόψεις των δημιουργών, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.

	Θα εξηγήσουμε το ευρετήριο της σημερινής συνεδρίας και θα ενημερώσουμε επίσης για το περιεχόμενο των 4 ενοτήτων (4 ώρες εκπαίδευσης συνολικά): 1. Εισαγωγή στη χρήση του smartphone/tablet 2. Ασφαλής και υπεύθυνη χρήση των τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) 3. Εφαρμογές ΤΠΕ για κινητά τηλέφωνα και tablet I (αναψυχή, υγεία, επικοινωνία) 4. Εφαρμογές ΤΠΕ για κινητά τηλέφωνα και tablet II (τραπεζικές συναλλαγές, καθημερινές ανάγκες και προσβασιμότητα, δημόσια διοίκηση).	
10 λεπτά	Η εξέλιξη της ψηφιακής τεχνολογίας έχει μεταμορφώσει τον τρόπο με τον οποίο αλληλεπιδρούμε με το περιβάλλον μας και τον τρόπο με τον οποίο πραγματοποιούμε τις καθημερινές μας δραστηριότητες. Ο ψηφιακός γραμματισμός είναι μια θεμελιώδης δεξιότητα για όλους μας, προκειμένου να μάθουμε πώς να πλοηγούμαστε στον ψηφιοποιημένο σύγχρονο κόσμο και να προσαρμοζόμαστε στις μεταβαλλόμενες ανάγκες.	 
	Σύγχρονες καθημερινές ανάγκες: • Ηλεκτρονικό ταχυδρομείο • Ψηφιακή επικοινωνία • Ψηφιακές συναλλαγές • Τηλεφωνικές υπενθυμίσεις	
	Ο ψηφιακός γραμματισμός αναφέρεται: • στις δεξιότητες που απαιτούνται για την επίτευξη ψηφιακής ικανότητας • στην ασφαλή και κριτική χρήση όλων των τεχνικών μέσων για χειρισμό της τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ) για την εργασία, τον ελεύθερο χρόνο, τη μάθηση και την επικοινωνία (Eurostat Glossary, 2019), • στην εξοικείωση με τα βασικά της ψηφιακής ασφάλειας και τη χρήση εξουσιοδοτημένου περιεχομένου.	

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή του παρόντος εγγράφου δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει μόνο τις απόψεις των δημιουργών, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.

