

**ΒΑΛΑΒΑΝΗΣ
ΠΑΝΑΓΙΩΤΗΣ**

Π2012091

**ΙΟΝΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΕΡΚΥΡΑ**

*Προστασία προσωπικών
δεδομένων και εξέλιξη
μηχανισμών
παρακολούθησης τρίτων
στον Παγκόσμιο Ιστό*

Εισαγωγή

- Στην σημερινή εποχή, το διαδίκτυο έχει γίνει αναπόσπαστο κομμάτι στις ζωές των ανθρώπων.
- Η καθημερινότητα απαιτείται σε μεγάλο βαθμό από συσκευές και καταναλωτικά αγαθά που προέρχονται από εταιρείες και οργανισμούς πολύ μακριά από τον τόπο διαμονής του εκάστοτε χρήστη.
- Η άνοδος του βιωτικού επιπέδου των λαών καθώς και η ανάγκη για διευκόλυνση καθημερινών αναγκών, βοήθησε στην ραγδαία εξέλιξη του τρόπου αλληλεπίδρασης των χρηστών του διαδικτύου.
- Η ανάπτυξη όμως αυτή, επέφερε και ορισμένες επιπτώσεις πάνω στο θέμα της ιδιωτικότητας και της ασφάλειας των προσωπικών δεδομένων.



Προστασία Προσωπικών Δεδομένων

Η προστασία των προσωπικών δεδομένων θεσπίζεται από τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (Ε.Ε. 2016/679) και αποφασίστηκε να τεθεί σε εφαρμογή από τις 25 Μαΐου 2018, αφήνοντας ένα περιθώριο περίπου 2 ετών στις επιχειρήσεις αλλά και σε όλους τους χρήστες του διαδικτύου να συμμορφωθούν με τα νέα δεδομένα.

Οι επικείμενες διατάξεις ισχύουν σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και δημιουργήθηκαν έπειτα από έντονες διαβουλεύσεις όλων των συνεργαζόμενων κρατών

Στόχος του Κανονισμού είναι η προστασία της ιδιωτικότητας αλλά και των ηλεκτρονικών επικοινωνιών. Για τον λόγο αυτό, στις ειδικές σημειώσεις που επισυνάπτονται, ορίζεται ένας στόχος που πρέπει να επιτευχθεί από όλα τα κράτη-μέλη.

Οι κανόνες που θα χρησιμοποιηθούν για την επίτευξη του στόχου αυτού διαφέρουν από χώρα σε χώρα ανάλογα με την κουλτούρα, την οικονομική της κατάσταση και γενικά τον τρόπο με τον οποίο είναι δομημένη κοινωνικά.

Προστασία Προσωπικών Δεδομένων στην Ελληνική πραγματικότητα

Το 2006 τροποποιήθηκε ο Νόμος για να μπορεί να προστατεύει τους πολίτες πιά αποτελεσματικά απο υποκλοπές και παραβιάσεις της ιδιωτικότητας μέσω των ηλεκτρονικών επικοινωνιών.

Με τον νέο Κανονισμό του 2016, επιβλήθηκε σε όλες τις επιχειρήσεις που βρίσκονται στην Ευρωπαϊκή Ένωση -και κατα συνέπεια και στην Ελλάδα- που συλλέγουν ή/και επεξεργάζονται δεδομένα φυσικών προσώπων, να υιοθετήσουν τις νέες οριοθετήσεις.

Οι περισσότερες επιχειρήσεις δημιούργησαν μία νέα θέση εργασίας, αυτή του Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer, DPO), ο οποίος πρέπει να είναι επιστημονικά καταρτισμένος σε θέματα προστασίας δεδομένων και να γνωρίζει όλο το νομικό πλαίσιο που τα περιβάλλει.

Για την προσαρμογή των οργανισμών ορίζεται απο τον αρμόδιο της κυβέρνησης ένας Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων ο οποίος καλείται να συντονίζει τους φορείς του δημοσίου.

