# MIG-DHL

Migrants Digital Health Literacy

# Εγχειρίδιο

## Θεματική Ενότητα 6

Δραστηριότητα στο ψηφιακό περιβάλλον υγείας


**Συγγραφείς:**

Josemar Alejandro Jimenez, Oxfam; Jenny Wielga, IAT



Με συγχρηματοδότηση από το πρόγραμμα «Erasmus+» της Ευρωπαϊκής Ένωσης

Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή της παρούσας έκδοσης, δεν συνιστά αποδοχή του περιεχομένου, το οποίο αντανακλά τις απόψεις μόνον των δημιουργών, και η Ευρωπαϊκή Επιτροπή δεν φέρει ουδεμία ευθύνη για οποιαδήποτε χρήση των πληροφοριών που εμπεριέχονται σε αυτό. Αριθμός προγράμματος: 2020-1-DE02-KA204-007679.

Με συγχρηματοδότηση από το πρόγραμμα «Erasmus+» της Ευρωπαϊκής Ένωσης

Αυτό το εγχειρίδιο για την θεματική ενότητα 6 αποτελεί μέρος του προγράμματος MIG-DHL το οποίο αποτελείται από 6 εκπαιδευτικές θεματικές ενότητες στο σύνολο, οι οποίες έχουν αναπτυχθεί στα πλαίσια της Στρατηγικής Σύμπραξης Erasmus+ **MIG-DHL- Migrants Digital Health Literacy.**

## Τα περιεχόμενα του εκπαιδευτικού προγράμματος:

**Το πρόγραμμα MIG-DHL**



Μπορείτε να βρείτε περισσότερες πληροφορίες στο: https://mig-dhl.eu/

Με συγχρηματοδότηση από
το πρόγραμμα «Erasmus+»
της Ευρωπαϊκής Ένωσης

MIG-DHL
Migrants Digital Health Literacy

## Δήλωση περί πνευματικών δικαιωμάτων:

Με συγχρηματοδότηση από
το πρόγραμμα «Erasmus+»
της Ευρωπαϊκής Ένωσης



# Περιεχόμενα

## Εισαγωγή

Το παρακάτω εγχειρίδιο έχει αναπτυχθεί στο πλαίσιο του IO2 του προγράμματος MIG-DHL. Αυτό το εγχειρίδιο καλύπτει τις έξι ενότητες που αναπτύχθηκαν κατά τη διάρκεια του προγράμματος MIG-DHL:

1.) Τι είναι ο ψηφιακός αλφαβητισμός για την υγεία και ποια η σημασία του;
2.) Κύρια προβλήματα υγείας κατά την άφιξη σε μία νέα χώρα
3.) Υπηρεσίες Υγειονομικής Περίθαλψης
4.) Γίνομαι ψηφιακά εγγράμματος
5.) Πλοήγηση στο Εθνικό Σύστημα Υγείας μέσω του Διαδικτύου
**6.) Δραστηριότητα στο ψηφιακό περιβάλλον υγείας**

Το εγχειρίδιο απευθύνεται ειδικά σε εκπαιδευτές και επαγγελματίες υποστήριξης (κοινωνικούς λειτουργούς, επαγγελματίες στο τομέα της υγείας κ.λ.π). Το εγχειρίδιο αποσκοπεί στη παροχή βαθύτερης κατανόησης σχετικά με τα θέματα που συζητούνται στις εκπαιδευτικές συνεδρίες, ώστε το περιεχόμενο του εκπαιδευτικού υλικού να γίνει πιο σαφές για τον εκπαιδευτή. Το εγχειρίδιο βοηθάει επίσης τους εκπαιδευτές να είναι πιο προετοιμασμένοι για να απαντήσουν σε ερωτήσεις καθώς το περιεχόμενό του είναι πιο λεπτομερές από τις πληροφορίες του εκπαιδευτικού υλικού. Επομένως, αυτό το εγχειρίδιο παρέχει πιο λεπτομερείς γνώσεις και συνδέσμους με πρόσθετους πόρους που σχετίζονται με το περιεχόμενο -κυρίως για τους εκπαιδευτές, αλλά και για άλλα άτομα που θα ήθελαν να μάθουν περισσότερα για τα θέματα που καλύπτονται στην εκπαίδευση που παρέχει το συγκεκριμένο πρόγραμμα.