	Ο ψηφιακός γραμματισμός έχει τα ακόλουθα οφέλη: • Ανοίγει έναν κόσμο ευκαιριών • Φέρνει τους ανθρώπους μαζί • Επιτρέπει τα πράγματα να λαμβάνουν χώρα εξ αποστάσεως (στην εποχή του Covid αυτό είναι πολύ σημαντικό) • Ενισχύει τις δεξιότητες και επιτρέπει τη διά βίου μάθηση • Προωθεί την ανεξαρτησία και την ενδυνάμωση.	
15 λεπτά	Προκειμένου να χρησιμοποιήσουμε τα εργαλεία Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) με ασφάλεια, θέλουμε να παρουσιάσουμε μερικές από τις κύριες απειλές που υπάρχουν στο διαδίκτυο. Σκοπός είναι να **υποδυθεί** κάποιος άλλο άτομο προκειμένου να κλέψει δεδομένα ή να τροποποιήσει τα δεδομένα που περιέχει ένας διακομιστής. Οι τεχνικές phishing χρησιμοποιούν επίσης απάτη ταυτότητας για να μας κάνουν να νομίζουμε ότι στέλνουμε τα δεδομένα μας σε έναν αξιόπιστο ιστότοπο, ενώ στην πραγματικότητα τα λαμβάνει ο χάκερ, π.χ. υποδύεται τον εαυτό του μέσω του facebook για να κλέψει τον κωδικό πρόσβασής μας. Το **Trojan** είναι λογισμικό που μεταμφιέζεται ως ευεργετικό και προσποιείται ότι το εγκαθιστούμε εμείς προκειμένου να αποκτήσει πρόσβαση στα δεδομένα μας ή να μετατρέψει τον υπολογιστή μας σε μέλος ενός botnet. Μπορεί να μεταμφιεστεί ως οτιδήποτε, σουίτες γραφείου, antivirus, τραπεζικό λογισμικό κ.λπ. Για το λόγο αυτό, είναι απαραίτητο να μην εμπιστευόμαστε οποιοδήποτε λογισμικό εγκαθιστούμε. Θα πρέπει να εγκαθιστούμε λογισμικά μόνο από αξιόπιστες πηγές (καταστήματα εφαρμογών) και θα πρέπει να ελέγχουμε κάθε λογισμικό που εγκαθιστούμε με ένα antivirus. **SPAM**: η έννοια του spam είναι πολύ ευρεία και καλύπτει κάθε ανεπιθύμητη επικοινωνία με κάποιον που μπορεί να γίνει ανύπαρκτη και να επαναληφθεί ή όχι. Κατά γενικό κανόνα παράγεται από το ηλεκτρονικό ταχυδρομείο, αλλά μπορεί να παραχθεί και με οποιοδήποτε άλλο μέσο, whatsapp, sms, τηλεφώνημα κ.λπ. Ο σκοπός μπορεί να είναι η απόκτηση πληροφοριών από ιστότοπο, η κλοπή δεδομένων, η εγκατάσταση κακόβουλου λογισμικού κ.λπ. Η **κοινωνική μηχανική** εκμεταλλεύεται την αδυναμία μας ως άνθρωποι να εμπιστευόμαστε τους άλλους και έτσι αποκτά τις απαραίτητες πληροφορίες για μια επίθεση. Για παράδειγμα... μια κλήση "υποστήριξης" που μας ζητάει τον κωδικό πρόσβασης υπηρεσίας για την επίλυση ενός προβλήματος. Κοινωνική μηχανική θεωρείται επίσης η μελέτη των δημόσιων πληροφοριών ενός χρήστη (κοινωνικά δίκτυα, προσωπικές ιστοσελίδες κ.λπ.) προκειμένου να	 

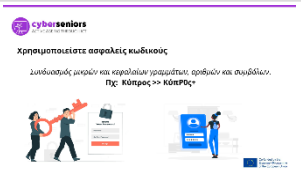
αποκτηθούν σχετικές πληροφορίες για μια επίθεση... π.χ. Δημοσιεύουμε το όνομα του κατοικίδιου ζώου μας στο Facebook με καθολική προβολή. Ένας υποτιθέμενος επιτιθέμενος θα προσθέσει αυτές τις πληροφορίες στη λίστα των κωδικών πρόσβασης που θα προσπαθήσει να εισέλθει στους λογαριασμούς.

Phishing: Το **Phishing** είναι μια τεχνική που οδηγεί στην εγκατάσταση κακόβουλου λογισμικού, στην κλοπή δεδομένων ή χρημάτων μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, ιστότοπων, τηλεφωνικών κλήσεων (vishing) ή SMS (smishing) που φαίνονται νόμιμα στην εμφάνιση και το πλαίσιο, αλλά μπορεί να μας οδηγήσουν σε έναν ιστότοπο όπου πρόκειται να κλέψουν δεδομένα, να διευκολύνουν την εγκατάσταση κακόβουλου λογισμικού ή να κλέψουν χρήματα από τις πιστωτικές μας κάρτες, μεταξύ άλλων.

Adware: είναι ένα λογισμικό που μας εμφανίζει διαφημίσεις στις εφαρμογές ή στις ιστοσελίδες που επισκεπτόμαστε, προκειμένου να αποφέρει κέρδη στον δημιουργό του κακόβουλου λογισμικού μέσω των κλικ μας στις διαφημίσεις.

Spyware: είναι ένα λογισμικό που κατασκοπεύει τις ενέργειές μας στη συσκευή μας. Εάν η συσκευή μας διαθέτει λειτουργίες πολυμέσων ή αισθητήρες θέσης, μπορεί να κατασκοπεύσει αυτές τις πληροφορίες, να ενεργοποιήσει κάμερες ή μικρόφωνα ή να αποκτήσει πρόσβαση στη θέση μας στο κινητό κ.λπ.