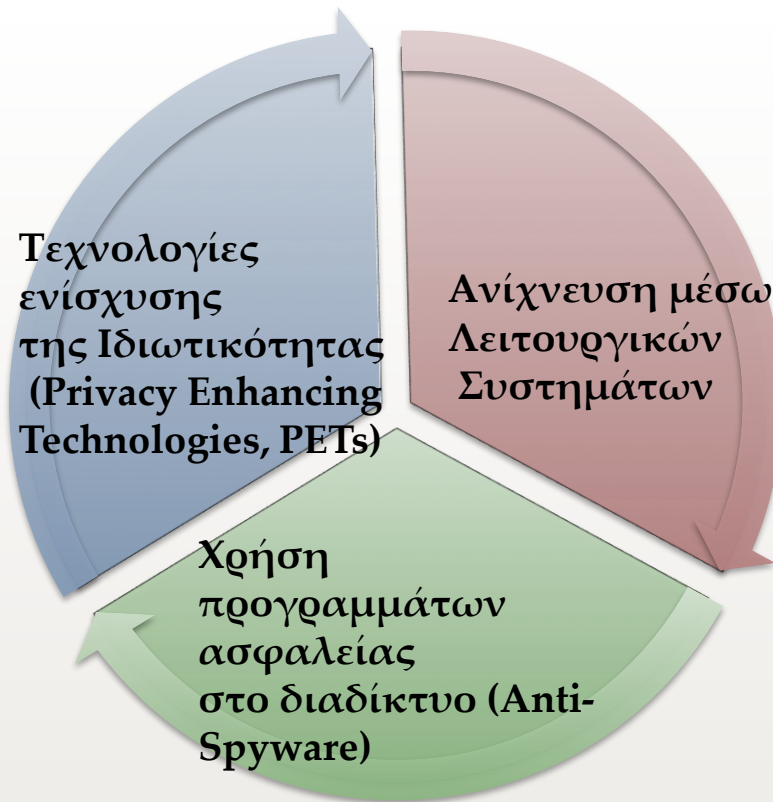
Έλεγχοι που έγιναν απο την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έξι μήνες μετά την οριστική εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων έδειξαν ότι ο δημόσιος τομέας στερείται διαφάνειας και συμμόρφωσης

Παράλληλα γίνονται μεγάλες προσπάθειες από τους συντονιστές DPO για άμεση εξαμάλυνση των θεμάτων που καθυστερούν την συμμόρφωση των οργανισμών με τον νέο Κανονισμό.

Μέτρα ασφαλείας για την Προστασία Προσωπικών Δεδομένων



Τρόποι ανίχνευσης των υποκλοπών



Εξέλιξη μηχανισμών παρακολούθησης τρίτων στον Παγκόσμιο Ιστό

Χρησιμοποιώντας
μεταδεδομένα
τηλεφώνου

Η
παρακολούθηση
μέσω GPS (Global
Positioning
System)

Μη συνειδητή
συνεργασία του
χρήστη
(CAPTCHA, IoT)

Ανάλυση τεχνικών προστασίας απο τις νέες μορφές διαδικτυακών υποκλοπών

Αποκλεισμός
διαφημιστικών
υπηρεσιών

Απόκρυψη της
διεύθυνσης IP

Τροποποίηση των
δεδομένων που
αποστέλλονται μέσω
του δικτύου

Αποκλεισμός cookies

DNT

Λειτουργία ιδιωτικής
περιήγησης

Διαγραφή της
προσωρινής μνήμης
και του ιστορικού του
προγράμματος
περιήγησης

Phishing

Το "ηλεκτρονικό" ψάρεμα είναι ένα έγκλημα στον κυβερνοχώρο στο οποίο ένας ή περισσότεροι χρήστες στοχοποιούνται μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου ή γραπτού μηνύματος από κάποιον που εμφανίζεται ως νόμιμο ίδρυμα για να εκμαιεύσει από τους χρήστες ευαίσθητα δεδομένα, όπως στοιχεία προσωπικής ταυτοποίησης, στοιχεία τραπεζικών και πιστωτικών καρτών και κωδικούς πρόσβασης

Μια πλήρης επίθεση phishing περιλαμβάνει τρεις ρόλους phishers. Πρώτον, οι αποστολείς στέλνουν ένα μεγάλο αριθμό ψευδών μηνυμάτων ηλεκτρονικού ταχυδρομείου τα οποία κατευθύνουν τους χρήστες σε δόλιες ιστοσελίδες. Δεύτερον, οι συλλέκτες δημιουργούν ψευδείς ιστότοπους

Οι phishers χρησιμοποιούν τις εμπιστευτικές πληροφορίες για να κάνουν μια πληρωμή. Οι οικονομικές ανταλλαγές συμβαίνουν συχνά μεταξύ αυτών των phishers

Τα τελευταία στατιστικά στοιχεία αποκαλύπτουν ότι οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα μαζί με τα social media και τα sites τυχερών παιχνιδιών εξακολουθούν να αποτελούν το επίκεντρο των phishers. Οι ΗΠΑ καλύπτουν το μεγαλύτερο ποσοστό στις επιθέσεις phishing, αντιπροσωπεύοντας το 43% των ιστότοπων ηλεκτρονικού "ψαρέματος" που ανακοινώθηκαν τον Ιανουάριο του 2012.

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" που αρχικά απευθύνονταν σε γενικούς καταναλωτές εξελίσσονται τώρα ώστε να συμπεριλαμβάνουν υψηλού επιπέδου στόχους, με στόχο την κλοπή πνευματικής ιδιοκτησίας, επιχειρηματικών μυστικών και ευαίσθητων πληροφοριών σχετικά με την εθνική ασφάλεια.

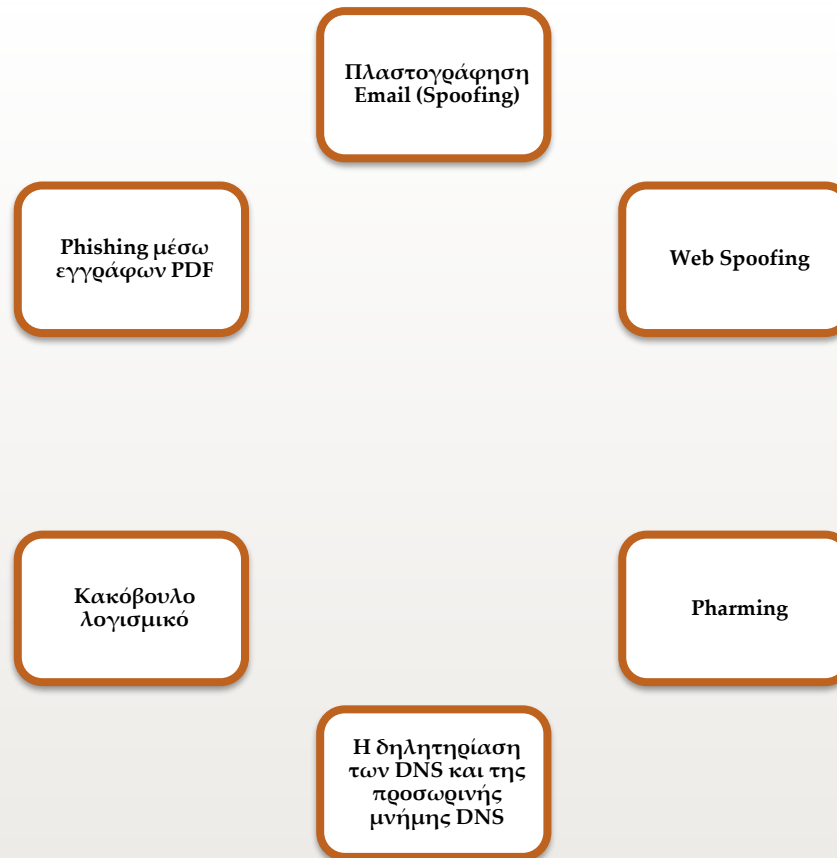
Τύποι phishing

Phishing με
κλόνους

Phishing
μέσω
τηλεφώνου

Phishing
τύπου Spear

Τεχνικές ηλεκτρονικού "ψαρέματος" και μέτρα αντιμετώπισης



Web Spoofing

Ένας πλαστογράφος (phisher) θα μπορούσε να δημιουργήσει έναν ιστότοπο που μοιάζει με έναν νόμιμο ιστότοπο, έτσι ώστε τα θύματα να πιστεύουν ότι πρόκειται για τον αυθεντικό ιστότοπο και να εισαγάγουν τους κωδικούς πρόσβασης και τα προσωπικά του στοιχεία, τα οποία συλλέγει ο phisher

Τα σύγχρονα προγράμματα περιήγησης έχουν ορισμένους ενσωματωμένους δείκτες ασφαλείας που μπορούν να προστατεύσουν τους χρήστες από απάτες ηλεκτρονικού "ψαρέματος"

Μόλις ο πλαστογραφημένος ιστότοπος είναι συνδεδεμένος στο διαδίκτυο, ο phisher πρέπει να κάνει τα υποψήφια θύματα να τον επισκεφθούν. Οι πλαστογράφοι έχουν την τάση να χρησιμοποιούν παραπλανητικές διευθύνσεις,

Οι δείκτες ασφαλείας των προγραμμάτων περιήγησης δεν είναι τόσο αποτελεσματικοί όσο κάποιος μπορεί να σκεφτεί. Τα Dynamic Skins Security φαίνεται να είναι μια καλή μέθοδος.

Κακόβουλο λογισμικό

Τα κακόβουλα προγράμματα μπορούν να χρησιμοποιηθούν για τη συλλογή εμπιστευτικών πληροφοριών απευθείας ή για να βοηθήσουν άλλες τεχνικές phishing.

Τα προϊόντα ασφάλειας πελατών είναι σε θέση να ανιχνεύσουν και να καταργήσουν το κακόβουλο λογισμικό, αλλά οι phishers μπορούν να καταστήσουν το malware μη ανιχνεύσιμο.

Οι συλλεγμένες πληροφορίες μπορούν να αποστέλλονται αυτόματα στους phishers μέσω ηλεκτρονικού ταχυδρομείου, διακομιστή ftp ή καναλιού IRC

Τα προϊόντα ασφάλειας των χρηστών αναπτύσσονται ευρέως. Το Microsoft Update αναπτύσσει επίσης μηνιαίως το "Εργαλείο αφαίρεσης κακόβουλου λογισμικού", το οποίο είναι ένας ελαφρύς σαρωτής κακόβουλου λογισμικού.

Πρόσθετα προληπτικά μέτρα

- Δεδομένου του κινδύνου phishing, ποιοι είναι οι τρόποι με τους οποίους τα άτομα και οι οργανώσεις μπορούν να προστατευθούν;
- Αν και είναι δύσκολο να εφαρμοστεί, η εκπαίδευση του χρήστη είναι ίσως ο καλύτερος μηχανισμός προστασίας. Αναγνωρίζοντας τη σοβαρότητα του θέματος, περισσότεροι μη κερδοσκοπικοί οργανισμοί και ομάδες ενώνουν τα χέρια τους για την καταπολέμηση της απάτης του ηλεκτρονικού "ψαρέματος".
- Σχετικά με τη νομοθεσία απαιτείται να υπάρξει ιδιαίτερη προσοχή σε αυτό το θέμα για να καθοριστεί ρητά το phishing και να αποδοθούν συγκεκριμένες ποινές για το ηλεκτρονικό ψάρεμα.