Η δομή του εγχειριδίου συμβαδίζει με τη δομή του εκπαιδευτικού προγράμματος. Κάθε ενότητα καλύπτεται σε ένα κεφάλαιο περίπου 6 έως 8 σελίδων.

Το συγκεκριμένο εγχειρίδιο περιέχει πληροφορίες σχετικά με την Ενότητα 6 «Δραστηριότητα στο ψηφιακό περιβάλλον υγείας» που καλύπτουν τις απαραίτητες θεωρητικές πληροφορίες για την υποστήριξη του περιεχομένου και των δραστηριοτήτων του DPTA_6.

## 6. Πως να είσαι ενεργός στο ψηφιακό περιβάλλον

Για να είναι κανείς ενεργός στο ψηφιακό περιβάλλον, είναι πολύ σημαντικό να γνωρίζει πώς να προστατεύει το απόρρητό του για τη βελτίωση της προστασίας των προσωπικών δεδομένων στο ψηφιακό περιβάλλον.

Ως εκ τούτου, αυτή η ενότητα επικεντρώνεται στην ασφάλεια του απορρήτου και αποτελεί συνέχεια των θεμάτων που έχουν ήδη εξεταστεί στην ενότητα 4. Ειδικότερα σχετίζεται με την ανάπτυξη ικανοτήτων σε σχέση με την ασφάλεια και την προστασία του απορρήτου και πιο συγκεκριμένα με το πως μπορούμε να προστατεύουμε τις συσκευές μας, το περιεχόμενο, τα προσωπικά μας δεδομένα και την ιδιωτικότητά μας στο ψηφιακό περιβάλλον. Η δράση αυτή επιτρέπει επίσης την προστασία της σωματικής και ψυχικής υγείας, της ευημερίας και της κοινωνικής ένταξης. Αυτό το μέρος σχετίζεται με τον τομέα ικανοτήτων 4 "Ασφάλεια" του DigiComp, ο οποίος έχει ήδη αναφερθεί στην ενότητα 4.

### 6.1 Προστασία του απορρήτου και των προσωπικών δεδομένων στο ψηφιακό περιβάλλον

Στο ψηφιακό περιβάλλον υπάρχουν πολλοί κίνδυνοι που απειλούν την ασφάλεια του απορρήτου και των προσωπικών δεδομένων. Ορισμένοι από τους κυριότερους παράγοντες κινδύνου, οι οποίοι επισημαίνονται και στο εκπαιδευτικό υλικό, περιγράφονται λεπτομερέστερα στο επόμενο μέρος.

#### 6.1.1 Χάκινγκ (Hacking)

Το χάκινγκ αναφέρεται σε δραστηριότητες που αποσκοπούν στην παραβίαση ψηφιακών συσκευών, όπως υπολογιστές, smartphones, tablets, ακόμη και ολόκληρα δίκτυα. Και ενώ το χάκινγκ μπορεί να μην γίνεται πάντα για κακόβουλους σκοπούς, στις μέρες μας οι περισσότερες αναφορές στο χάκινγκ, και στους χάκερς, το/τους χαρακτηρίζουν ως παράνομη δραστηριότητα από εγκληματίες του κυβερνοχώρου με κίνητρο το οικονομικό κέρδος, τη διαμαρτυρία, τη συλλογή πληροφοριών (κατασκοπεία), ακόμα και γιατί αυτή πρόκληση τους φαίνεται διασκεδαστική.

Το χάκινγκ είναι συνήθως τεχνικής φύσης. Είναι πιθανό όμως οι χάκερς να χρησιμοποιήσουν την ψυχολογία για να εξαπατήσουν τον χρήστη ώστε να κάνει κλικ σε ένα κακόβουλο συνημμένο αρχείο ή να παράσχει προσωπικά δεδομένα.