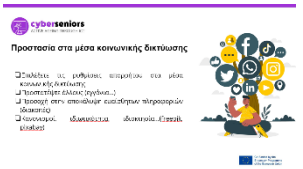
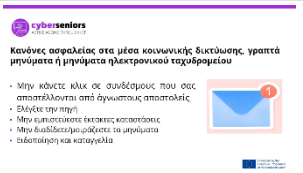
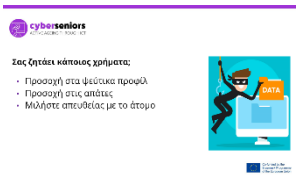
Οι μισοί από τους ηλικιωμένους δεν χρησιμοποιούν τη λειτουργία κωδικού πρόσβασης σε τουλάχιστον μία από τις συσκευές τους με δυνατότητα σύνδεσης στο διαδίκτυο, δημιουργώντας έτσι την πιθανότητα να μπορεί να τον εντοπίσει οποιοσδήποτε.



Κλειδώστε όλες τις συσκευές σας, συμπεριλαμβανομένου του υπολογιστή, του tablet και του smartphone, με ισχυρούς κωδικούς πρόσβασης. Αυτό θα κρατήσει μακριά τα αδιάκριτα βλέμματα και θα αποτελέσει άμυνα σε περίπτωση που οι συσκευές σας χαθούν ή κλαπούν.

Πόσο συχνά πρέπει να αλλάζετε τους κωδικούς πρόσβασης;
Αν δεν αντιληφθείτε παραβίαση κωδικού πρόσβασης, δεν υπάρχει λόγος να αλλάζετε συχνά τους κωδικούς σας, αν ο καθένας από αυτούς είναι ισχυρός και μοναδικός.

Ωστόσο, αν πιστεύετε ότι κάποιος από τους λογαριασμούς σας έχει παραβιαστεί, αλλάξτε αμέσως τον κωδικό πρόσβασής σας.

	Κατά τη δημιουργία αναρτήσεων στα μέσα κοινωνικής δικτύωσης, μπορείτε να επιλέξετε τις ρυθμίσεις απορρήτου για να επιλέξετε ποιο κοινό θα δει την ανάρτησή σας. Θα μπορούσε να είναι μόνο οι φίλοι που προσθέσατε στο κοινωνικό δίκτυο, θα μπορούσε να είναι μια δημόσια ανάρτηση για οποιονδήποτε ή θα μπορούσε να είναι μια ιδιωτική ανάρτηση μόνο για εσάς. Μπορείτε επίσης να καθορίσετε ή να μην καθορίσετε την τοποθεσία σας. Βεβαιωθείτε ότι τα προσωπικά σας στοιχεία δεν κοινοποιούνται (κωδικοί πρόσβασης, αριθμός τηλεφώνου, email κ.λπ.)	
	Κατά τη διάρκεια της επικοινωνίας σας μέσω κοινωνικών δικτύων, μηνυμάτων και ηλεκτρονικού ταχυδρομείου, θα πρέπει να είστε προσεκτικοί και να μην κάνετε κλικ σε συνδέσμους που σας στέλνει ένα άγνωστο άτομο. Οι εγκληματίες του κυβερνοχώρου μπορούν να υποδυθούν, για παράδειγμα, υπαλλήλους του Facebook ή την υπηρεσία ασφαλείας του Instagram. Μην εμπιστεύεστε αυτά τα μηνύματα, αν τα λαμβάνετε μέσω μιας κανονικής συνομιλίας, μιας ανάρτησης ή από μια κανονική σελίδα του Facebook. Τα μηνύματα ασφαλείας θα σας αποστέλλονται μέσω ειδοποιήσεων ή θα είναι διαθέσιμα στις ρυθμίσεις. Οι υπάλληλοι των μέσων κοινωνικής δικτύωσης δεν θα σας ζητήσουν ποτέ τον κωδικό πρόσβασής σας ή τις προσωπικές σας πληροφορίες.	
	Εάν οι φίλοι σας ή η οικογένειά σας σας ζητήσουν βοήθεια σε περίπτωση επειγόντως περιστατικού, καλέστε τους πάντα τηλεφωνικώς, ώστε να επιβεβαιώσετε ότι το μήνυμα προήλθε όντως από αυτούς. Αλλιώς, τα μηνύματα μπορεί να προέρχονται από εγκληματίες του κυβερνοχώρου. Μπορούν να δημιουργήσουν ένα προφίλ ίδιο με ενός μέλους της οικογένειας ή φίλου σας και να προσπαθήσουν να αποσπάσουν χρήματα από εσάς.	
	Μπορείτε να χρησιμοποιήσετε το εργαλείο **«Βρες το τηλέφωνό μου»** από την Google. Αν έχετε συνδέσει τον λογαριασμό σας Google (gmail) στο τηλέφωνό σας, πληκτρολογείστε στην Αναζήτηση Google και «Εύρεση του τηλεφώνου μου» (Find my phone). Πρώτα, θα πρέπει να επιτρέψετε στην Google να χρησιμοποιήσει τα δεδομένα τοποθεσίας σας, τις πληροφορίες της συσκευής και τα συμβάντα σύνδεσης για να εντοπίσετε τις συσκευές και τα αξεσουάρ σας. Η τοποθεσία της συσκευής μπορεί να μην είναι πάντα ακριβής, αλλά θα δείτε έναν χάρτη με την τρέχουσα θέση του τηλεφώνου σας. Θα είναι επίσης διαθέσιμα τα δεδομένα σχετικά με το επίπεδο φόρτισης και τη σύνδεση δικτύου κινητής τηλεφωνίας. Θα έχετε πολλές επιλογές:	

