



ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ

ΕΝΟΤΗΤΑ 2

Άσκηση 1

Παίξτε & μάθετε με κουίζ

Εκτιμώμενη διάρκεια

10 λεπτά

Υλικό

Συσκευή με πρόσβαση στο Διαδίκτυο για την
αποσαφήνιση αμφιβολιών
Χαρτί και στυλό

Οδηγίες

Στην επόμενη σελίδα έχετε 5 ερωτήσεις κουίζ
σχετικά με την ασφάλεια στο διαδίκτυο!

Βάλτε σε κύκλο τις ερωτήσεις και βρείτε τις
απαντήσεις με επεξηγήσεις στην 3η σελίδα - όχι
κρυφοκοιτάγματα!



1. Ποια είναι η συνηθέστερη μέθοδος μεταφοράς ιών;

- A. Ηλεκτρονικό ταχυδρομείο
- B. Άμεσο μήνυμα
- Γ. Λήψη από το Διαδίκτυο
- Δ. Φορητά μέσα

2. Ποιο από τα παρακάτω θα ήταν ο καλύτερος κωδικός πρόσβασης;

- A. MySecret
- B. lw2c^tILV
- Γ. Abc123
- Δ. George1234

3. Η αδελφή σας σας στέλνει ένα e-mail στη δουλειά με μια προφύλαξη οθόνης που λέει ότι θα σας άρεσε πολύ. Τι πρέπει να κάνετε;

- A. Να την κατεβάσετε στον υπολογιστή σας, αφού προέρχεται από αξιόπιστη πηγή.
- B. Προωθήστε το μήνυμα σε άλλους φίλους για να το μοιραστείτε.
- Γ. Καλέστε το τμήμα πληροφορικής και ζητήστε τους να σας βοηθήσουν να το εγκαταστήσετε.
- Δ. Διαγράψτε το μήνυμα.

4. Όταν λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια άγνωστη επαφή που περιέχει συνημμένο αρχείο, θα πρέπει:

- A. Να ανοίξετε το συνημμένο για να δείτε το περιεχόμενό του
- B. Να διαγράψετε το email
- Γ. Προωθήστε το μήνυμα ηλεκτρονικού ταχυδρομείου στους συναδέλφους σας για να τους επιτρέψετε να ανοίξουν πρώτα το συνημμένο
- Δ. Προωθήστε το μήνυμα ηλεκτρονικού ταχυδρομείου στον προσωπικό σας λογαριασμό ηλεκτρονικού ταχυδρομείου ώστε να μπορείτε να το ανοίξετε στο σπίτι



1. Ποια είναι η πιο συνηθισμένη μέθοδος μεταφοράς ιών;

A. Ηλεκτρονικό ταχυδρομείο

Το ηλεκτρονικό ταχυδρομείο είναι η πιο κοινή μέθοδος παράδοσης ιών. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν συχνά το ηλεκτρονικό ταχυδρομείο ως φορέα για τη διανομή κακόβουλου λογισμικού. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να φαίνονται ότι προέρχονται από αξιόπιστες πηγές, γεγονός που τα καθιστά ιδιαίτερα επικίνδυνα. Μόλις ο παραλήπτης ανοίξει το συνημμένο αρχείο ή κάνει κλικ στο σύνδεσμο, ο ιός μπορεί να μεταφορτωθεί και να εκτελεστεί στη συσκευή του.

2. Ποιο από τα παρακάτω θα ήταν ο καλύτερος κωδικός πρόσβασης;

B. lw2c^tILV

Επειδή ακολουθεί τις βασικές αρχές για τη δημιουργία ενός ισχυρού κωδικού πρόσβασης: **Πολυπλοκότητα:** Περιλαμβάνει ένα μείγμα από κεφαλαία γράμματα, πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες, καθιστώντας δύσκολο για τους επιτιθέμενους να το μαντέψουν ή να το σπάσουν με ωμή βία. **Μήκος:** Είναι επαρκώς μεγάλο, γεγονός που προσθέτει ένα ακόμη επίπεδο ασφάλειας. Οι μεγαλύτεροι κωδικοί πρόσβασης είναι γενικά πιο δύσκολο να παραβιαστούν. **Μη προβλεψιμότητα:** Ο κωδικός πρόσβασης δεν περιλαμβάνει εύκολα μαντεύσιμες λέξεις ή μοτίβα, τα οποία είναι είτε κοινά, είτε απλά, είτε σχετίζονται με τον χρήστη.

3. Η αδελφή σας σας στέλνει ένα e-mail στη δουλειά με μια προφύλαξη οθόνης.

Δ. Διαγράψτε το μήνυμα.

4 μεγάλοι κίνδυνοι:

1. Ορισμένες προφυλάξεις οθόνης περιέχουν ιούς.
2. Κάνοντας κλικ σε έναν κακόβουλο σύνδεσμο μπορεί να μολυνθεί ο υπολογιστής.
3. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου μπορεί να είναι πλαστές, οπότε επειδή το μήνυμα ηλεκτρονικού ταχυδρομείου λέει ότι προέρχεται από κάποιον γνωστό σας, δεν μπορείτε να είστε σίγουροι γι' αυτό χωρίς να το ελέγξετε.
4. Ορισμένοι ιστότοποι και σύνδεσμοι φαίνονται νόμιμοι, αλλά στην πραγματικότητα είναι φάρσες που έχουν σχεδιαστεί για να κλέψουν τις πληροφορίες σας.



ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ

ΕΝΟΤΗΤΑ 2

Άσκηση 2

Είναι ασφαλής η επίσκεψη του συνδέσμου;

Εκτιμώμενη διάρκεια

10 λεπτά

Υλικό

Συσκευή με πρόσβαση στο Διαδίκτυο για την
αποσαφήνιση αμφιβολιών
Χαρτί και στυλό

Οδηγίες

Διαβάστε το κείμενο
Σκεφτείτε

Θα περάσουμε μαζί από την άσκηση για να
καταλάβουμε γιατί ο σύνδεσμος είναι ασφαλής ή
όχι.



1. Αποφασίστε, αν ο σύνδεσμος είναι ασφαλής για να τον επισκεφθείτε:

Ας υποθέσουμε ότι λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια τράπεζα που σας ζητά να κάνετε κλικ σε έναν σύνδεσμο όπως ο παρακάτω και να υποβάλετε προσωπικά δεδομένα, όπως όνομα χρήστη, κωδικούς πρόσβασης και στοιχεία πιστωτικής κάρτας.

<http://url5423.eka.de/ls/click?>

[upn=V1OaWNMSPs2Lb0JqHpnYTLRIk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSIC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asDvdva](http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnYTLRIk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSIC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asDvdva)

Μη βιάζεστε, σκεφτείτε το καλά και αποφασίστε αν ο σύνδεσμος αυτός είναι ασφαλής για να τον επισκεφθείτε.

Η απάντηση.

Αυτός ο σύνδεσμος δεν είναι ασφαλής για διάφορους λόγους:

- Χρησιμοποιεί http αντί για https.
- Το όνομα τομέα δεν σχετίζεται με την επίσημη ονομασία της τράπεζας.
- Ο σύνδεσμος είναι ύποπτα μακρύς.
- Το όνομα τομέα του συνδέσμου είναι διαφορετικό από το όνομα τομέα της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα.
- Μια πραγματική τράπεζα δεν θα ζητήσει ποτέ ονόματα χρηστών, κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών.



ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ

ΕΝΟΤΗΤΑ 2

Άσκηση 3

Η βαθμολογία της διαδικτυακής σας ασφάλειας

Εκτιμώμενη διάρκεια

10 λεπτά

Υλικό

Η συσκευή με πρόσβαση στο Διαδίκτυο περνάει από
ένα online τεστ.

Στυλό για το off-line τεστ.

Οδηγίες

Το τεστ μπορεί να διεξαχθεί ατομικά ή σε ομάδα ατόμων. Μπορεί να χρησιμοποιηθεί ως διαδικτυακό τεστ ή με χαρτί και στυλό. Οι απαντήσεις είναι ΝΑΙ και ΟΧΙ.

Το διαδικτυακό τεστ θα σας προετοιμάσει σκορ ασφαλείας ή ο μέντοράς σας μπορεί να προετοιμάσει και να εξηγήσει τα αποτελέσματα.



Απαντήστε με ΝΑΙ ή ΟΧΙ

1. Χρησιμοποιείτε έλεγχο ταυτότητας δύο παραγόντων στις συσκευές σας; Για παράδειγμα, τόσο τον έλεγχο ταυτότητας με δακτυλικό αποτύπωμα όσο και έναν κωδικό πρόσβασης.
2. Χρησιμοποιείτε θησαυροφυλάκιο κωδικών πρόσβασης; Εδώ αποθηκεύονται με ασφάλεια όλοι οι κωδικοί πρόσβασης για πολλούς λογαριασμούς σας.
3. Χρησιμοποιείτε ιδιωτική περιήγηση όταν βρίσκεστε στο διαδίκτυο;
4. Ρυθμίζετε την προβολή όλων των μέσων κοινωνικής δικτύωσης σε ιδιωτική;
5. Δημοσιεύετε τακτικά φωτογραφίες στα μέσα κοινωνικής δικτύωσης που μοιράζονται την τοποθεσία σας;
6. Ελέγχετε τακτικά τις τραπεζικές σας συναλλαγές για να βεβαιωθείτε ότι δεν υπάρχουν έξοδα που αγνοείτε;
7. Πριν εισαγάγετε τα στοιχεία της πιστωτικής σας κάρτας όταν κάνετε ηλεκτρονικές αγορές, βεβαιώνετε ότι υπάρχει ένδειξη λουκέτου ή απόδειξη ότι ο ιστότοπος που επισκέπτεστε είναι ασφαλής;
8. Έχετε εγκαταστήσει λογισμικό ασφαλείας στον υπολογιστή σας, όπως λογισμικό κατά των ιών, κατά του spyware ή τείχος προστασίας;
9. Εάν ο υπολογιστής σας σας ζητήσει να ενημερώσετε το λογισμικό, θα το κάνετε αμέσως;
10. Χρησιμοποιείτε διαφορετικό κωδικό πρόσβασης για κάθε λογαριασμό στον οποίο έχετε σύνδεση;

Συγχαρητήρια!

Η βαθμολογία σας για την ασφάλεια στο διαδίκτυο είναι ***** _____ *****

Ασφάλεια σούπερ σταρ!