Στην πραγματικότητα, είναι ακριβές να χαρακτηρίσουμε το χάκινγκ ως έναν γενικό όρο-ομπρέλα για τη δραστηριότητα που βρίσκεται πίσω από τα περισσότερα, αν όχι όλα, τα κακόβουλα λογισμικά και τις κακόβουλες κυβερνοεπιθέσεις στους χρήστες υπολογιστών, τις επιχειρήσεις και τις κυβερνήσεις. Οι συνήθεις τεχνικές που χρησιμοποιούν οι χάκερς περιλαμβάνουν:

- ρομποτικά δίκτυα (botnets)

- πειρατεία προγραμμάτων περιήγησης (hijacks)

- επιθέσεις άρνησης παροχής υπηρεσιών (DDoS)

- ιούς κρυπτογράφησης (Ransomware)

- rootkits

- trojans

- ιούς

- σκουλήκια υπολογιστών (computer worms)

Τύποι χάκινγκ/χάκερς

Σε γενικές γραμμές, μπορούμε να πούμε ότι οι χάκερς προσπαθούν να εισβάλουν σε υπολογιστές και δίκτυα για οποιονδήποτε από τους παρακάτω τέσσερις λόγους:

- Υπάρχει εγκληματικό οικονομικό όφελος, δηλαδή κλοπή αριθμών πιστωτικών καρτών ή εξαπάτηση τραπεζικών συστημάτων.

- Έπειτα, οι χάκερς μέσα σε αυτήν την υποκουλτούρα αποκτούν αξιοπιστία και βελτιώνουν τη φήμη τους κάτι που αποτελεί κίνητρο για άλλους, καθώς αφήνουν το σημάδι τους σε ιστοσελίδες ως απόδειξη ότι κατάφεραν να τις χακάρουν.

- Στη συνέχεια, υπάρχει η εταιρική κατασκοπεία, όταν οι χάκερς μιας εταιρείας επιδιώκουν να κλέψουν πληροφορίες σχετικά με τα προϊόντα και τις υπηρεσίες ενός ανταγωνιστή για να αποκτήσουν πλεονέκτημα στην αγορά.

Πώς να προστατευτείτε από τους χάκερς

- Προστασία κατά του κακόβουλου λογισμικού: Πρώτα απ' όλα, κατεβάστε ένα αξιόπιστο προϊόν κατά του κακόβουλου λογισμικού (ή εφαρμογή για το τηλέφωνο), το οποίο μπορεί τόσο να ανιχνεύσει και να εξουδετερώσει κακόβουλο λογισμικό όσο και να αποκλείσει συνδέσεις με κακόβουλους ιστότοπους ηλεκτρονικού ψαρέματος (phishing).

- Προσοχή στις εφαρμογές: Δεύτερον, κατεβάζετε εφαρμογές για τηλέφωνα μόνο από τις νόμιμες αγορές που ελέγχονται για εφαρμογές που φέρουν κακόβουλο λογισμικό, όπως το Google Play και το Amazon Appstore. (Σημειώστε ότι η πολιτική της Apple περιορίζει τους χρήστες iPhone να κάνουν λήψη μόνο από το App Store). Ακόμα κι έτσι, κάθε φορά που κατεβάζετε μια εφαρμογή, ελέγχετε πρώτα τις αξιολογήσεις και τις κριτικές. Εάν έχει χαμηλή βαθμολογία και μικρό αριθμό λήψεων, είναι καλύτερο να αποφύγετε τη συγκεκριμένη εφαρμογή.

- Προστατέψτε τις πληροφορίες σας: Να ξέρετε ότι καμία τράπεζα ή σύστημα ηλεκτρονικών πληρωμών δεν θα σας ζητήσει ποτέ τα στοιχεία σύνδεσης, τον αριθμό κοινωνικής ασφάλισης ή τους αριθμούς πιστωτικών καρτών σας μέσω ηλεκτρονικού ταχυδρομείου.

- Ενημερώστε το λογισμικό σας: Είτε χρησιμοποιείτε το τηλέφωνό σας είτε έναν υπολογιστή, βεβαιωθείτε ότι το λειτουργικό σας σύστημα παραμένει ενημερωμένο.