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή του παρόντος εγγράφου δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει μόνο τις απόψεις των δημιουργών, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.

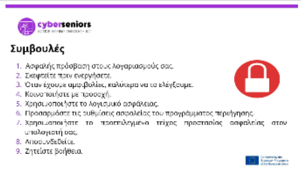
<table>
<tr>
<td></td>
<td>

Μπορείτε να ενεργοποιήσετε τον συναγερμό στο τηλέφωνό σας. Η συσκευή θα χτυπήσει για πέντε λεπτά ακόμα και αν το τηλέφωνο βρίσκεται σε αθόρυβη λειτουργία.
Μπορείτε να κλειδώσετε το τηλέφωνό σας και να αποσυνδεθείτε από τον Λογαριασμό σας Google. Μπορείτε επίσης να εμφανίσετε ένα μήνυμα κειμένου στην οθόνη του τηλεφώνου.
Μπορείτε να διαγράψετε τα δεδομένα της συσκευής επαναφέροντάς την στις εργοστασιακές ρυθμίσεις. Μετά από αυτό, δεν θα μπορείτε πλέον να παρακολουθείτε τη συσκευή σας.

</td>
<td></td>
</tr>
<tr>
<td></td>
<td>
9 συμβουλές για να είστε ασφαλείς στο διαδίκτυο

1) Ασφαλής πρόσβαση στους λογαριασμούς σας. Δεδομένου ότι οι κωδικοί πρόσβασης μπορούν να κλαπούν, η προσθήκη ελέγχου ταυτότητας δύο βημάτων σε λογαριασμούς παρέχει ένα δεύτερο επίπεδο προστασίας. Πολλές διαδικτυακές υπηρεσίες, συμπεριλαμβανομένων εφαρμογών και ιστότοπων, προσφέρουν δωρεάν επιλογές που θα μπορούσαν να σας βοηθήσουν να προστατεύσετε τις πληροφορίες σας και να διασφαλίσετε ότι εσείς είστε αυτό που στην πραγματικότητα προσπαθείτε να αποκτήσετε πρόσβαση στον λογαριασμό σας - όχι κάποιος που έχει τον κωδικό πρόσβασής σας.

2) Σκεφτείτε πριν ενεργήσετε. Τα μηνύματα ηλεκτρονικού ταχυδρομείου και η επικοινωνία που δημιουργούν μια αίσθηση επείγοντος, όπως ένα πρόβλημα με τον τραπεζικό λογαριασμό ή τους φόρους σας, είναι πιθανότατα απάτη. Εξετάστε το ενδεχόμενο να απευθύνετε απευθείας στην εταιρεία τηλεφωνικά για να προσδιορίσετε αν το μήνυμα ηλεκτρονικού ταχυδρομείου είναι γνήσιο ή όχι.

