# Τεχνολογίες για ανώνυμη περιήγηση

| | | | |
|---|---|---|---|
| Ιστότοπος: | Κοινότητα Υποστήριξης Εκπαιδευτικών eTwinning | Εκτυπώθηκε από: | ΠΑΡΑΣΚΕΥΗ ΚΑΡΚΑΒΕΛΗ |
| Μάθημα: | V. Ασφάλεια στο διαδίκτυο – Αξιολόγηση και ανάπτυξη κριτικής σκέψης για το ψηφιακό περιεχόμενο | Ημερομηνία: | Τρίτη, 10 Δεκεμβρίου 2024, 6:18 PM |
| Βιβλίο: | Τεχνολογίες για ανώνυμη περιήγηση | | |

# Πίνακας περιεχομένων

# 1. Εισαγωγή

## Εισαγωγή

Στην παρούσα ενότητα θα εξετάσουμε μερικά από τα πιο διαδεδομένα εργαλεία και τεχνολογίες που συμβάλλουν στην επίτευξη ανωνυμίας. Ειδικότερα, θα εστιάσουμε σε εφαρμογές όπως τα VPN, το δίκτυο Tor και εξειδικευμένα λειτουργικά συστήματα, τα οποία παρέχουν αυξημένη προστασία και ασφάλεια στην ψηφιακή καθημερινότητα.

# 2. VPN

## Τι είναι ένα δίκτυο VPN;

Ένα VPN (Virtual Private Network - Εικονικό Ιδιωτικό Δίκτυο) είναι μια υπηρεσία που προστατεύει την ιδιωτικότητά σας στο διαδίκτυο και διατηρεί τα δεδομένα σας ασφαλή. Όταν χρησιμοποιείτε ένα VPN, η διαδικτυακή σας κίνηση περνά μέσα από έναν "ασφαλή τούνελ" που κρυπτογραφεί τα δεδομένα σας. Αυτό σημαίνει ότι κανείς, ούτε ο πάροχος του ίντερνετ σας (ISP), ούτε χάκερ, ούτε τρίτοι, μπορεί να δει τι κάνετε online. Επιπλέον, το VPN κρύβει την πραγματική σας διεύθυνση IP και σας εμφανίζει σαν να βρίσκεστε σε άλλη τοποθεσία, αυξάνοντας την ανωνυμία σας.


Image by freepik

## Πώς να χρησιμοποιήσετε ένα VPN;

### Επιλογή VPN Υπηρεσίας:

Επιλέξτε μια αξιόπιστη υπηρεσία VPN. Υπάρχουν δωρεάν και επί πληρωμή επιλογές, αλλά τα επί πληρωμή VPN συχνά προσφέρουν καλύτερη ασφάλεια και ταχύτητα. Μερικές δημοφιλείς υπηρεσίες είναι το NordVPN, το ExpressVPN, και το ProtonVPN.

### Εγκατάσταση του VPN:

Κατεβάστε την εφαρμογή VPN στη συσκευή σας (υπολογιστή, κινητό, tablet ή router). Οι περισσότερες υπηρεσίες προσφέρουν εύκολους οδηγούς εγκατάστασης.

### Σύνδεση στο VPN:

Ανοίγετε την εφαρμογή του VPN και συνδέεστε με τα στοιχεία σας (όνομα χρήστη και κωδικό). Στη συνέχεια επιλέγετε έναν διακομιστή (server) σε μια χώρα της επιλογής σας. Μπορείτε να επιλέξετε τον πλησιέστερο για καλύτερη ταχύτητα ή έναν σε άλλη χώρα για πρόσβαση σε γεωγραφικά περιορισμένο περιεχόμενο.

Αφού συνδεθείτε, το VPN λειτουργεί στο παρασκήνιο. Κάθε φορά που συνδέεστε στο διαδίκτυο, η κίνησή σας είναι κρυπτογραφημένη και προστατευμένη.