- Περιηγηθείτε προσεκτικά: Αποφύγετε να επισκέπτεστε μη ασφαλείς ιστοσελίδες και μην κατεβάζετε ποτέ μη επαληθευμένα συνημμένα αρχεία ή μην κάνετε κλικ σε συνδέσμους σε άγνωστα μηνύματα ηλεκτρονικού ταχυδρομείου.

- Ασφάλεια κωδικών πρόσβασης: Αν ένας χάκερ ανακαλύψει έναν από τους κωδικούς πρόσβασης που χρησιμοποιείτε για πολλές υπηρεσίες, διαθέτει εφαρμογές που μπορούν να παραβιάσουν τους άλλους λογαριασμούς σας. Γι' αυτό, κάντε τους κωδικούς σας μεγάλους και περίπλοκους, αποφύγετε να χρησιμοποιείτε τον ίδιο κωδικό για διαφορετικούς λογαριασμούς, και αντ' αυτού χρησιμοποιήστε έναν διαχειριστή κωδικών πρόσβασης. Διότι η παραβίαση ακόμη και ενός μόνου λογαριασμού ηλεκτρονικού ταχυδρομείου μπορεί να είναι ιδιαίτερα επιζήμια. (Malwarebytes, 2020).

### 6.1.2 Ιοί υπολογιστών

Ο ιός του υπολογιστή είναι μια από τις πιο συνηθισμένες μορφές πειρατείας. Παρόμοια με τον ιό της γρίπης, έχει σχεδιαστεί για να εξαπλώνεται από υπολογιστή σε υπολογιστή και έχει την ικανότητα να αναπαράγεται. Ομοίως, με τον ίδιο τρόπο που οι ιοί της γρίπης δεν μπορούν να αναπαραχθούν χωρίς κύτταρο ξενιστή, οι ιοί υπολογιστών δεν μπορούν να αναπαραχθούν και να εξαπλωθούν χωρίς προγραμματισμό, όπως ένα αρχείο ή ένα έγγραφο. Με πιο τεχνικούς όρους, ένας ιός υπολογιστών είναι ένας τύπος κακόβουλου κώδικα ή προγράμματος που έχει γραφτεί για να μεταβάλλει τον τρόπο λειτουργίας ενός υπολογιστή και έχει σχεδιαστεί για να εξαπλώνεται από τον έναν υπολογιστή στον άλλο. Ένας ιός εισάγεται ή εισέρχεται σε ένα νόμιμο πρόγραμμα ή έγγραφο που υποστηρίζει μακροεντολές προκειμένου να εκτελέσει τον κώδικά του. Κατά τη διαδικασία αυτή, ένας ιός έχει τη δυνατότητα να προκαλέσει απροσδόκητα ή επιζήμια αποτελέσματα, όπως να βλάψει το λογισμικό του συστήματος αλλοιώνοντας ή καταστρέφοντας δεδομένα.

Πώς επιτίθεται ένας ιός υπολογιστή; Μόλις ένας ιός συνδεθεί επιτυχώς σε ένα πρόγραμμα, αρχείο ή έγγραφο, ο ιός θα παραμείνει σε αδράνεια μέχρι οι συνθήκες να αναγκάσουν τον υπολογιστή ή τη συσκευή να εκτελέσει τον κώδικά του. Για να μολύνει ένας ιός τον υπολογιστή σας, πρέπει να εκτελέσετε το μολυσμένο πρόγραμμα, το οποίο με τη σειρά του προκαλεί την εκτέλεση του κώδικα του ιού. Αυτό σημαίνει ότι ένας ιός μπορεί να παραμείνει αδρανής στον υπολογιστή σας, χωρίς να εμφανίσει σημαντικά συμπτώματα. Ωστόσο, μόλις ο ιός μολύνει τον υπολογιστή σας, ο ιός μπορεί να μολύνει και άλλους υπολογιστές στο ίδιο δίκτυο. Η κλοπή κωδικών πρόσβασης ή δεδομένων, η καταγραφή πληκτρολογήσεων, η αλλοίωση αρχείων, η αποστολή spam στις επαφές ηλεκτρονικού ταχυδρομείου σας, ακόμη και η κατάληψη του υπολογιστή σας είναι μερικά μόνο από τα καταστροφικά και ενοχλητικά πράγματα που μπορεί να κάνει ένας ιός. Ενώ ορισμένοι ιοί μπορεί να μην προκαλέσουν κάποια βλάβη, άλλοι μπορεί να έχουν βαθιά και επιζήμια αποτελέσματα. Αυτό περιλαμβάνει τη διαγραφή δεδομένων ή την πρόκληση μόνιμης βλάβης στον σκληρό σας δίσκο. Ειδικά όταν, ορισμένοι ιοί έχουν σχεδιαστεί με σκοπό το οικονομικό κέρδος.