3) Όταν έχουμε αμφιβολίες, καλύτερα να το διαγράψουμε. Κάνοντας κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου είναι συχνά ο τρόπος με τον οποίο οι απατεώνες έχουν πρόσβαση σε προσωπικές πληροφορίες. Εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου φαίνεται ασυνήθιστο, ακόμα και αν γνωρίζετε το άτομο που το έστειλε, είναι καλύτερο να το διαγράψετε. Θυμηθείτε ότι οι απατεώνες μπορούν να συλλέξουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των φίλων σας και να σας στέλνουν μηνύματα που παριστάνουν αυτούς. Ενεργοποιήστε τα φίλτρα ανεπιθύμητης αλληλογραφίας για το λογαριασμό ηλεκτρονικού ταχυδρομείου σας για να φιλτράρετε ύποπτα μηνύματα.
</td>
<td>


</td>
</tr>
</table>

4) Κοινοποιήστε με προσοχή. Έχετε επίγνωση του τι κοινοποιείτε δημόσια σε ιστότοπους κοινωνικών μέσων όπως το Facebook. Προσαρμόστε τις ρυθμίσεις απορρήτου σας για να περιορίσετε ποιος μπορεί να δει τις πληροφορίες σας. Αποφύγετε την κοινή χρήση της τοποθεσίας σας.

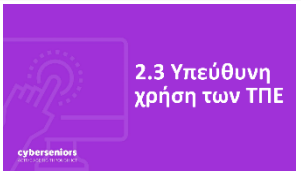
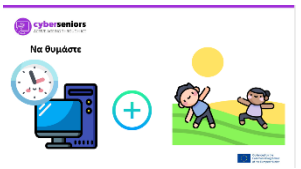
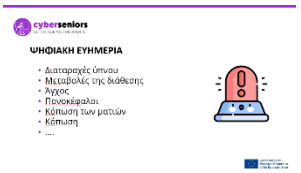
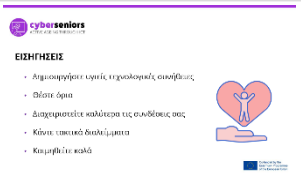
5) Χρησιμοποιήστε το λογισμικό ασφάλειας. Εγκαταστήστε λογισμικό ασφαλείας στις συσκευές σας από αξιόπιστη πηγή και διατηρήστε το ενημερωμένο. Είναι καλύτερο να εκτελείτε τακτικά το λογισμικό προστασίας από ιούς και λογισμικό προστασίας από λογισμικό υποκλοπής spyware. Να είστε προσεκτικοί με τις ενημερώσεις ασφαλείας από αναδυόμενες διαφημίσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου. Μπορεί στην πραγματικότητα να είναι κακόβουλο λογισμικό που θα μπορούσε να μολύνει τον υπολογιστή σας.

6) Προσαρμόστε τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησης. Πιθανότατα αναζητάτε ειδήσεις, πληροφορίες και προϊόντα χρησιμοποιώντας ένα πρόγραμμα περιήγησης στο Διαδίκτυο, όπως firefox, Google Chrome, Internet Explorer και Safari. Προσαρμόστε τις ρυθμίσεις σας σε καθένα από αυτά τα προγράμματα περιήγησης για να ορίσετε τις επιλογές σας για βέλτιστη ασφάλεια. Αυτά τα μενού μπορούν συχνά να βρεθούν στην επάνω δεξιά γωνία του προγράμματος περιήγησής σας. Εξετάστε το ενδεχόμενο να διαγράψετε το ιστορικό περιήγησής σας στο τέλος της περιόδου λειτουργίας σας, ώστε να μην αφήσετε ίχνη ευαίσθητων δεδομένων.