Μπορείτε όμως να ενημερωθείτε περισσότερο διαβάζοντας τα παρακάτω άρθρα:

https://www.pcsteps.gr/

# 3. Δίκτυο TOR

## Τι είναι αυτό το περιβόητο Tor;

Η πλήρης ονομασία του είναι: **The Onion Router** (Tor) και πρωτοδημιουργήθηκε πριν κάποια χρόνια για τις ανάγκες του ναυτικού των ΗΠΑ. Η λέξη onion (=κρεμμύδι) υποδηλώνει τα πολλαπλά "στρώματα" που χρησιμοποιεί κατά την λειτουργία του. Οι σκοποί που πλέον χρησιμοποιείται είναι πολλοί και δεν είναι όλοι κατ' ανάγκη και ηθικοί. Έχοντας ως κύριο στόχο την ανωνυμία, όπως είναι ευνόητο, μπορεί να το χρησιμοποιήσει ο καθένας για διαφορετικούς σκοπούς. Είναι γεγονός ότι μέσω του Tor, διακινείται πορνογραφία σε όλα τα επίπεδα, μα και πως χρησιμοποιείται για κυβερνοεπιθέσεις ή ακόμα και για πρόσβαση με χώρες όπου υπάρχει λογοκρισία στο διαδίκτυο.

## Πώς δουλεύει το Tor

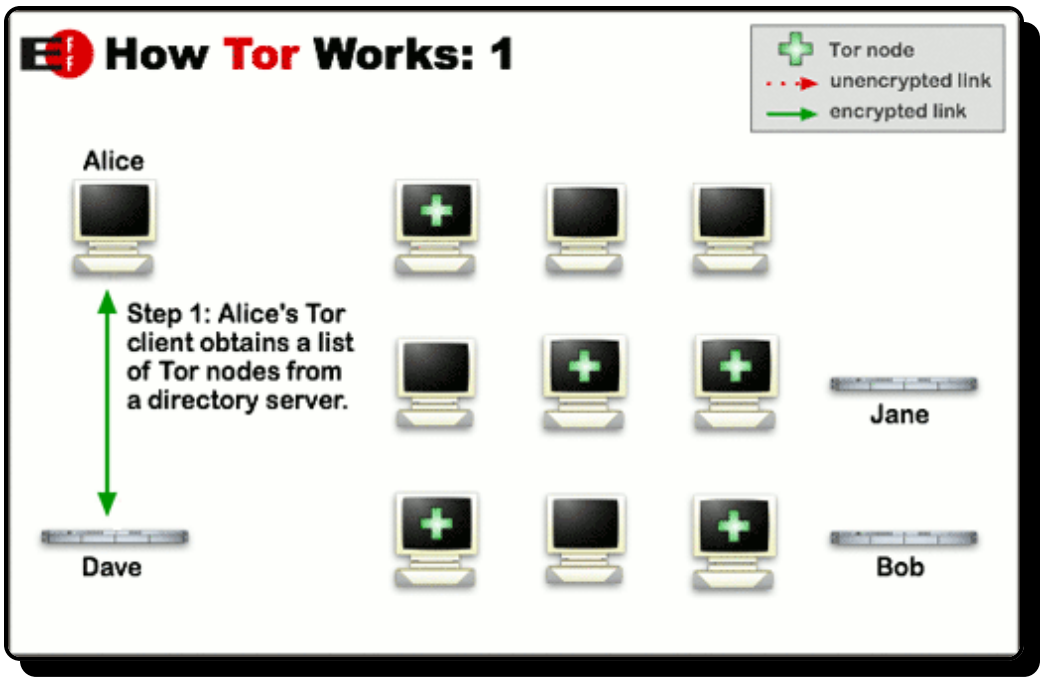
Φανταστείτε ένα δίκτυο με συνδεδεμένους πολλούς (χιλιάδες) υπολογιστές (=σταθμούς), οι οποίοι είναι συνδεδεμένοι στο δίκτυο Tor (κάνουν δηλαδή χρήση της εφαρμογής).