Πώς εξαπλώνονται οι ιοί υπολογιστών; Σε έναν ψηφιακό κόσμο, ο υπολογιστής μπορεί να προσβληθεί από ιό με πολλούς τρόπους, μερικοί πιο προφανείς από άλλους. Οι ιοί

μπορούν να εξαπλωθούν μέσω συνημμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου και γραπτών μηνυμάτων, λήψεων αρχείων από το Διαδίκτυο και συνδέσμων απάτης στα μέσα κοινωνικής δικτύωσης. Οι φορητές συσκευές και τα smartphones σας μπορούν να μολυνθούν με ιούς για κινητά μέσω ύποπτων λήψεων εφαρμογών. Οι ιοί μπορούν να κρύβονται μέσα σε συνημμένα κοινωνικά διαμοιραζόμενου περιεχομένου, όπως αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο. Για να αποφύγετε την επαφή με έναν ιό, είναι σημαντικό να είστε προσεκτικοί όταν σερφάρετε στον ιστό, κατεβάζετε αρχεία και ανοίγετε συνδέσμους ή συνημμένα αρχεία. Για να παραμείνετε ασφαλείς, μην κατεβάζετε ποτέ συνημμένα αρχεία κειμένου ή ηλεκτρονικού ταχυδρομείου που δεν περιμένετε ή αρχεία από ιστότοπους που δεν εμπιστεύεστε.

Ποια είναι τα σημάδια ενός ιού υπολογιστή; Μια επίθεση από ιό υπολογιστή μπορεί να προκαλέσει διάφορα συμπτώματα. Ακολουθούν ορισμένα από αυτά:

- Συχνά αναδυόμενα παράθυρα. Τα αναδυόμενα παράθυρα μπορεί να σας ενθαρρύνουν να επισκεφθείτε ασυνήθιστες ιστοσελίδες. Ή μπορεί να σας προτρέπουν να κατεβάσετε προγράμματα προστασίας από ιούς ή άλλα προγράμματα λογισμικού.

- Αλλαγές στην αρχική σας σελίδα. Η συνήθης αρχική σας σελίδα μπορεί για παράδειγμα να αλλάξει σε μα άλλη ιστοσελίδα, ενώ ενδέχεται να μην μπορείτε να την επαναφέρετε.

- Μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από το λογαριασμό του ηλεκτρονικού ταχυδρομείου σας. Ένας χάκερ μπορεί να πάρει τον έλεγχο του λογαριασμού σας ή να στείλει μηνύματα ηλεκτρονικού ταχυδρομείου στο όνομά σας από άλλον μολυσμένο υπολογιστή.

- Συχνές ζημιές. Ένας ιός μπορεί να προκαλέσει μεγάλη ζημιά στον σκληρό σας δίσκο. Αυτό μπορεί να προκαλέσει το ανεπανόρθωτη ζημιά στη συσκευή σας. Μπορεί επίσης να εμποδίσει τη συσκευή σας να επανέλθει σε λειτουργία.

- Ασυνήθιστα αργή απόδοση του υπολογιστή. Μια ξαφνική αλλαγή της ταχύτητας επεξεργασίας μπορεί να σηματοδοτεί ότι ο υπολογιστής σας έχει ιό.

- Άγνωστα προγράμματα που ξεκινούν όταν ενεργοποιείτε τον υπολογιστή σας. Μπορεί να αντιληφθείτε ένα άγνωστο πρόγραμμα όταν εκκινήσετε τον υπολογιστή σας ή μπορεί να το παρατηρήσετε ελέγχοντας τη λίστα ενεργών εφαρμογών του υπολογιστή σας.