7) Χρησιμοποιήστε το προεπιλεγμένο τείχος προστασίας ασφαλείας στον υπολογιστή σας. Το λειτουργικό σας σύστημα (OS) πιθανότατα έχει προεπιλεγμένες ρυθμίσεις τείχους προστασίας που θα προστατεύουν τον υπολογιστή σας χωρίς να χρειάζονται ρύθμιση. Εάν το λογισμικό προστασίας από ιούς περιλαμβάνει πρόσθετη ασφάλεια τείχους προστασίας που μπορείτε να προσαρμόσετε ξεχωριστά, εξετάστε το ενδεχόμενο να επικοινωνήσετε με έναν τεχνικό Η/Υ για βοήθεια, για να διασφαλίσετε ότι είστε προστατευμένοι με ασφάλεια χωρίς να μπλοκάρετε υπερβολικά ιστότοπους και προγράμματα που χρησιμοποιείτε τακτικά.

8) Αποσυνδεθείτε. Θυμηθείτε να αποσυνδέεστε από εφαρμογές και ιστότοπους όταν ολοκληρώσετε τη χρήση τους. Αφήνοντάς τα ανοιχτά στην οθόνη του υπολογιστή σας θα μπορούσε να σας κάνει ευάλωτους σε κινδύνους ασφάλειας και προστασίας προσωπικών δεδομένων.

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή του παρόντος εγγράφου δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει μόνο τις απόψεις των δημιουργών, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.

	9) Εξετάστε το ενδεχόμενο υποστήριξης. Εάν ζείτε μόνοι ή περνάτε πολύ χρόνο μόνοι σας, σκεφτείτε μια αξιόπιστη πηγή για να χρησιμεύσει ως ένα δεύτερο σύνολο ματιών και αυτιών. Τα ενήλικα μέλη της οικογένειας και τα εγγόνια που είναι γνώστες των υπολογιστών μπορεί να είναι πρόθυμα να βοηθήσουν.	
5 λεπτά	**Ψηφιακή ευημερία** Είναι απαραίτητο να διατηρείται μια ψυχική και σωματική ισορροπία. Διαχειριστείτε τις αλληλεπιδράσεις σας με τα ψηφιακά εργαλεία Η ψηφιακή ευημερία επηρεάζει τη γενική μας ευημερία και το αντίστροφο. Η καλύτερη πρόταση είναι να βρούμε μια ισορροπία μεταξύ των δύο "κόσμων", ώστε να έχουμε τον καλύτερο εμπλουτισμό και τα θετικά οφέλη σε κάθε τομέα, μειώνοντας τους κινδύνους από την υπερβολική χρήση ψηφιακών εργαλείων που, όπως είδαμε, μπορούν να μας επηρεάσουν με διαφορετικούς τρόπους. Χρησιμοποιήστε την τεχνολογία για να αλληλεπιδράσετε με τον φυσικό κόσμο και τους άλλους ανθρώπους με ενεργό τρόπο.	 
	Αυτές είναι ορισμένες συνέπειες της κατάχρησης της τεχνολογίας: • Διαταραχές ύπνου • Μεταβολές της διάθεσης • Άγχος • Πονοκέφαλοι • Κόπωση των ματιών • Κόπωση	
	Εισηγήσεις για ψηφιακή ευημερία: • Δημιουργήστε υγιείς τεχνολογικές συνήθειες • Θέστε όρια • Διαχειριστείτε καλύτερα τις συνδέσεις σας • Κάντε τακτικά διαλείμματα • Κοιμηθείτε καλά	
5 λεπτά	**ΟΛΟΚΛΗΡΩΣΗ ΣΥΝΕΔΡΙΑΣ**	

	Θα αφήσουμε λίγο χρόνο πριν το τέλος της συνεδρίασης για να επιλύσουμε αμφιβολίες ή ανησυχίες σχετικά με το τι παρατηρήθηκε στη σημερινή συνεδρίαση, θα εκτιμήσουμε τη συμμετοχή τους και θα τους ενθαρρύνουμε να εξασκηθούν στο σπίτι, ώστε να μην ξεχάσουν αυτά που έμαθαν σήμερα.	

ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή του παρόντος εγγράφου δεν συνιστά έγκριση του περιεχομένου που αντικατοπτρίζει μόνο τις απόψεις των δημιουργών, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.