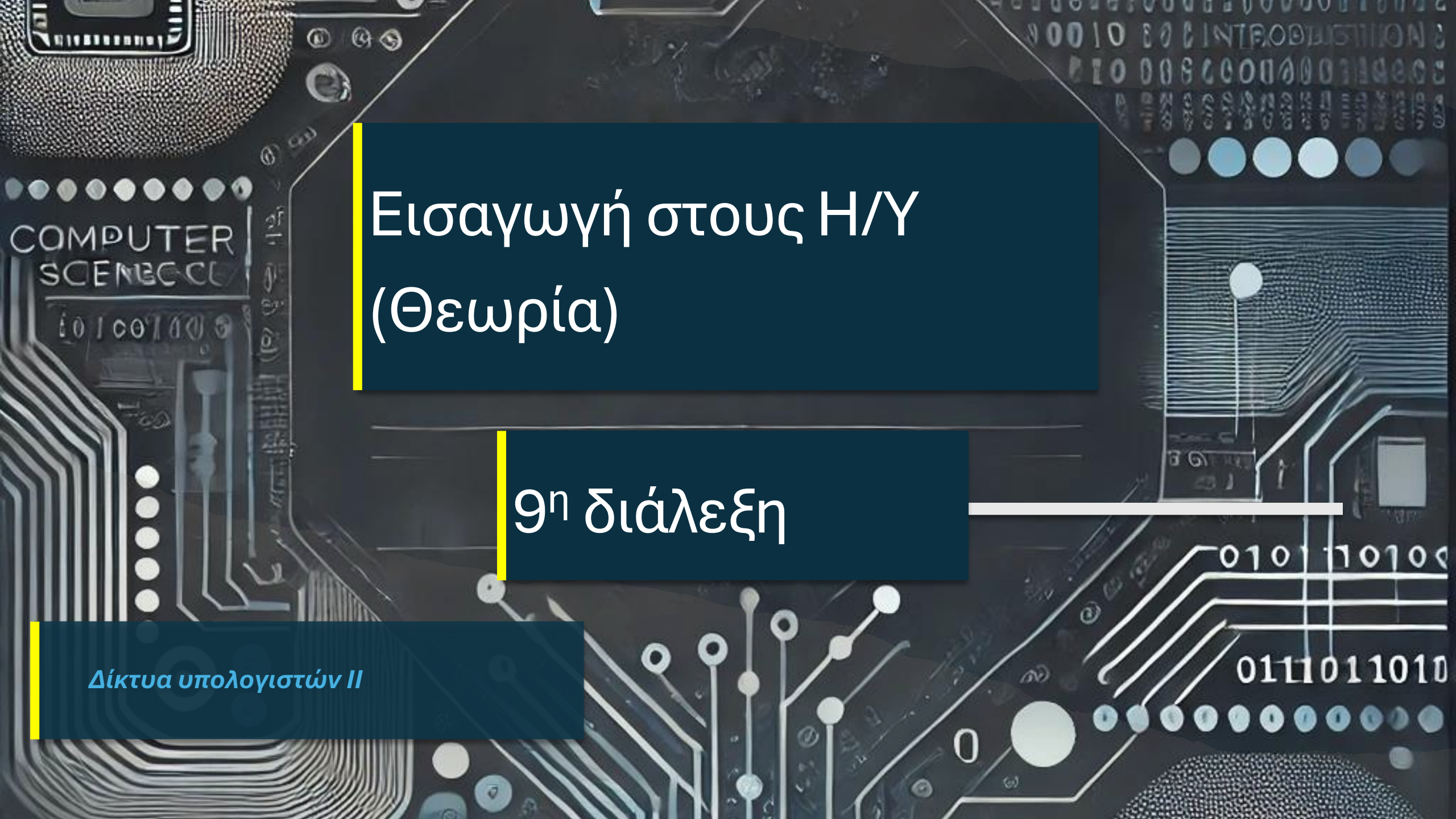



# Εισαγωγή στους Η/Υ (Θεωρία)

## 9η διάλεξη

*Δίκτυα υπολογιστών II*

# Συμμετρική Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση αποτελεί μια βασική τεχνολογία για την ασφάλεια των δεδομένων, τόσο στις επικοινωνίες όσο και στην αποθήκευσή του.

Διασφαλίζει (κατά το δυνατόν) ότι τα δεδομένα που ανταλλάσσονται μεταξύ αποστολέα και παραλήπτη (ή τα αποθηκευμένα) παραμένουν εμπιστευτικά και προστατευμένα από μη εξουσιοδοτημένη πρόσβαση.

Βασίζεται στη χρήση μαθηματικών αλγορίθμων που μετατρέπουν το αρχικό μήνυμα (plaintext) σε μια κρυπτογραφημένη μορφή (ciphertext), η οποία είναι ακατανόητη χωρίς το σωστό **κλειδί** αποκρυπτογράφησης. Υπάρχουν δύο κύριοι τύποι κρυπτογράφησης: η συμμετρική και η ασύμμετρη.

Στη **συμμετρική** κρυπτογράφηση, χρησιμοποιείται **το ίδιο κλειδί** τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων, κάτι που την καθιστά γρήγορη αλλά απαιτεί ασφαλή μέθοδο ανταλλαγής του κλειδιού. Δηλαδή – όπως συμβαίνει και στον φυσικό κόσμο – το ίδιο κλειδί κλειδώνει και ξεκλειδώνει τα δεδομένα.

Πχ έχω έναν ακέραιο αριθμό (το κλειδί) με τον οποίο κάνω XOR τα δεδομένα μου πχ κείμενο και προκύπτει ένα νέο σύνολο δεομένων (ciphertext). Με τον ίδιο αριθμό (κλειδί) κάνοντας XOR το ciphertext παίρνω το αρχικό κείμενο, αφού:

$$\underbrace{(\text{data XOR key})}_{\text{Κρυπτογραφημένα Δεδομένα}} \text{ XOR key} = \text{data}$$

# Ασύμμετρη Κρυπτογράφηση δεδομένων

Στην **ασύμμετρη** κρυπτογράφηση, χρησιμοποιείται **ένα ζεύγος κλειδιών**, το **δημόσιο** και το **ιδιωτικό**. Όπου το ένα κλειδί κρυπτογραφεί το μήνυμα και μόνο το αντίστοιχο (άλλο) μπορεί να το αποκρυπτογραφήσει, εξαλείφοντας την ανάγκη κοινής ανταλλαγής κλειδιών.