Εκπαίδευση χρηστών

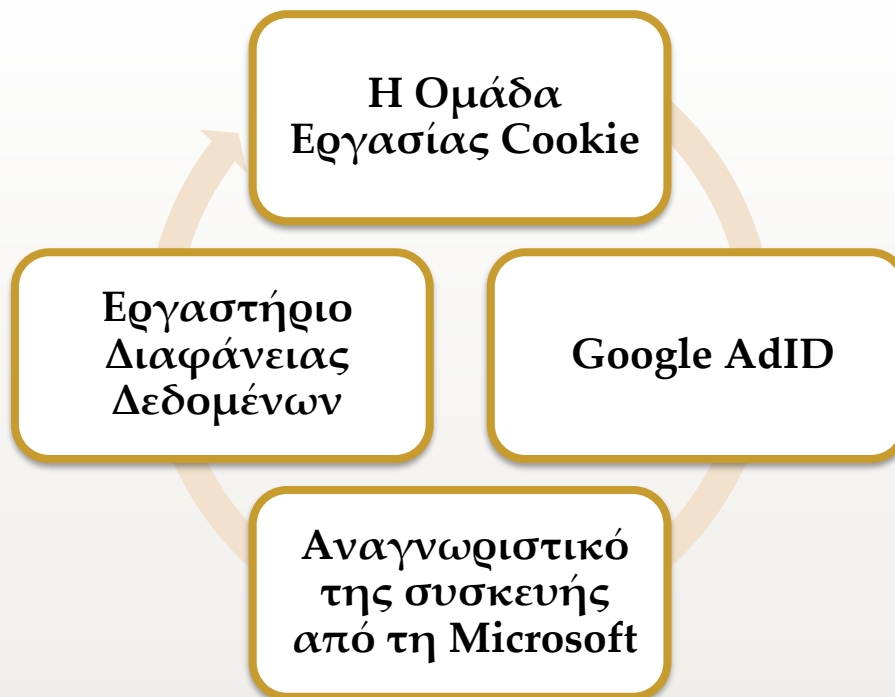
- Μια μελέτη σχετικά με την αποτελεσματικότητα πολλών εκπαιδευτικών υλικών κατά του ηλεκτρονικού "ψαρέματος" υποδηλώνει ότι τα εκπαιδευτικά υλικά μείωσαν την τάση των χρηστών να εισάγουν πληροφορίες σε ιστοσελίδες ηλεκτρονικού "ψαρέματος" κατά 40%.
- Ωστόσο, ορισμένα από τα εκπαιδευτικά υλικά ελάττωσαν επίσης ελαφρώς στην τάση των συμμετεχόντων να κάνουν κλικ σε νόμιμους συνδέσμους.
 - Αυτό οδηγεί στην πεποίθηση ότι είναι πρωταρχικής σημασίας να βρεθεί ένας νέος και αποτελεσματικός τρόπος εκπαίδευσης ενός μεγάλου μέρους του πληθυσμού
- Σήμερα, το phishing αναγνωρίζεται από τους χρήστες ως μια πραγματική και δυνητικά επιζήμια απειλή.
- Εάν υπάρχουν κατάλληλοι έλεγχοι κατά του ηλεκτρονικού "ψαρέματος" (phishing), υπάρχουν μεγάλες πιθανότητες να στραφούν οι πελάτες σε ασφαλέστερο μέρος για να κάνουν επιχειρήσεις.

Ομάδες κατά της απάτης

Το Phish Tank, το οποίο ξεκίνησε τον Οκτώβριο του 2006, είναι ένα συνεργατικό κέντρο εκκαθάρισης για δεδομένα και πληροφορίες σχετικά με το ηλεκτρονικό ψάρεμα στο διαδίκτυο.

Το APWG, που δημιουργήθηκε το 2003, είναι μια διεθνής κοινοπραξία που συγκεντρώνει επιχειρήσεις που έχουν πληγεί από επιθέσεις ηλεκτρονικού "ψαρέματος", εταιρείες ασφάλειας προϊόντων και υπηρεσιών, υπηρεσίες επιβολής του νόμου, κυβερνητικές υπηρεσίες, εμπορικές ενώσεις, περιφερειακές διεθνείς συμφωνίες συνθηκών και εταιρείες επικοινωνιών.

Το μέλλον της παρακολούθησης



Η Ομάδα Εργασίας Cookie (Donoghue, 2014) του Γραφείου Διαδραστικής Διαφήμισης ΙΑΒ (ΙΑΒ, 2014) σχεδιάζει μια νέα τεχνολογία για την παρακολούθηση χρηστών σε πολλαπλές συνεδρίες και συσκευές.

Σύμφωνα με άρθρο του Σεπτεμβρίου 2013 (Barr, 2013), η Google αναπτύσσει το AdID, ένα ανώνυμο αναγνωριστικό, το οποίο μπορεί να χρησιμοποιηθεί για τη διαφήμιση και την αντικατάσταση των cookies μέσω τρίτων.