- Ασυνήθιστες δραστηριότητες όπως η αλλαγή κωδικού πρόσβασης. Αυτό θα μπορούσε να σας εμποδίσει να συνδεθείτε στον υπολογιστή σας.

Ακολουθούν μερικά από τα πράγματα που μπορείτε να κάνετε για να βοηθήσετε στην ασφάλεια του υπολογιστή σας και να προστατευτείτε από τους ιούς:

-Χρησιμοποιήστε ένα αξιόπιστο προϊόν προστασίας από ιούς και διατηρήστε το ενημερωμένο.

-Αποφύγετε να κάνετε κλικ σε οποιεσδήποτε αναδυόμενες διαφημίσεις.

-Να σαρώνετε πάντα τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου πριν τα ανοίξετε.

- Να σαρώνετε πάντα τα αρχεία που κατεβάζετε χρησιμοποιώντας προγράμματα ανταλλαγής αρχείων (Norton, 2020).

### 6.1.3 Κλοπή δεδομένων

(περιλαμβάνει: πληροφορίες λογαριασμού πιστωτικής κάρτας, διαπιστευτήρια πελατών)

Η κλοπή δεδομένων είναι η πράξη κλοπής ψηφιακών πληροφοριών που είναι αποθηκευμένες σε υπολογιστές, διακομιστές ή ηλεκτρονικές συσκευές ενός άγνωστου θύματος με σκοπό την παραβίαση της ιδιωτικής ζωής ή την απόκτηση εμπιστευτικών πληροφοριών. Οι πληροφορίες μπορεί να περιλαμβάνουν οτιδήποτε, από οικονομικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών ή τραπεζικούς λογαριασμούς, μέχρι προσωπικές πληροφορίες, όπως αριθμούς κοινωνικής ασφάλισης, αριθμούς αδειών οδήγησης και αρχεία υγείας.

Πώς συμβαίνει η κλοπή δεδομένων; Η κλοπή δεδομένων συμβαίνει με διάφορους τρόπους. Τις περισσότερες φορές, συμβαίνει επειδή κάποιος εισέβαλε σε ένα σύστημα υπολογιστή για να κλέψει ευαίσθητες πληροφορίες, όπως οι πιστωτικές σας κάρτες ή τα προσωπικά σας

στοιχεία, ή επειδή ένας υπάλληλος μιας εταιρείας χειρίστηκε λανθασμένα τις πληροφορίες. Σε έναν ολοένα και πιο ψηφιακό κόσμο, εκατοντάδες διαφορετικές επιχειρήσεις και οργανισμοί κατέχουν τις προσωπικές σας πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης, την ταχυδρομική σας διεύθυνση, την ημερομηνία γέννησης και τα στοιχεία του τραπεζικού σας λογαριασμού.

Πώς να προστατευτείτε; Η κλοπή δεδομένων είναι ένα πραγματικό πρόβλημα και μπορεί να συμβεί σε οποιονδήποτε. Παρόλο που δεν υπάρχει τρόπος να αποτρέψετε εντελώς την κλοπή δεδομένων, υπάρχουν πολλές προφυλάξεις που μπορείτε να λάβετε για να περιορίσετε τον κίνδυνο που διατρέχετε.

- Πληρώστε με μετρητά αντί για πιστωτικές ή χρεωστικές κάρτες.

- Χρησιμοποιήστε πιστωτική ή χρεωστική κάρτα με τεχνολογία pin-and-chip.

- Προστατέψτε τον υπολογιστή σας από ιούς και κακόβουλο λογισμικό εγκαθιστώντας, χρησιμοποιώντας και ενημερώνοντας λογισμικό προστασίας από ιούς και λογισμικό κατά της κατασκοπείας σε όλους τους υπολογιστές και τις ηλεκτρονικές σας συσκευές.

- Διατηρείτε όλα τα λειτουργικά συστήματα και τα προγράμματα λογισμικού ενημερωμένα, εγκαθιστώντας τακτικά ενημερώσεις για την ασφάλεια, τα προγράμματα περιήγησης στο διαδίκτυο, τα λειτουργικά συστήματα και τα προγράμματα λογισμικού αμέσως μόλις γίνουν διαθέσιμες.