Στην ασύμμετρη κρυπτογράφηση τα δύο κλειδιά είναι μαθηματικά συνδεδεμένα μεταξύ τους, αλλά η γνώση του ενός (δημοσίου) δεν επιτρέπει την εύκολη αποκάλυψη του άλλου (ιδιωτικού). Αυτή η ιδιότητα στηρίζεται σε δύσκολα μαθηματικά προβλήματα, όπως η παραγοντοποίηση μεγάλων αριθμών.

Το ιδιωτικό κλειδί το έχει μόνο το μέρος της επικοινωνίας που θέλουμε να εξασφαλίσει την ταυτότητά του, ενώ το δημόσιο είναι γνωστό σε όλους ή τουλάχιστον σε όσους θέλουν να επικοινωνήσουν με τον κάτοχο του ιδιωτικού κλειδιού.

Ανάλογα την εφαρμογή μπορεί ο αποστολέας ή ο παραλήπτης να κατέχουν ένα ιδιωτικό κλειδί.

**Κρυπτογράφηση μηνυμάτων**

Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει ένα μήνυμα. Μόνο το ιδιωτικό κλειδί του παραλήπτη μπορεί να αποκρυπτογραφήσει το μήνυμα, εξασφαλίζοντας την εμπιστευτικότητα. Ταυτόχρονα μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα που στέλνει οποιοδήποτε και κανένας άλλος.

**Ψηφιακές Υπογραφές**

Ο αποστολέας δημιουργεί μια υπογραφή με το ιδιωτικό του κλειδί. Ο παραλήπτης μπορεί να την επαληθεύσει με το δημόσιο κλειδί του αποστολέα, επιβεβαιώνοντας την ταυτότητα του αποστολέα και την ακεραιότητα του μηνύματος.

# Κρυπτογράφηση δεδομένων

Σημειώστε ότι:

- Εάν πρέπει να είναι **ταυτόχρονα** εγγυημένη η ταυτότητα τόσο του παραλήπτη, όσο και του αποστολέα, θα πρέπει να χρησιμοποιηθούν **δύο ζεύγη** κλειδιών, ώστε ο κάθε ένας από τους δύο να έχει το δικό του ιδιωτικό κλειδί, εξασφαλίζοντας την ταυτότητά του.
- Επειδή η ασύμμετρη κρυπτογράφηση είναι πολύ απαιτητική σε υπολογιστικούς πόρους των συστημάτων (ισχύς επεξεργαστή και μνήμη) και απαιτεί σαφώς περισσότερο χρόνο από την συμμετρική, στις επικοινωνίες χρησιμοποιείται ένας συνδυασμός τους:
    1. Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται για να γίνει η ανταλλαγή των κλειδιών της συμμετρικής κρυπτογράφησης, ενώ
    2. Το κυρίως μήνυμα είναι κρυπτογραφημένο με συμμετρική κρυπτογράφηση με συμμετρικά κλειδιά, τα οποία αλλάζουν κατά τη διάρκεια της επικοινωνίας ώστε να δυσκολεύουν όποιον προσπαθήσει να αποκρυπτογραφήσει το εκάστοτε μήνυμα.
- Όσον αφορά την ασύμμετρη κρυπτογράφηση κατά την αποθήκευση δεδομένων, γίνεται εκμετάλλευσή της από μια κατηγορία κακόβουλου λογισμικού (malware), τα λεγόμενα **ransomware**, όπου τα δεδομένα του δίσκου μας, κρυπτογραφούνται με ασύμμετρο τρόπο και οι εκβιαστές ζητούν χρήματα ώστε να μας δώσουν το ιδιωτικό κλειδί της αποκρυπτογράφησης.

# DNS

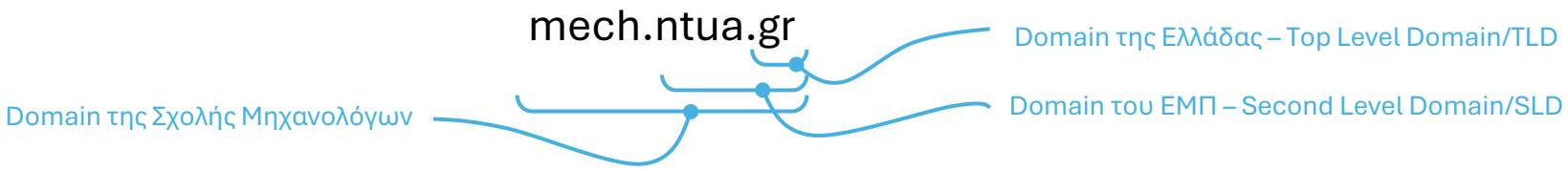
Επειδή οι διευθύνσεις IP είναι «ακατάλληλες» για απομνημόνευση από τον άνθρωπο, αλλά και επειδή μπορεί κατά καιρούς οι διευθύνσεις ενός server να μεταβάλλονται, δημιουργήθηκε η υπηρεσία DNS (Domain Name System ή ονοματοδοσίας) η οποία φροντίζει γι' αυτή την αντιστοίχιση.

Με την πάροδο του χρόνου και τις εξελίξεις στην τεχνολογία, αυτή η υπηρεσία μας παρέχει ακόμα περισσότερες πληροφορίες σχετικά με το κάθε domain.

Όταν λέμε λοιπόν ότι η διεύθυνση πχ ενός server είναι:

www.mech.ntua.gr

αυτό μέσω του συστήματος DNS αντιστοιχίζεται σε μία IP διεύθυνση, αλλά είναι χωρισμένο σε τμήματα, τα domains. Αυτά στο παραπάνω παράδειγμα είναι:




Το κάθε domain συνήθως εξυπηρετείται από ξεχωριστό server (ή ομάδα από servers αν υπάρχει μεγάλη ζήτηση). Έτσι για το gr domain (που είναι TLD) υπάρχουν οι αντίστοιχοι servers οι οποίοι γνωρίζουν για το κάθε SLD ποιος DNS server το εξυπηρετεί. Όμοια για το ntua.gr ο server γνωρίζει το mech.ntua.gr (και κάθε άλλο subdomain) ποιοι name servers το εξυπηρετούν, κ.ο.κ. αντίστοιχα υπάρχουν και κάποιοι κεντρικοί DNS servers (οι Root Name Servers) που γνωρίζουν τους DNS servers των TLDs.