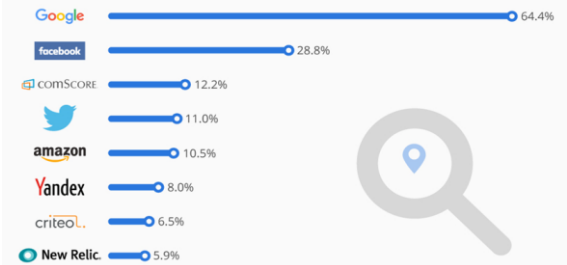
Ένα άρθρο από τον Οκτώβριο 2013 (Peterson, 2013) αποκαλύπτει ότι η Microsoft εργάζεται για την ανάπτυξη της δικής της τεχνολογίας παρακολούθησης χρησιμοποιώντας ένα αναγνωριστικό συσκευής. Η τεχνολογία έχει σχεδιαστεί για να καλύπτει επιφάνεια εργασίας, κινητά και xbox. Η άδεια χρήσης του αναγνωριστικού θα δίνεται στη Microsoft από τον χρήστη όταν εκείνος δέχεται τη συμφωνία χρήστη ή τους όρους παροχής υπηρεσιών.

Το Εργαστήριο Διαφάνειας Δεδομένων (Data Transparency Lab, DTL, 2014) είναι μια κοινότητα που στοχεύει στην αποσαφήνιση της χρήσης των προσωπικών δεδομένων στο διαδίκτυο και στη διερεύνηση τρόπων για ένα εμπόριο δεδομένων στο μέλλον το οποίο θα διέπεται από σεβασμό και πλήρη διαφάνεια.

Στατιστικά στοιχεία

They Know What You Clicked Last Summer

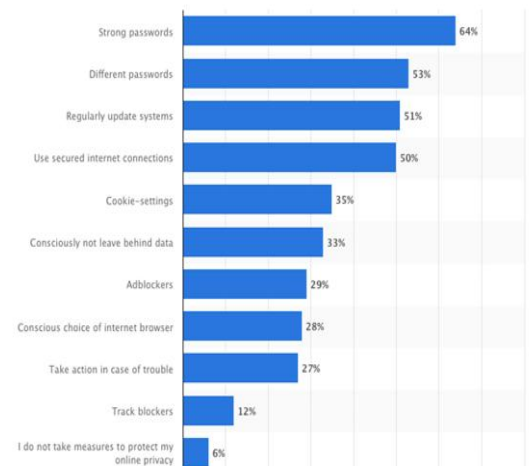
Percentage of global page loads tracked by the following companies



Based on the analysis of more than 144 million page loads by 850,000 users in more than 20 countries
Sources: Ghostery, Cligz

statista

statista



Where Are People Concerned About Online Privacy?

% of internet users increasingly concerned about online privacy to due internet companies*

Total



74%

Americas

United States



83%

Mexico



77%

Europe

France



78%

Italy



78%

Great Britain



76%

Germany



67%

Russia



61%

Asia

India



83%

China



76%

Turkey



74%

Japan



67%

Africa

South Africa



84%

Nigeria



75%

Tunisia



59%

Oceania

Australia



71%

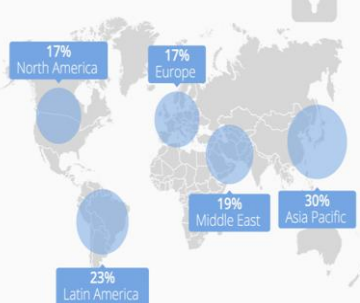
* Selected countries. Telephone interviews and online surveys were conducted between December 29, 2017, and March 5, 2018, with 12,956 people between the ages of 16 and 64 years old

Where Do People Use VPNs?

Top countries that use VPNs as a percent of total internet users



Percent of all internet users who use VPNs by region



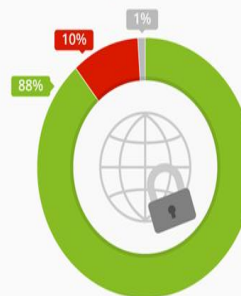
@StatistaCharts Source: GlobalWebIndex

statista

Most Parents Sit Down with Teens About Online Privacy

Share of parents in the U.S. who have spoken to their teenagers about online privacy in 2018*

Yes No No answer



* National sample conducted in the U.S. between May 5th to May 7th, 2018, which included 19,063 adults, of whom 3,222 were parents with children between 13 and 17 years old, along with 985 teenagers age 13 to 17 years



@StatistaCharts

Sources: Common Sense Media, SurveyMonkey

statista

ΕΥΧΑΡΙΣΤΩ!!

ΕΡΩΤΗΣΕΙΣ