- Μην ανοίγετε μη αξιόπιστα μηνύματα ηλεκτρονικού ταχυδρομείου ή συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου, καθώς μπορεί να είναι μηνύματα ηλεκτρονικού ψαρέματος.

- Ελέγχετε τακτικά τις καταστάσεις της πιστωτικής σας κάρτας και την πιστωτική σας αναφορά για μη εξουσιοδοτημένες χρεώσεις και νέες πιστωτικές γραμμές.

- Χρησιμοποιείτε έναν ισχυρό, μοναδικό κωδικό πρόσβασης για όλους τους ιστότοπους που απαιτούν σύνδεση και να τους αλλάζετε τακτικά, ειδικά εάν ο κωδικός πρόσβασης ενός λογαριασμού έχει παραβιαστεί.

- Χρησιμοποιείτε μόνο ασφαλείς συνδέσεις Wi-Fi.

- Απορρίψτε σωστά τα έγγραφα που περιέχουν ευαίσθητες πληροφορίες καταστρέφοντάς το και αφαιρώντας όλα τα δεδομένα από τις ηλεκτρονικές συσκευές (Michaud, 2021).

### 6.1.4 Ανεπιθύμητα μηνύματα (Spam-mails)

Ορισμένες φορές λαμβάνετε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου - από τη μία, αυτό είναι χρονοβόρο επειδή πρέπει να ταξινομήσετε τα ανεπιθύμητα μηνύματα, αλλά από την άλλη, τα λεγόμενα μηνύματα spam μπορεί επίσης να περιέχουν κινδύνους όπως ιούς ή επιβλαβή προγράμματα που εγκαθίστανται στον υπολογιστή σας όταν ανοίγετε το μήνυμα και μπορούν π.χ. να κατασκοπεύσουν τα δεδομένα πρόσβασής σας. Το "ψάρεμα" είναι επίσης ένας συνηθισμένος τύπος διαδικτυακής απάτης, όπου οι εγκληματίες στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου που μοιάζουν με επίσημα μηνύματα με σκοπό να αποκαλύψουν στον χρήστη στοιχεία που μπορούν να χρησιμοποιηθούν για κλοπή ταυτότητας.

- Τι προτείνεται να κάνετε:
  - ✓ αποφεύγετε να ανοίγετε συνημμένα μηνύματα, εκτός αν έχουν περάσει από πρόγραμμα προστασίας από ιούς,
  - ✓ να θυμάστε να αποσυνδέεστε, ιδίως όταν χρησιμοποιείτε κοινόχρηστο δημόσιο υπολογιστή,
  - ✓ διαγράψτε όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστα πρόσωπα,
  - ✓ μην απαντάτε ποτέ σε ανεπιθύμητα μηνύματα.
- Πώς να αναγνωρίζετε τα μηνύματα spam;
  - ✓ Γραμματικά και ορθογραφικά λάθη
  - ✓ Μηνύματα σε ξένη γλώσσα
  - ✓ Λείπει το όνομα
  - ✓ Επείγουσα ανάγκη για δράση - ειδικά σε συνδυασμό με απειλή
  - ✓ Αίτημα εισαγωγής προσωπικών δεδομένων (π.χ. PIN ή TAN)
  - ✓ Αίτημα ανοίγματος αρχείου
  - ✓ Δεν έχετε λάβει ποτέ μηνύματα ηλεκτρονικού ταχυδρομείου από την τράπεζα ή δεν είναι πελάτης μέχρι στιγμής (Verbraucherzentrale, 2021).

**Βιβλιογραφία**

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. doi:10.2760/38842

Michaud, Katelyn. (2021). *What is Data Theft?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Google Search Operators.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Essential Skills for Consumer Health in a Networked World. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *What is a computer virus?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Hacking definition: What is hacking?* https://www.malwarebytes.com/hacker

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet*. https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

World Health Organization [WHO]. 2017. *Digital Health Literacy*. https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf