

Προστασία ιδιωτικότητας: ελέγξτε το ψηφιακό σας αποτύπωμα

/ Πεμπτουσία· Ορθοδοξία-Πολιτισμός-Επιστήμες



Online privacy tips: 3 τρόποι για να ελέγξετε το ψηφιακό σας αποτύπωμα

Έχετε αφήσει στοιχεία για το ποιος είστε και τι σας αρέσει σε όλο το Διαδίκτυο. Εδώ θα δούμε πώς μπορείτε να περιορίσετε αυτό που αφήνετε πίσω σας - το ψηφιακό σας αποτύπωμα ή αλλιώς digital footprint.

Όπως οι πραγματικές πατημασιές, έτσι και το ψηφιακό αποτύπωμα δείχνει ένα

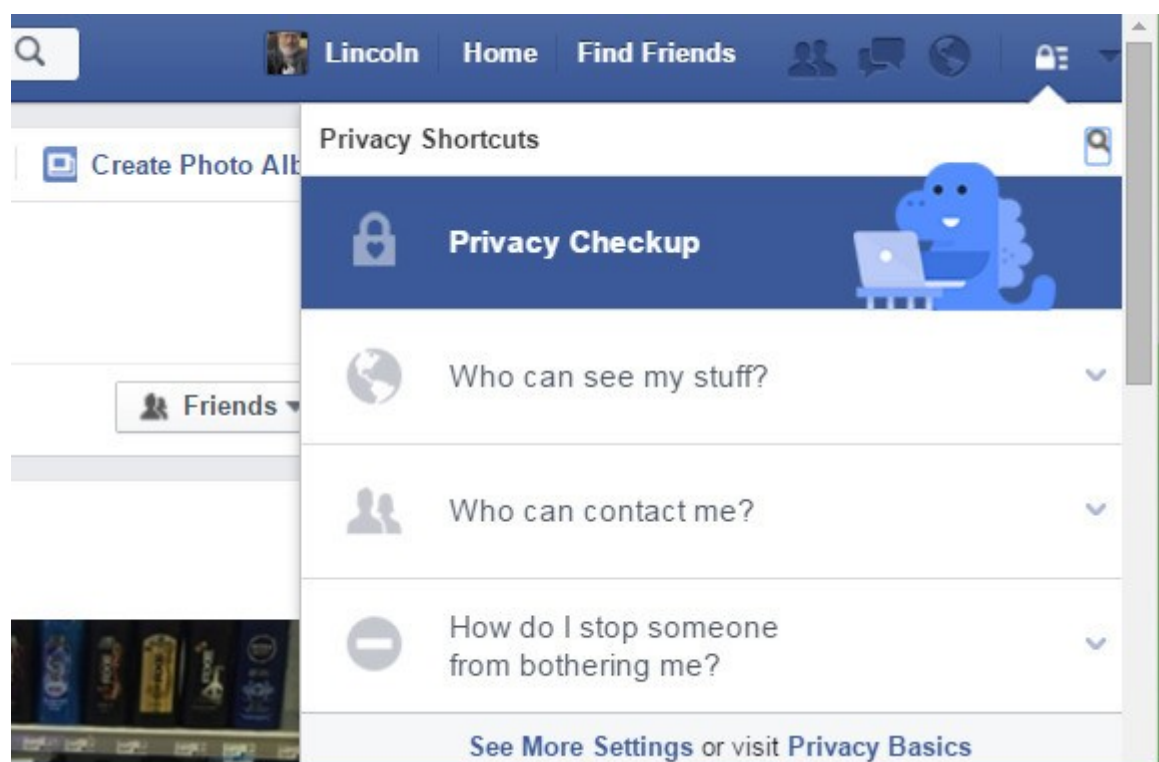
ολόκληρο ιστορικό του πού ήσασταν και τι είχατε κάνει. Δείχνουν τις αναζητήσεις σας, ό, τι αγοράσατε, ποια site επισκεφτήκατε, καθώς και τις απόψεις που έχετε εκφράσει στα κοινωνικά δίκτυα.

Πολλές κερδοσκοπικές εταιρείες, τόσο νόμιμες όσο και παράνομες, μπορούν να βγάλουν κέρδος με το να γνωρίζουν καλύτερα το ιστορικό σας. Οι κυβερνήσεις, επίσης, θα ήθελαν να μπουν σ' αυτό το παιχνίδι.

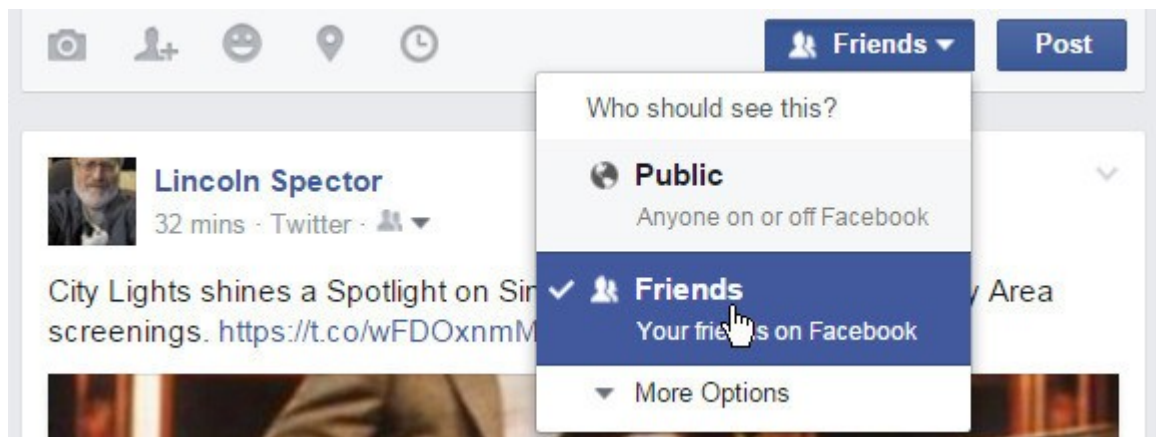
Έτσι παρακάτω μπορείτε να πάρετε μια καλή ιδέα ώστε να αποκτήσετε και πάλι τον έλεγχο από το [ψηφιακό](#) σας αποτύπωμα.

1. **Να είστε προσεκτικοί με τα social media**

Σε κάθε online υπηρεσία που χρησιμοποιείτε, ελέγξτε τις ρυθμίσεις απορρήτου. Στο [Facebook](#), για παράδειγμα, θα τις βρείτε κάνοντας κλικ στο εικονίδιο κλειδώματος στην επάνω δεξιά γωνία της οθόνης και περνώντας ανάμεσα από τις διάφορες επιλογές.



Αλλά αυτό δεν είναι αρκετό. Πριν καταχωρήσετε την ανάρτησή σας, επανεξετάστε αυτό που λέτε και βλέποντάς το αναρωτηθείτε αν αυτό είναι κάτι που θα θέλατε οι γονείς σας, τα παιδιά σας, τα πεθερικά σας, το αφεντικό σας ή η εφορία να διαβάσουν. Και τότε σιγουρευτείτε ότι θα το κάνετε εμφανές μόνο στα άτομα που θέλετε να το δουν.



2. Χρησιμοποιήστε πολλαπλές ταυτότητες

Οι πληροφορίες που μοιράζεστε σε έναν δικτυακό τόπο μπορούν να συνδυαστούν με πληροφορίες από έναν άλλο, δημιουργώντας ένα πιο πλήρες αρχείο για το ποιο είστε! Για να προστατεύσετε τον εαυτό σας, προσπαθήστε να είστε διαφορετικοί άνθρωποι σε διαφορετικά sites.

A screenshot of a 'Create your account' form. It has three input fields: 'First name' with the value 'Lincoln', 'Last name' with the value 'Spector', and 'Email address' which is empty. Below the email field, there is a suggestion for a 'New Masked Email' with the address 'lincoln@[redacted].com'. A mouse cursor is pointing at this suggestion.

Μερικά sites σας προσδιορίζουν με βάση το όνομα, αλλά πολλά σας αναγνωρίζουν και από τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Έτσι, χρησιμοποιήστε διαφορετικές διευθύνσεις σε διαφορετικά sites. Σκεφτείτε ακόμη και την περίπτωση να χρησιμοποιείτε και διαφορετικές πιστωτικές κάρτες.

Το Blur, μια δωρεάν επέκταση του [Chrome](#) και του Firefox, σας επιτρέπει να καλύψετε (mask) τη διεύθυνση ηλεκτρονικού σας ταχυδρομείου. Όταν εισάγετε το email σας σε μια ηλεκτρονική φόρμα, το Blur σας δίνει τη δυνατότητα να δημιουργήσετε μια νέα, τυχαία διεύθυνση. Αυτή η διεύθυνση αντιστοιχεί στην

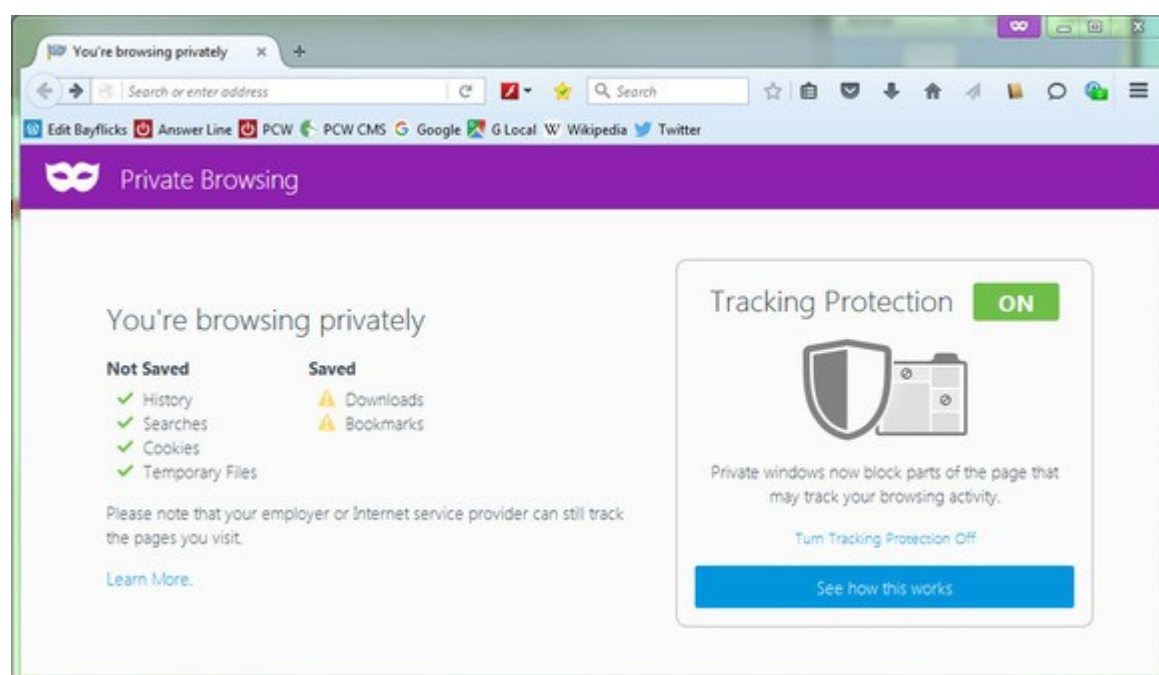
πραγματική σας διεύθυνση, την οποία όμως ποτέ δεν βλέπει ο αποστολέας.

Εάν είστε πρόθυμοι να πληρώσετε \$39 το χρόνο ή \$79 για τρία χρόνια -το Blur Premium μπορεί να καλύπτει και τους αριθμούς τηλεφώνου και πιστωτικής κάρτας σας.

3. **Αναζητήστε ιδιωτικά**

Το πρόγραμμα περιήγησής σας γνωρίζει πάρα πολλά για εσάς και μοιράζεται τις πληροφορίες αυτές με πάρα πολλούς αγνώστους. Αλλά υπάρχουν μέθοδοι για να ελέγξετε αυτή την κατάσταση.

Ο [browser](#) σας έχει σχεδόν σίγουρα ένα «ιδιωτικό παράθυρο» όπου δεν θα σώσει τα cookies σας, τις αναζητήσεις ή το ιστορικό σας. Στον Chrome, λέγεται New incognito window (Παράθυρο για ανώνυμη χρήση). Στον Internet Explorer και στον [Edge](#), λέγεται InPrivate Browsing (Ιδιωτική αναζήτηση) και τέλος, στον Firefox, New Private Window (Νέο ιδιωτικό παράθυρο). Καλά όλα αυτά αλλά δεν είναι τέλεια! Η κυβέρνηση μπορεί ακόμα να δει πού ήσασταν και κάθε [site](#) που επισκέπτεστε εξακολουθεί να βλέπει την IP διεύθυνσή σας.



Μια ακόμα καλύτερη λύση είναι να χρησιμοποιήσετε το πρόγραμμα περιήγησης Tor, το οποίο κρύβει την IP διεύθυνση σας και κρυπτογραφεί τα πάντα για το μεγαλύτερο μέρος της διαδρομής μεταξύ του υπολογιστή σας και με όποιον άλλο επικοινωνείτε, εξαφανίζοντας κατά κάποιο τρόπο το [ψηφιακό](#) σας αποτύπωμα. Σκεφτείτε την ως μια πολύ ιδιωτική ιδιωτική λειτουργία!

Πηγή: secnews.gr