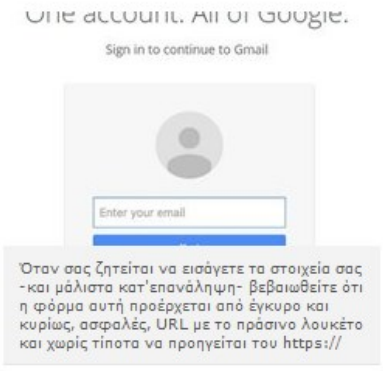
data:text/html στην αρχή της διεύθυνσης;

Υποκλοπή login/password στο Gmail από την προεπισκόπηση επισυναπτόμενων αρχείων

Δημοσίευση: 17 Μαρ 2017, 12:05 | Τελευταία ενημέρωση: 17 Μαρ 2017, 12:05



Όταν σας ζητείται να εισάγετε τα στοιχεία σας -και μάλιστα κατ'επανάληψη- βεβαιωθείτε ότι η φόρμα αυτή προέρχεται από έγκυρο και κυρίως, ασφαλές, URL με το πράσινο λουκέτο και χωρίς τίποτα να προηγείται του https://

Στην ταχύτητα με την οποία διεκπεραιώνουμε τα e-mail μας ποντάρουν όσοι κακόβουλα εφαρμόζουν μια τεχνική υποκλοπής στοιχείων που είναι γνωστή από την αρχή του έτους. Ο χρήστης κάνει κλικ στο εικονίδιο επισυναπτόμενου αρχείου στο Gmail για να δει, χωρίς να κάνει λήψη του αρχείου, το περιεχόμενό του. Αντί όμως της προεπισκόπησης, καλείται να εισάγει ξανά τα στοιχεία εισόδου του στην υπηρεσία. Το εικονίδιο του attachment είναι ένα screenshot έγκυρου προηγούμενου attachment και δεν πρόκειται για αρχείο περιεχομένου.

Πολλοί, ακόμα και οι πλέον ενημερωμένοι χρήστες, το κάνουν, θεωρώντας πως είναι μια απαίτηση ασφαλείας (ότι δηλαδή μόνο ο χρήστης με τα σωστά στοιχεία μπορεί να δει το περιεχόμενο του αρχείου).

Εντούτοις, η πανομοιότυπη σελίδα login στις υπηρεσίες της Google δεν φιλοξενείται σε ασφαλείς server της Google, αν και στη γραμμή διευθύνσεων του browser φαίνεται να προέρχεται από το έγκυρο https://accounts.google.com.

Από τη στιγμή που οι άγνωστοι λάβουν τα στοιχεία που πληκτρολόγησε ο χρήστης, μπαίνουν στο λογαριασμό τους και, μάλλον αυτοματοποιημένα, βρίσκουν ένα μήνυμα με attachment στα Απεσταλμένα, παίρνουν μια οθονιά του και το επισυνάπτουν σε νέο δόλιο μήνυμα με έγκυρη επικεφαλίδα και αποδέκτες όλους όσοι βρίσκονται στο βιβλίο επαφών, παραπέμποντας από την υποτιθέμενη προεπισκόπηση στην πλαστή σελίδα login από όπου θα υποκλέψουν τα στοιχεία των αποδεκτών που θα ξεγελαστούν.

Ένα από τα tips που γνωρίζουν οι πιο επιφυλακτικοί χρήστες είναι να κοιτούν τη γραμμή διευθύνσεων του browser, αναζητώντας μια έγκυρη διεύθυνση που ξεκινά με https://. Στην προκειμένη περίπτωση, προβάλλεται το https://accounts.google.com.

- Οι πιο προσεκτικοί διέκριναν πως **πριν από το https:// προηγείται το data:text/html** και στο (απομακρυσμένο) τέλος της διεύθυνσης ακολουθεί η παραπομπή σε ένα αρχείο που δεν είναι άλλο από την πλαστή σελίδα login στις υπηρεσίες της Google. Η σελίδα αυτή εμφανίζεται σε νέα καρτέλα όταν ο χρήστης κάνει κλικ στο επισυναπτόμενο αρχείο για να το δει σε προεπισκόπηση.

Μετά την αποκάλυψη της επιτυχημένης αυτής τεχνικής "phishing" (κατά το fishing, για το «ψάρεμα» στοιχείων), οι ειδικοί συνιστούν στους χρήστες να βεβαιώνονται ότι **δεν προηγείται τίποτα του https://** και ότι υπάρχει **το πράσινο κλειστό λουκέτο στην αρχή της γραμμής διευθύνσεων.**

Η Google έχει τροποποιήσει τον Chrome από τα τέλη Φεβρουαρίου 2017, στην έκδοση 56.0.2924 ώστε να εμφανίζει το μήνυμα **Not Secure** όταν χρησιμοποιείται αυτή η μέθοδος phishing.

- **Εάν χρησιμοποιείτε Chrome, ελέγξτε εάν έχετε την ενημερωμένη έκδοσή του**

Μπορείτε να δείτε από πού καταγράφηκε σύνδεση στο λογαριασμό σας στο Gmail -ή, άλλες υπηρεσίες της Google- διαβάζοντας το ακόλουθο άρθρο:

- **Πώς θα διακόψετε την πρόσβαση στο Google σας** από τη συσκευή που χάσατε ή, πώς θα διαπιστώσετε ότι κάποιος μπαίνει στο λογαριασμό σας από συσκευή που δεν αναγνωρίζετε ως δική σας

Ένα ακόμα συνηθισμένο φαινόμενο:

- **Πώς να κλείσετε το Facebook που αφήσατε ανοικτό σε ξένο υπολογιστή** ή, πώς θα διακόψετε την πρόσβαση τρίτου στο λογαριασμό σας

tech.in.gr