Ένας πολύ βασικός παράγοντας είναι και το πλήθος των χρηστών

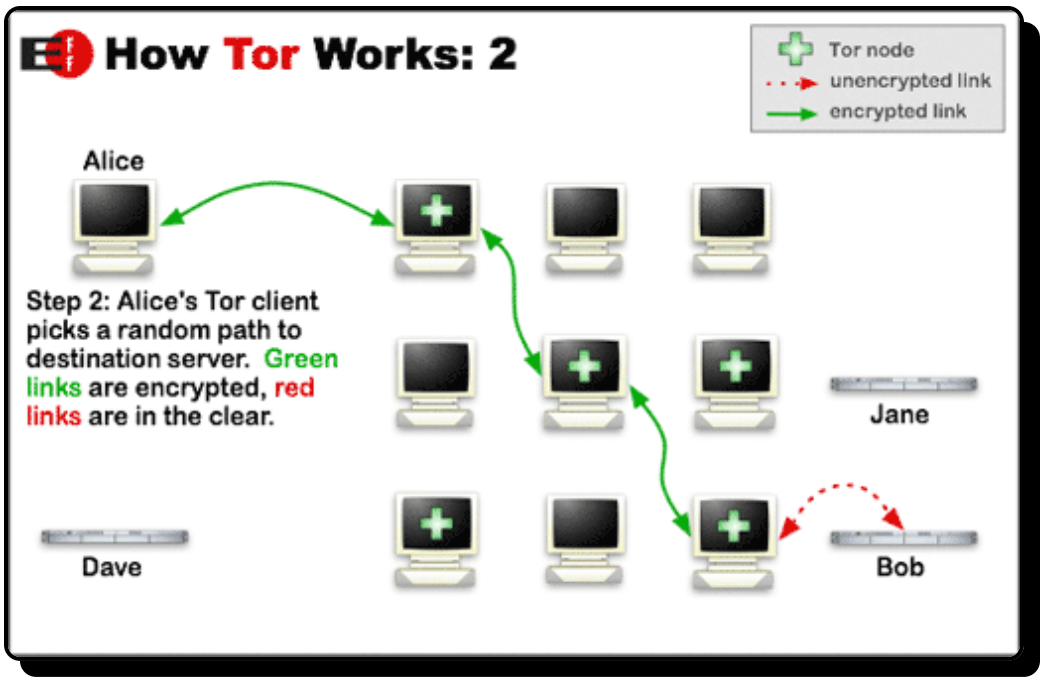
που είναι συνδεδεμένοι μέσω Tor, καθώς όσο πιο μεγάλος ο αριθμός, τόσο πιο καλή η συνολική ποιότητα του δικτύου, μα και ακόμα πιο μεγάλη η ατομική ανωνυμία που μπορεί να επιτευχθεί. Θέλοντας λοιπόν να γίνει κάποια ανταλλαγή πληροφορίας (αρχείου) από έναν υπολογιστή σε κάποιον άλλον, αυτή η πληροφορία (αρχείο), θα ταξιδέψει κρυπτογραφημένα, μέσα από ένα από τα χιλιάδες εναλλακτικά μονοπάτια που δίνουν οι συνδεδεμένοι υπολογιστές μεταξύ τους.

Ας το δούμε και με τις εικόνες, όπου είναι περισσότερο κατανοητό:

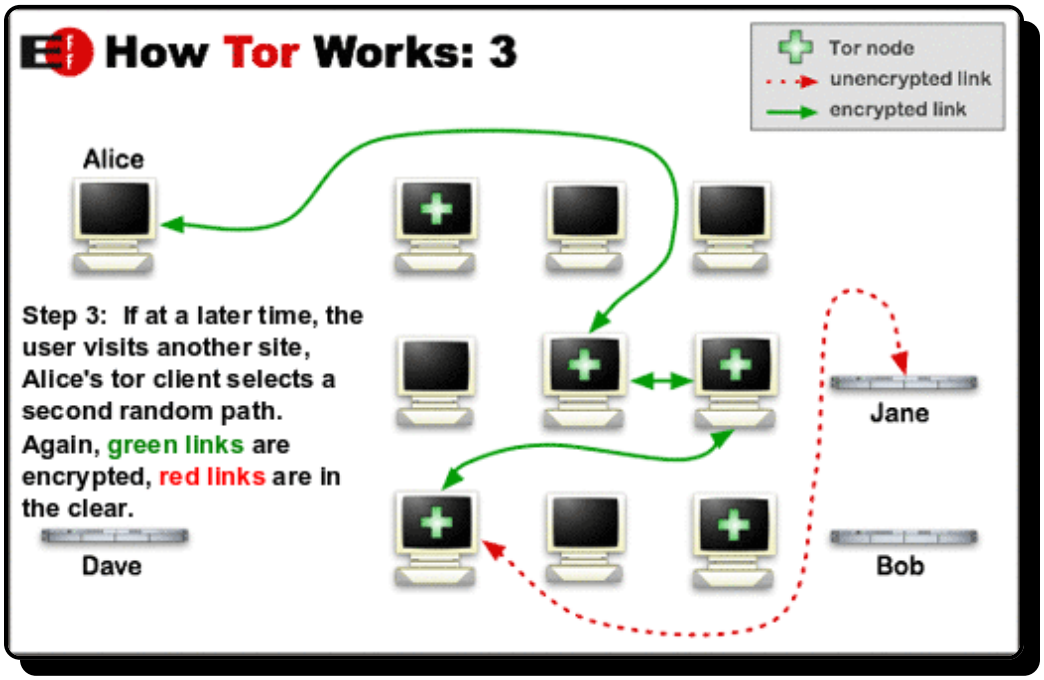
- Ανοίγοντας κάποιος χρήστης του Tor, θα συνδεθεί σε κάποιον τυχαίο από τους διαθέσιμους εκείνη την στιγμή κόμβους.
  Αυτή η τυχαία επιλογή σύνδεσης κάθε φορά, εξασφαλίζει την ανωνυμία καθώς η διαδρομή της αποστολής της κάθε πληροφορίας, δεν αφήνει εμφανή ίχνη, από το πού ξεκίνησε η αποστολή και ποιος ήταν ο τελικός αποδέκτης:




- Στη συνέχεια αρχίζοντας η αποστολή της πληροφορίας, αυτή θα μεταπηδάει από κόμβο σε κόμβο (τυχαία), πλήρως κρυπτογραφημένη και δίνοντας τις πληροφορίες που χρειάζεται ο κάθε κόμβος για μια νέα κρυπτογράφηση και αποστολή σε άλλο κόμβο και ούτω καθεξής, ωσότου φτάσει στον τελικό παραλήπτη, όπου και θα μπορέσει να διαβάσει τη πληροφορία κανονικά:




- Αν τώρα ο υπολογιστής client, ο χρήστης δηλαδή, επιθυμεί να αποστείλει μια άλλη πληροφορία ακόμα ή να επισκεφθεί κάποια ιστοσελίδα θα γίνει η ίδια διαδικασία, με διαφορετική (τυχαία και πάλι) διαδρομή αυτή την φορά, επιτυγχάνοντας έτσι τη μεγίστη δυνατή ανωνυμία:



## Περιγραφή

Το Tor είναι διαθέσιμο για όλα τα λειτουργικά συστήματα και μπορεί να χρησιμοποιηθεί τόσο σαν κανονικά εγκατεστημένη εφαρμογή όσο και σαν portable, από κάποιο USB στικάκι.

Στην ουσία, όπως αναφέρει και το ίδιο

> Το Tor project, δεν είναι απλά μια εφαρμογή, μα είναι τρόπος ζωής.

Και αυτό ισχύει, καθώς θα πρέπει να αλλάξετε τις μέχρι τώρα συνήθειες που είχατε κατά την πλοήγησή σας. Αυτό σημαίνει πως απευθύνεται σε ανθρώπους που λαμβάνουν σοβαρά υπόψη το ηλεκτρονικό απόρρητο και το δικαίωμα της ανωνυμίας.

> Είναι ευνόητο, πως δεν έχει κανένα απολύτως νόημα, να χρησιμοποιείτε το Tor για να συνδεθείτε στο Facebook ή να διαβάσετε το GMail σας, κλπ. Από την στιγμή δηλαδή που δίνετε κάπου τα στοιχεία σας, δεν υπάρχει και λόγος για ανωνυμία.

## Tor και Dark Web

Σύμφωνα με τον Roger Dingledine, έναν από τους τρεις ιδρυτές του Tor Project, Σκοτεινό Διαδίκτυο (**Dark Web** ή **Βαθύ Διαδίκτυο** ή **Deep**

**Web** ή **Dark Net** ή **Deep Net** ή **Hidden Web**), δεν υπάρχει. Οι άνθρωποι προσπαθούν απλά να προστατευθούν από την παρακολούθηση και να προστατεύσουν την ιδιωτική τους ζωή. Είναι οι οικογένειες που προσπαθούν να προστατεύσουν τα παιδιά τους από το να παρακολουθούν το κάθε τους κλικ στο διαδίκτυο. Το Διαδίκτυο είναι - θα έπρεπε να είναι - πηγή γνώσης και έρευνας, και όχι το μάτι του Big Brother.

Σε καμία περίπτωση, ΔΕΝ είναι η διαδικτυακή «στέγη» εγκληματιών, όπως ισχυρίζονται μερικοί, παπαγαλίζοντας αυτά που τους καθοδηγούν να πουν και να επιβάλλουν στις συνειδήσεις των ανθρώπων.

Ο Roger Dingledine, άσκησε έντονη κριτική στους δημοσιογράφους που παρουσιάζουν το σύστημα προστασίας του ιδιωτικού απορρήτου (το Tor) ως κρησφύγετο των εμπόρων ναρκωτικών και των παιδεραστών. Θα πρέπει κάποτε να σταματήσει αυτή η προπαγάνδα πως το Tor το χρησιμοποιούν αποκλειστικά εγκληματίες για να διεισδύσουν ανώνυμα στο Dark Web προκειμένου να κρύβονται από τις αρχές.

Κι επειδή τα νούμερα λένε πάντα την αλήθεια, ας μιλήσουμε με αριθμούς.

Στην πραγματικότητα, επισήμανε ο Dingledine, **μόνο το 3% των**

χρηστών του Tor συνδέονται με κρυφές υπηρεσίες (.onion),

γεγονός που υποδηλώνει ότι η συντριπτική πλειοψηφία των χρηστών του δικτύου το χρησιμοποιούν για την ανώνυμη περιήγησή τους σε δημόσιους ιστότοπους για εντελώς νόμιμους σκοπούς. Και προφανώς το χρησιμοποιούν για να μην παρακολουθείται η καθημερινότητά τους από τις εκάστοτε ιστοσελίδες.

> Με πολύ απλά λόγια και για να γίνει απόλυτα κατανοητό, οι χρήστες του Tor - από τους δημοσιογράφους έως τους ακτιβιστές αλλά και τους απλούς χρήστες - χρησιμοποιούν τον Tor για να αποκρύψουν την ταυτότητά τους από τους ιδιοκτήτες ιστοτόπων. Και, όπως είναι προφανές, μόνον υπόκοσμος δεν είναι όλοι αυτοί.

Στην ουσία, δεν μπορούμε να μιλάμε για Σκοτεινό διαδίκτυο. Δεν υπάρχει. Δεν είναι παρά μόνο πολύ λίγες ιστοσελίδες.
Δεν αποτελεί λοιπόν έκπληξη το γεγονός ότι ο πιο δημοφιλής ιστότοπος που επισκέπτονται οι χρήστες Tor είναι το Facebook. Το 2014 ο γίγαντας των διαφημίσεων αγκάλιασε τον Tor, δημιουργώντας μια κρυμμένη υπηρεσία ως πύλη στο κοινωνικό του δίκτυο. Πλέον, πάνω από ένα εκατομμύριο άνθρωποι συνδέονται με την αυτοκρατορία του Mark Zuckerberg (ιδρυτής του Facebook) χρησιμοποιώντας το δίκτυο ανωνυμοποίησης Tor. Είναι βέβαια ένα

μικρό ποσοστό της βάσης χρηστών του Facebook, δεδομένου ότι οι χρήστες του Facebook ξεπερνούν το ένα δισεκατομμύριο, αλλά είναι πολύ σημαντικό για ένα έργο όπως το Tor.

* Μπορείτε να διαβάσετε σχετικά με το Dark Web εδώ: https://www.pcsteps.gr

## Αναφορές - Επιπλέον υλικό

- https://ellak.gr/2014/07/the-tor-project-diatiriste-tin-anonimia-ke-tin-idiotikotita-sas-sto-diadiktio/
- Tor έναντι VPN - Ποιο είναι πιο ασφαλές

# 4. Λειτουργικά συστήματα για ανωνυμία

## Λειτουργικά συστήματα για ανωνυμία

Οι διανομές Linux που επικεντρώνονται στην ιδιωτικότητα και την ανωνυμία έχουν σχεδιαστεί για να παρέχουν υψηλά επίπεδα προστασίας δεδομένων και απορρήτου. Αυτές οι διανομές χρησιμοποιούν τεχνολογίες όπως το Tor, την απομόνωση εφαρμογών, και τη μη καταγραφή δεδομένων στο σύστημα. Απευθύνονται σε δημοσιογράφους, ακτιβιστές, ερευνητές, ή οποιονδήποτε θέλει να προστατεύσει τα προσωπικά του δεδομένα στον ψηφιακό κόσμο.

Tails (The Amnesic Incognito Live System)

Μια διανομή Linux σχεδιασμένη για πλήρη ανωνυμία και ιδιωτικότητα. Όλη η διαδικτυακή κίνηση δρομολογείται μέσω του Tor, και δεν αφήνει κανένα ίχνος στον υπολογιστή (εκτός αν αποθηκευτούν δεδομένα σκόπιμα).

Whonix

Μια διανομή που παρέχει προηγμένη ανωνυμία μέσω της χρήσης δύο εικονικών μηχανών – μία για τις εφαρμογές και μία για τη δρομολόγηση μέσω Tor.

## Qubes OS

Διανομή που βασίζεται στην απομόνωση εφαρμογών μέσω εικονικών μηχανών, παρέχοντας υψηλή ασφάλεια. Υποστηρίζει τη χρήση Tails ή Whonix για επιπλέον επίπεδα προστασίας.

**Σύνδεσμος**: qubes-os.org