# DNS

Ο κάθε DNS server γνωρίζει αντιστοιχίσεις για το (ή τα) domains του. Η κάθε μία από αυτές τις αντιστοιχίσεις (εγγραφές ή records) έχει τις παρακάτω πληροφορίες:

- Όνομα πχ www
- Τιμή πχ το IP του www
- Τύπος εγγραφής (“A” αν πρόκειται για IPv4 εγγραφή, “AAAA” αν πρόκειται για IPv6 εγγραφή, TXT για γενικής χρήσης εγγραφή, κ.ο.κ)
- TTL (Time To Live), χρόνος σε δευτερόλεπτα για τον οποίο η αντιστοίχιση θεωρούμε ότι δεν αλλάζει

Όταν λέμε λοιπόν ότι η διεύθυνση πχ ενός server είναι:

www.mech.ntua.gr

Τότε μέσω του συστήματος DNS εντοπίζεται ο DNS server του mech.ntua.gr και γίνεται σε αυτόν η ερώτηση τι IP έχει το www, και ο server παρέχει την απάντηση (μαζί με το TTL).

# DNS

Επειδή οι χρήστες του Internet είναι πάρα πολλοί, προκειμένου να αποφευχθεί η υπερφόρτωση των DNS, αλλά και να κερδηθεί χρόνος από τη διαδικασία της ερώτησης χρησιμοποιούνται οι παρακάτω τεχνικές:

- Κάθε δίκτυο έχει έναν DNS resolver, ο οποίος ενδεχομένως μπορεί και να γνωρίζει κάποιες απαντήσεις εκ των προτέρων. Στο σπίτι μας και αυτό τον ρόλο τον έχει το Modem/Router του παρόχου.
- Κάθε DNS resolver έχει μία προσωρινή μνήμη (cache) που θυμάται τις ερωτήσεις που του έχουν γίνει καθώς και τις απαντήσεις τους (για όσο ορίζει το TTL της κάθε απάντησης)
- Εάν δεν βρεθεί η απάντηση, μόνο τότε ξεκινά η διαδικασία της αναζήτησης του επίσημου (authoritative) server του συγκεκριμένου domain που μας ενδιαφέρει.
- Αντίστοιχη cache έχει και η κάθε συσκευή που βρίσκεται στο δίκτυο και κάνει ερωτήματα DNS (πχ κινητό, Η/Υ)

Η δομή του συστήματος DNS μας παρέχει:

- Αποκέντρωση
- Ασφάλεια
- Επιτάχυνση (μέσω caching)
- Ιεραρχική Δομή

# Επίπεδο Εφαρμογής: Ηλεκτρονική Αλληλογραφία (e-mails)

Η υπηρεσία ηλεκτρονικής αλληλογραφίας ή ταχυδρομείο (e-mail) αποτελείται από δύο υπηρεσίες (αποστολής και λήψης) και οι οποίες αρχικά δεν ήταν σχεδιασμένες να παρέχουν καμία περισσότερη προστασία από όσο έχει και το φυσικό ταχυδρομείο. Η λογική του όλου συστήματος e-mail βασίζεται στο ότι ο κάθε χρήστης έχει μία προσωπική θυρίδα όπου αποθηκεύονται όλα τα μηνύματα που προορίζονται γι' αυτόν.

Στην διεύθυνση κάθε θυρίδας, δηλαδή μία «διεύθυνση e-mail» όπως συνηθίζουμε να λέμε, διακρίνονται δύο μέρη, τα οποία ενώνονται με το σύμβολο @:

- Το όνομα του χρήστη και
- Το όνομα του domain (το οποίο συνεπάγεται τη IP διεύθυνση του mail server)

Ο χώρος κάθε θυρίδας είναι πεπερασμένος και ο χρήστης πρέπει να φροντίζει να έχει πάντα αρκετό χώρο ώστε να λαμβάνει νέα μηνύματα.

Κάθε μήνυμα e-mail περιλαμβάνει:

- Διεύθυνση παραλήπτη
- Διεύθυνση αποστολέα (κατά δήλωση)
- Θέμα/Τίτλο του μηνύματος
- Σώμα μηνύματος (μπορεί να είναι απλό κείμενο ή HTML κείμενο)
- Συνημμένα αρχεία

# Επίπεδο Εφαρμογής: Αποστολή e-mails

Η πρώτη υπηρεσία αφορά την αποστολή των μηνυμάτων προς κάποιον server ο οποίος αποθηκεύει τα μηνύματα στις θυρίδες των χρηστών. Το πρωτόκολλο αυτό ονομάζεται SMTP (Simple Mail Transfer Protocol). Ένας SMTP server παρέχει τις ακόλουθες υπηρεσίες προς τον χρήστη:

- Προαιρετικά ελέγχει την ταυτότητα του αποστολέα
- Ενδεχομένως υπογράφει ψηφιακά το e-mail του αποστολέα (κάποια βασικά στοιχεία του) με το private key, ώστε να είναι πιο αξιόπιστη η ταυτότητά του αποστολέα (DKIM). Αυτή επαληθεύεται μέσω του public key, το οποίο υπάρχει διαθέσιμο στο DNS του αποστολέα.
- Ο server προωθεί στον κατάλληλο server του παραλήπτη (βάσει του των εγγραφών του DNS του παραλήπτη) – ενδεχομένως με τη μεσολάβηση κάποιων e-mail gateways.

Εάν κάποιο από τα βήματα αυτά αποτύχει, ενδεχομένως αποστέλλεται σχετικό ενημερωτικό e-mail στον αποστολέα.

