

## ΘΕΜΑ 4

**4.1.** Ένα τείχος προστασίας είναι ένα σύστημα ασφαλείας που προστατεύει ένα δίκτυο υπολογιστών ή έναν μεμονωμένο υπολογιστή από ανεπιθύμητη πρόσβαση.

Αυτό το πετυχαίνει παρακολουθώντας την κίνηση των δεδομένων στο δίκτυο ενώ χρησιμοποιεί καθορισμένους κανόνες για να απαγορεύσει οποιαδήποτε είσοδο δεν έχει έγκριση.

**4.2.** Το *προσωπικό τείχος προστασίας* είναι ένα λογισμικό εγκατεστημένο στον υπολογιστή και σκοπό έχει την προστασία του από μια εξουσιοδοτημένη εξωτερική πρόσβαση σε αυτόν. Αντίθετα το *εξωτερικό τείχος προστασίας* λειτουργεί σε μια εξωτερική συσκευή που βρίσκεται στο δίκτυο (όπως λ.χ. σε ένα δρομολογητή ή σε μια άλλη συσκευή όπως το DMZ (demilitarized zone)) [1]

**4.3.** Ο Μάριος **δεν πρέπει να απαντήσει** στο μήνυμα που δέχθηκε ούτε και να καταχωρήσει τα στοιχεία του και την πιστωτική του κάρτα στην φόρμα στο διαδίκτυο που το μήνυμα τον παραπέμπει. Προφανώς πρόκειται για μια περίπτωση phishing [2]. Δηλαδή προσπάθεια υποκλοπής προσωπικών δεδομένων μέσω μηνύματος.

Το firewall **δεν μπορεί να προστατέψει** στο να μην δεχθεί ο Μάριος τέτοια μηνύματα, τα οποία αποτελούν και αρκετά συχνό φαινόμενο σήμερα.

Το firewall θα μπορούσε ίσως να παίξει κάποιο ρόλο προστασίας, μόνο αν αναγνώριζε την ιστοσελίδα που παραπέμπει το μήνυμα ως υψηλού κινδύνου (High-risk web pages and urls). [3]  
Στην περίπτωση αυτή θα τον ειδοποιούσε όταν επισκεπτόταν τον συγκεκριμένο ιστότοπο με ανάλογο μήνυμα.

[1] <https://securemynetwork.wordpress.com/2013/07/19/τι-είναι-to-dmz/> accessed 15/3/22

[2] <https://el.safetynetdetectives.com/blog/τι-είναι-to-phishing-απλός-οδηγός-με-παραδείγ/#how-accessed> accessed 15/2/22

[3] <https://www.paloguard.com/URL-Filtering.asp> accessed 15/2/22

Σημ. Οι ιστότοποι υψηλού κινδύνου περιλαμβάνουν:

*Ιστότοπους που είχαν προηγουμένως επιβεβαιωθεί ότι είναι ιστότοποι κακόβουλου λογισμικού ή που σχετίζονται με επιβεβαιωμένη κακόβουλη δραστηριότητα κλπ.*