Σε κάθε έναν από τους servers που εμπλέκονται (SMTP servers, Mail Gateways, Mail Server παραλήπτη) μπορεί να γίνεται έλεγχος εάν το περιεχόμενο του e-mail (πχ συνημμένα) περιέχει κακόβουλο ή ύποπτο λογισμικό.

# Επίπεδο Εφαρμογής: Παραλαβή e-mails

Η δεύτερη υπηρεσία αφορά την λήψη και διαχείριση των μηνυμάτων από τους παραλήπτες και μπορεί να χρησιμοποιηθεί είτε το POP3 (Post Office Protocol) είτε το IMAP (Internet Mail Access Protocol). Αυτά τα πρωτόκολλα τα παρέχει (συχνά και τα δύο) ο Mail Server του παραλήπτη.

Αυτός παρέχει τις ακόλουθες υπηρεσίες:

- Ο server του παραλήπτη ενδεχομένως επιβεβαιώνει ότι ο αποστολέας (η IP του SMTP server) δικαιούται να στέλνει e-mails εκ μέρους του, βάσει των εγγραφών που διατίθενται στο DNS του αποστολέα. Επίσης ενδέχεται να ελέγχει αν ο αποστολέας (το IP του SMTP server) είναι καταχωρημένος σε λίστα αποστολέων με παραπλανητικά ή επικίνδυνα μηνύματα.
- Ενδέχεται να ελέγχει και το περιεχόμενο του μηνύματος (συνημμένα, κλπ) για την ύπαρξη κακόβουλου ή ύποπτου λογισμικού.
- Ο server του παραλήπτη αποθέτει το e-mail στη θυρίδα του παραλήπτη

# Επίπεδο Εφαρμογής: Παραλαβή e-mails

Στο e-mail υπάρχουν οι παρακάτω τυπικές κακόβουλες περιπτώσεις:

**Phishing (Απάτη με σκοπό την κλοπή στοιχείων)**

Το phishing είναι μια τεχνική απάτης που χρησιμοποιεί μηνύματα ηλεκτρονικής αλληλογραφίας για να υποκλέψει ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, ή προσωπικά δεδομένα. Τα emails φαίνονται συνήθως ως προερχόμενα από αξιόπιστες πηγές (π.χ. τράπεζες, εταιρείες ή ακόμη και συναδέλφους σας)

Τι να κάνετε:

- **Επαληθεύστε τον αποστολέα**: Ελέγξτε τη διεύθυνση του αποστολέα προσεκτικά. Ο αποστολέας μπορεί να φαίνεται νόμιμος, αλλά μικρές αλλαγές στη διεύθυνση μπορεί να υποδηλώνουν απάτη. Ιδανικά **επικοινωνήστε μαζί του** με άλλο τρόπο: τηλεφωνήστε στον φίλο σας που υποτίθεται ότι σας έστειλε e-mail που δεν περιμένατε, επικοινωνήστε με την τράπεζα σχετικά με το e-mail που λάβατε και σας ζητάει να κάνετε κάτι «σημαντικό» ή «επείγον» ή να συνδεθείτε στο σύστημά της.
- **Μην κάνετε κλικ σε συνδέσμους** ή επισυνάψτε αρχεία από άγνωστες ή ύποπτες πηγές. – Αν πχ σας ανησύχησε το e-mail για κάτι που αφορά την τράπεζά σας, τότε **συνδεθείτε** στην τράπεζα **με αποθηκευμένο link** ή όπως συνδέεστε όταν το κάνετε με δική σας πρωτοβουλία
- **Μην δίνετε προσωπικές πληροφορίες** μέσω email ή μηνυμάτων.
- Χρησιμοποιήστε παρόχους email που ενσωματώνουν έλεγχο SPF, DKIM, και DMARC για την προστασία από πλαστογράφηση αποστολέα.

# Επίπεδο Εφαρμογής: Παραλαβή e-mails

## Malware (Κακόβουλα συνημμένα)

Τα κακόβουλα συνημμένα είναι αρχεία που περιέχουν ιούς, trojans, ransomware ή άλλες κακόβουλες εφαρμογές που μπορούν να καταστρέψουν δεδομένα ή να αποκτήσουν πρόσβαση στους υπολογιστές και τα προσωπικά σας αρχεία.

Τι να κάνετε:

- **Μην ανοίγετε συνημμένα αρχεία** από άγνωστες πηγές ή αν δεν περιμένατε το email.
- **Σάρωση των συνημμένων με antivirus**: Βεβαιωθείτε ότι το antivirus λογισμικό σας είναι ενεργό και επικαιροποιημένο για να ανιχνεύει νέες απειλές.
- Αν το email είναι από έναν **άγνωστο**, διαγράψτε το χωρίς να ανοίξετε τα συνημμένα αρχεία.

## Spam (Ανεπιθύμητη αλληλογραφία)

Τα spam emails είναι συνήθως ανεπιθύμητες ή διαφημιστικές μηνύματα, που μπορούν επίσης να περιέχουν κακόβουλους συνδέσμους ή να σας παραπλανήσουν σε απάτες.

Τι να κάνετε:

- **Αναφέρετε ως spam** τα μηνύματα που είναι ανεπιθύμητα μέσω του προγράμματος email σας.
- **Φιλτράρετε το spam**: Ενεργοποιήστε τα φίλτρα για να αποκλείσετε ανεπιθύμητα μηνύματα.
- **Μην απαντάτε σε spam μηνύματα ή κάνετε κλικ σε διαφημίσεις ή συνδέσμους σε αυτά.** Το μόνο που πετυχαίνετε είναι να επιβεβαιώνετε ότι η διεύθυνσή σας λειτουργεί και ότι διαβάζετε τα μηνύματά σας, με αποτέλεσμα να προσελκύετε ακόμα περισσότερα spam.

# Επίπεδο Εφαρμογής: Παραλαβή e-mails

**Malicious Links (Σύνδεσμοι προς Κακόβουλες Ιστοσελίδες)**

Τα phishing emails περιλαμβάνουν συχνά κακόβουλους συνδέσμους που κατευθύνουν τον χρήστη σε ψεύτικες ιστοσελίδες που έχουν σχεδιαστεί για να υποκλέψουν προσωπικά δεδομένα ή να μολύνουν τον υπολογιστή σας με malware.

Τι να κάνετε:

- **Μην κάνετε κλικ σε συνδέσμους** αν δεν είστε σίγουροι για την προέλευση του email.
- Κυρίως **πληκτρολογήστε** τη διεύθυνση της ιστοσελίδας στον περιηγητή σας (browser) και όχι μέσω του συνδέσμου του email, αν πρέπει να επισκεφτείτε μία ιστοσελίδα (εννοείται ότι αντιγράφοντας τον σύνδεσμο που προτείνει το e-mail)
- **Ελέγξτε προσεκτικά τη διεύθυνση** URL για να βεβαιωθείτε ότι είναι αυθεντική (π.χ., "www.bank.com" αντί για "www.banx.com").

# WWW – World Wide **Web**

Η πιο διάσημη υπηρεσία του Internet είναι το Web το οποίο υλοποιείται μέσω του πρωτοκόλλου **HTTP** (HyperText Transfer Protocol). Ο client της επικοινωνίας ονομάζεται φυλλομετρητής (**browser**), ενώ ο server **Web** ή HTTP server.

Η κάθε ιστοσελίδα που παρουσιάζεται στον browser του χρήστη αποτελείται από ένα αρχείο **HTML** (HyperText Markup Language), το οποίο περιγράφει το περιεχόμενο της σελίδας που προβάλλεται, καθώς και όλα τα υπόλοιπα απαραίτητα στοιχεία για την σωστή και καλαίσθητη προβολή της.

Η γλώσσα **HTML** είναι μια γλώσσα περιγραφής δεδομένων και όχι μία γλώσσα προγραμματισμού. Περιγράφει τη δομή και το περιεχόμενο μιας ιστοσελίδας και έχει τη δυνατότητα να περιέχει υπερσυνδέσεις (δηλαδή συνδέσμους που οδηγούν σε άλλες ιστοσελίδες), καθώς και διάφορα άλλα βοηθητικά αρχεία (πχ πολυμέσα, εικόνες).

# WWW – World Wide **Web**

Το σύνολο των ιστοσελίδων που φιλοξενούνται στον ίδιο server κάτω από την ίδια διεύθυνση, ονομάζεται ιστότοπος (website ή site).

Η διεύθυνση του ιστοτόπου είναι της μορφής:

`http://www.mech.ntua.gr`

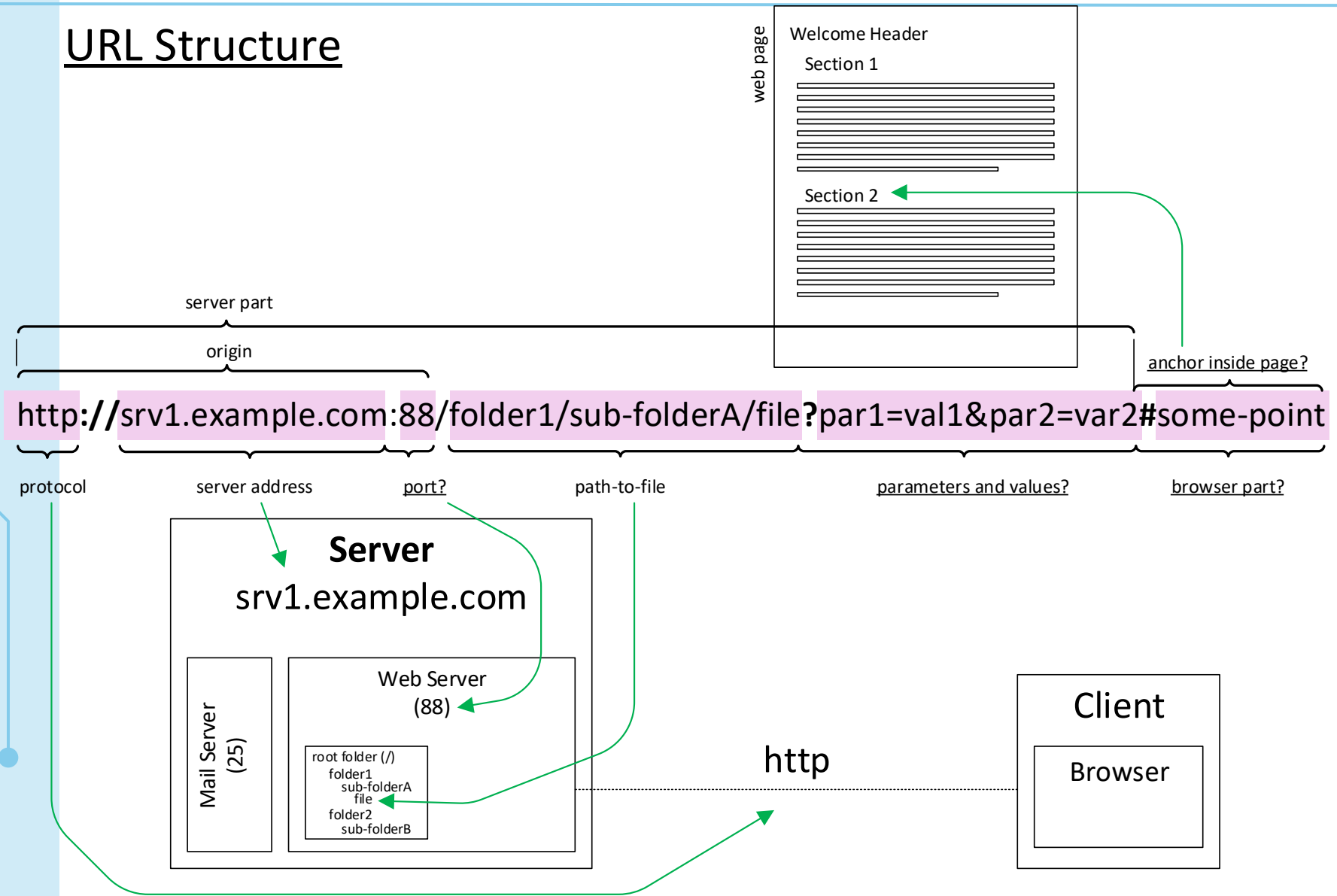
Μια τέτοια «απλή» διεύθυνση οδηγεί στην «αρχική σελίδα» (home page) του ιστοτόπου. Οι διευθύνσεις όλων των σελίδων του ίδιου ιστοτόπου ξεκινάνε με αυτό το λεκτικό.

Η κάθε σελίδα έχει τη δική της μοναδική διεύθυνση που ονομάζεται και **URL** (Universal ή Uniform Resource Locator).

Κάθε στοιχείο της σελίδας έχει επίσης το δικό του URL. Αυτό συμβαίνει επειδή όλα τα βοηθητικά αρχεία μιας ιστοσελίδας δεν περιλαμβάνονται μέσα στον κώδικα της HTML, αλλά μόνο ως αναφορά μέσω του URL τους.

# Η δομή ενός URL

## URL Structure



# Σύνταξη HTML

Η HTML αποτελείται από περιοχές κώδικα που βρίσκονται ανάμεσα σε ειδικές λέξεις κλειδιά που ονομάζονται **tags** και έχουν τη μορφή:

```
<tag attr1="val1" attr2="val2">content</tag>
```

Κάθε ένα τέτοιο αντιστοιχεί σε μία ορθογώνια περιοχή στη σελίδα. Επίσης το περιεχόμενό του μπορεί να περιέχει άλλα HTML tags.

Τα tags δέχονται κάποιες παραμέτρους που τροποποιούν τη συμπεριφορά ή την εμφάνισή τους ή παρέχουν κάποιες πρόσθετες πληροφορίες.

# Σύνταξη HTML

Τα ονόματα των tags μερικές φορές προσδίδουν κάποια διαφορετική εμφάνιση, κυρίως όμως νοηματοδοτούν το περιεχόμενο (semantic names). Η διαφορετικότητα στην εμφάνιση γίνεται κυρίως με τη χρήση μιας άλλης γλώσσας περιγραφής, της CSS.

Μερικά tags δεν έχουν περιεχόμενο, έτσι δεν χρειάζεται να τερματιστούν και μπορεί να είναι της μορφής:

```
<tag attr1="val1" attr2="val2">
```

Τέτοιο μπορεί να είναι ένα tag που περιγράφει μια εικόνα.

Κάποια tags μπορεί να υπάρχουν μόνο μία φορά σε μία ιστοσελίδα, πχ `<html>`, `<head>`, `<body>`, `<title>`

# Δομή της HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport«
          content="width=device-width, initial-scale=1.0">
    <title>Hello World</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body class="page-body">
  <header class="page-header">
    <h1 class="main-title">Hello World!</h1>
  </header>
  <main class="content">
    <p class="description">Welcome to my first HTML page.
        This is a simple example of using HTML and
        CSS to create a visually appealing web page.
    </p>
    <img class="image" src="example-image.jpg"
         alt="A hypothetical image" width="400"><br>
    <a href="https://www.ntua.gr">E.M.Π.</a>
  </main>
  <footer class="page-footer">
    <p class="footer-text">© 2024 My First Web Page</p>
  </footer>
</body>
</html>
```

Πρότυπο της HTML

Γλώσσα του κειμένου

Κωδικοποίηση χαρακτήρων

Τίτλος Ιστοσελίδας

Βοηθητικό αρχείο CSS
(ρυθμίζει την εμφάνιση)

<h1> Κεφαλίδα κειμένου

<header>
Πάνω μέρος

<p> Παράγραφος κειμένου

<main>
Κύριο
περιεχόμενο

<body>
Ορατό περιεχόμενο
σελίδας

<img> Αναφορά σε εικόνα

Υπερσύνδεσμος προς το ΕΜΠ

<p> Παράγραφος κειμένου

<footer>
Κάτω μέρος

# Δομή της CSS

Τα αρχεία CSS (Cascading StyleSheets) κατά κύριο λόγο περιγράφουν την εμφάνιση των tags ή των «κλάσεων» μιας HTML σελίδας. Οι κλάσεις είναι ονοματισμένες ομάδες ρυθμίσεων. Η μορφή ενός αρχείου είναι κάπως όπως αυτό.

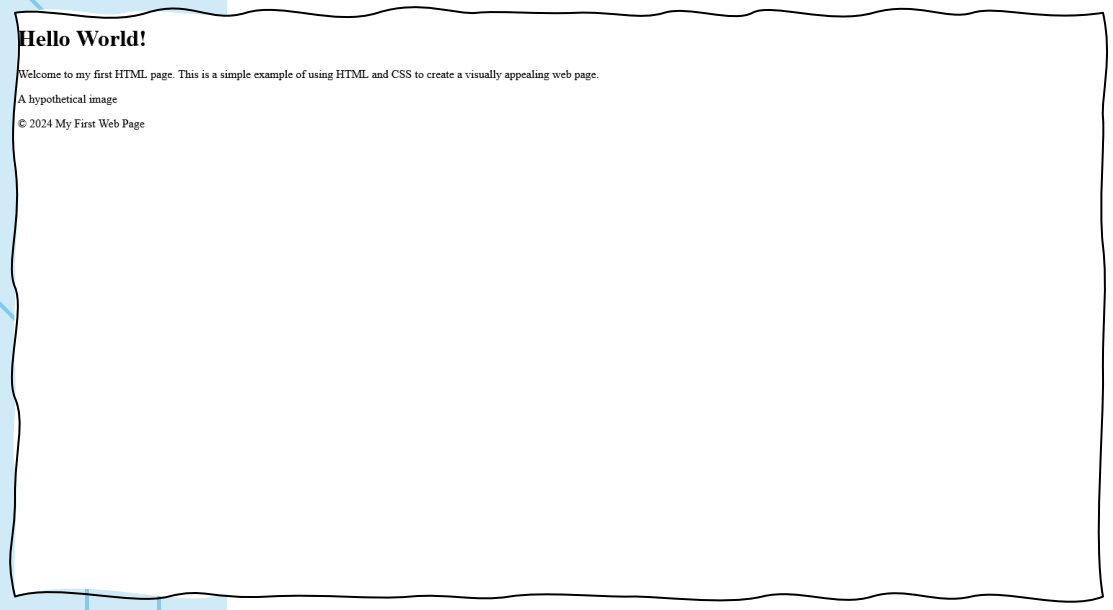
```
.page-body {
    font-family: Arial, sans-serif;
    background-color: #f4f4f9;
    color: #333;
    margin: 0;
    padding: 0;
    text-align: center;
}

/* Στυλ για την κεφαλίδα */
.page-header {
    background-color: #4CAF50;
    padding: 20px;
}

.main-title {
    color: white;
    margin: 0;
    font-size: 2.5em;
}
```

```
/* Στυλ για το κύριο περιεχόμενο */
.content {
    margin: 20px auto;
    max-width: 800px;
    padding: 20px;
    text-align: center;
}

.description {
    font-size: 1.2em;
    color: #555;
    margin-bottom: 20px;
}

.image {
    border: 3px solid #ddd;
    border-radius: 10px;
    box-shadow: 2px 2px 10px
                rgba(0, 0, 0, 0.1);
    max-width: 100%;
}
```

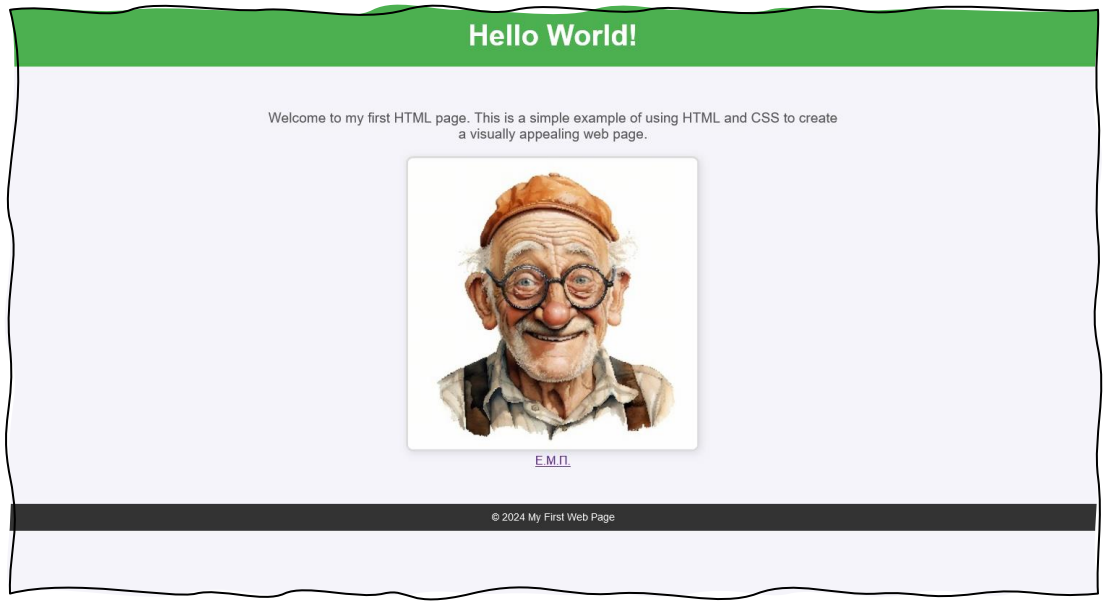
```
/* Στυλ για το υποσέλιδο */
.page-footer {
    background-color: #333;
    color: white;
    padding: 10px 0;
    margin-top: 30px;
}

.footer-text {
    margin: 0;
    font-size: 0.9em;
}
```

# Επίδραση του CSS

## Ιστοσελίδα (μόνο HTML)




## Ιστοσελίδα με CSS και εικόνα




Δείτε το https://csszengarden.com/ για να καταλάβετε πόσο μπορεί να επηρεάσει το CSS την εμφάνιση μιας HTML.

# HTTPS : Κρυπτογραφημένο HTTP

Όταν ένας χρήστης στέλνει πληροφορίες σε έναν ιστότοπο, θέλει να είναι σίγουρος για τουλάχιστον δύο πράγματα:

1. Ότι μιλάει όντως με τον ιστότοπο που νομίζει ότι μιλάει
2. Ότι οι πληροφορίες τους δεν μπορούν να υποκλαπούν κατά τη μεταφορά

Αυτά τα δύο, τα εγγυάται το https μέσω της χρήσης κρυπτογράφησης των διακινούμενων πληροφοριών με ένα private κλειδί του Web Server και ένα public key για τον client

Τα κλειδιά δημιουργούνται από ανεξάρτητες αρχές, οι οποίες επιβεβαιώνουν στον browser ότι το κλειδί είναι όντως του ιστοτόπου που μας ενδιαφέρει.

Πλέον είναι σημαντικό τα sites στα οποία συνδεόμαστε και αποστέλλουμε κρίσιμα ή προσωπικά στοιχεία, να χρησιμοποιούν μόνο κρυπτογραφημένη σύνδεση, τόσο για την κυρίως web σελίδα, όσο και για όλα τα URLs στα οποία αναφέρεται αυτή.

# Ασφάλεια στους υπολογιστές

Παρότι υπάρχουν όλοι αυτοί οι μηχανισμοί ασφαλείας, πάντα ο κάθε χρήστης πρέπει να είναι υποψιασμένος και προσεκτικός.

Ας δούμε μερικές γενικές αλήθειες:

- Ποτέ κανένας διαχειριστής συστήματος δεν χρειάζεται το password σας
- Ποτέ δεν χρειάζεται κανείς επιβεβαίωση για να σας καταθέσει χρήματα στην τράπεζα
- Κανένας άγνωστος ετοιμοθάνατος, ζάμπλουτος από την Αφρική δεν θέλει να σας χαρίσει χρήματα
- Η μάνα του «Αντετοκούνμπο» δεν θα σας ζητήσει να υποστηρίξετε τη φιλανθρωπική της οργάνωση – έχω βάσιμες πληροφορίες ότι γνωρίζει πλουσιότερους από εσάς

…

# Ασφάλεια στους υπολογιστές

Γι’αυτό να:

- Μην χρησιμοποιείτε απλά passwords ή τέτοια που να πρέπει να τα σημειώνετε. Δημιουργήστε μνημονικά κάποιο password και αναπαραστήστε το με τουλάχιστον 8-10 χαρακτήρες χρησιμοποιώντας ευφάνταστα τα σύμβολα του υπολογιστή για να αντικαταστήσουν κάποιους χαρακτήρες. Πχ
  - Ατιμούτσικο : @e-m0751-co
  - Είσαι επιθετικός : ~=EC*>0=~
- Μην δίνετε ποτέ τα passwords σας για οποιοδήποτε λόγο
- Μην πατάτε links πουθενά (είτε ιστοσελίδες, είτε e-mails) χωρίς να ελέγχετε τον πραγματικό προορισμό τους πολύ προσεκτικά. Αφήστε το ποντίκι πάνω στον σύνδεσμο και συνήθως κάτω αριστερά εμφανίζεται ο πραγματικός προορισμός του. Προσοχή σε παρεμφερή ονόματα domains (πχ mtua αντί ntua)

# Ασφάλεια στους υπολογιστές

Επίσης να:

- Προσέχετε να μην βλέπει κανείς την οθόνη σας όταν συμπληρώνετε στοιχεία
- Μην χρησιμοποιείτε για ευαίσθητες πληροφορίες κοινόχρηστους Η/Υ
- Μην συνδέεστε σε ελεύθερα WiFi, μπορούν εύκολα να υποκλέψουν ακόμα και κρυπτογραφημένες συνδέσεις
- Χρησιμοποιείστε κρυπτογραφημένο VPN όταν είστε σε άγνωστα δίκτυα
- Προτιμήστε την καλωδιακή σύνδεση από την ασύρματη σύνδεση

**Προσοχή!** Οι περισσότερες και πιο επιτυχημένες παραβιάσεις ασφαλείας δεν βασίζονται σε τεχνικές αδυναμίες, αλλά σε ανθρώπινες. Οι τεχνικές αυτές ονομάζονται social hacking ή social engineering!

# Πραγματικές Περιπτώσεις

**Η υπόθεση "Microsoft Tech Support Scam"**

- **Τι συνέβη:** Σε αυτή τη διάσημη απάτη, απατεώνες τηλεφωνούσαν σε ανυποψίαστους χρήστες, ισχυριζόμενοι ότι ήταν τεχνικοί υποστήριξης της Microsoft. Τους έλεγαν ότι ο υπολογιστής τους είχε «μολυνθεί από ιούς» ή παρουσίαζε «προβλήματα ασφαλείας» και τους ζητούσαν να εγκαταστήσουν ένα εργαλείο απομακρυσμένης πρόσβασης για "επιδιόρθωση". Στην πραγματικότητα, το εργαλείο έδινε πλήρη έλεγχο στους απατεώνες, που στη συνέχεια έκλεβαν δεδομένα, εγκαθιστούσαν ransomware ή ζητούσαν χρήματα για «συνδρομή υποστήριξης».
- **Αντίκτυπος:** Εκατοντάδες χιλιάδες χρήστες σε όλο τον κόσμο έχουν πέσει θύματα αυτής της τακτικής. Το 2019, η Microsoft ανέφερε ότι λάμβανε περίπου **13.000 καταγγελίες ανά μήνα** για τέτοιες απάτες.

**Η υπόθεση του Matt Honan**

- **Τι συνέβη:** Ο Matt Honan, δημοσιογράφος του Wired, έπεσε θύμα επίθεσης το 2012 όταν επιτιθέμενοι εκμεταλλεύτηκαν διαδικασίες κοινωνικής μηχανικής για να αποκτήσουν πρόσβαση στους online λογαριασμούς του. Οι επιτιθέμενοι τηλεφώνησαν στην υποστήριξη της Apple και, χρησιμοποιώντας κομμάτια προσωπικών πληροφοριών (που είχαν βρει στο διαδίκτυο), έπεισαν τους υπαλλήλους να επαναφέρουν το Apple ID του. Στη συνέχεια, χρησιμοποίησαν αυτόν τον λογαριασμό για να αποκτήσουν πρόσβαση στο Gmail και στο Twitter του.
- **Αντίκτυπος:** Οι επιτιθέμενοι διέγραψαν τα δεδομένα του από όλες τις συσκευές του, συμπεριλαμβανομένων οικογενειακών φωτογραφιών και εγγράφων. Το περιστατικό έγινε διάσημο ως παράδειγμα των κινδύνων της κοινωνικής μηχανικής.

**Η υπόθεση της Crelan Bank**

- **Τι συνέβη:** Το 2016, η βελγική τράπεζα Crelan έχασε πάνω από **70 εκατομμύρια ευρώ** μέσω μιας επίθεσης κοινωνικής μηχανικής. Οι επιτιθέμενοι τηλεφωνούσαν σε υπαλλήλους της εταιρείας, υποδυόμενοι υψηλόβαθμα στελέχη, και τους έπεισαν να πραγματοποιήσουν μεταφορές χρημάτων σε λογαριασμούς που ελέγχονταν από τους ίδιους.
- **Αντίκτυπος:** Η υπόθεση αποκάλυψε πόσο ευάλωτες είναι ακόμη και μεγάλες επιχειρήσεις απέναντι σε τακτικές κοινωνικής μηχανικής που βασίζονται στη δημιουργία αίσθησης επείγοντος και εμπιστοσύνης.

# Τι πρέπει οπωσδήποτε να γνωρίζω από τη διάλεξη;

- **Τη γενική λογική της κρυπτογράφησης (συμμετρική και ασύμμετρη) και το πως πρακτικά συνδυάζονται**
- **Τις δύο εφαρμογές της ασύμμετρης κρυπτογράφησης: κρυπτογράφηση μηνυμάτων και ψηφιακές υπογραφές**
- **Τη δομή και λογική του συστήματος DNS**
- **Τη γενική λογική του συστήματος e-mails (θυρίδα, διεύθυνση, κίνδυνοι)**
- **Τη γενική λογική των ιστοσελίδων (HTML, CSS, κίνδυνοι)**
- **Τα γενικότερα ζητήματα ασφαλείας που προκύπτουν**
- **Τον κίνδυνο του social engineering**