Κίνδυνοι: Υποκλοπή Προσωπικών Δεδομένων (Phishing)

Περιγραφή:

Υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών,ης κ.λπ). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα (cracker) να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς, κ.λπ.  
  
Κάποιοι θεωρούν τις Απάτες (Scams) ως ένα είδος υποκλοπής, μόνο που οι Απάτες συνήθως δεν ενδιαφέρονται για τις προσωπικές μας πληροφορίες, αλλά προσπαθούν να προκαλέσουν τον οίκτο μας για τον ανθρώπινο πόνο ώστε να προσφέρουμε λεφτά για να βοηθήσουμε ένα δήθεν καλό σκοπό. Για παράδειγμα, σχεδόν κάθε μεγάλη καταστροφή (σεισμός, πλημμύρες, πείνα, πόλεμος) έχει προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες να προσφέρουν λεφτά για να βοηθήσουν για κάποιο καλό σκοπό. Πολλοί άνθρωποι έχουν χάσει πολλά λεφτά για τέτοιους “καλούς” σκοπούς. Κάποιοι έχουν χάσει ακόμα και τη ζωή τους, καθώς έχουν ταξιδέψει σε άλλες χώρες για να γνωρίσουν αυτούς που επωφελούνταν των προσφορών τους.

|  |  |  |
| --- | --- | --- |
| Κίνδυνοι | Που μπορεί να συμβεί: | |
|  | Κίνδυνος | Μέσω ηλεκτρονικών μηνυμάτων (e-mail) που ξεγελούν το χρήστη ώστε να οδηγηθεί σε πλαστές ιστοσελίδες |
|  | Κίνδυνος | Κατά το φυλλομέτρημα οποιασδήποτε σοβαρής ιστοσελίδας, η οποία έχει μολυνθεί απο ιο |
|  | Κίνδυνος | Κατά τη περιήγηση σε ιστοσελίδες με αναληθή προϊόντα και πληροφορίες |
|  | Κίνδυνος | Κατά τη χρήση οποιουδήποτε φυλλομετρητή Διαδικτύου, ο οποίος έχει μολυνθεί με πρόγραμμα που καταγράφει προσωπικές και οικονομικές πληροφορίες, τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Τρόποι Αντιμετώπισης | Αντιμετώπιση: | |
|  | Αντιμετώπιση | Ελέγχουμε πάντοτε τον αποστολέα ενός μηνύματος και διερευνούμε την υπόστασή του |
|  | Αντιμετώπιση | Γνωρίζουμε ότι νόμιμοι φιλανθρωπικοί οργανισμοί συνήθως στέλνουν ηλεκτρονικές εκκλήσεις για βοήθεια μόνο σε ανθρώπους που το έχουν ζητήσει. Άλλες παρόμοιες εκκλήσεις, που σχεδόν πάντα ακολουθούν ένα μεγάλο καταστροφικό γεγονός, είναι συνήθως ψευδείς. Επισκεπτόμαστε την επίσημη ιστοσελίδα του οργανισμού για να επιβεβαιώσουμε την αξιοπιστία της έκκλησης |
|  | Αντιμετώπιση | Ελέγχουμε πάντα τη νομιμότητα φιλανθρωπικών ιδρυμάτων, αναζητώντας σχετικές επίσημες ιστοσελίδες (π.χ. http://www.charitynavigator.org) |
|  | Αντιμετώπιση | Τηλεφωνούμε ή πηγαίνουμε απευθείας στην ιστοσελίδα ενός φιλανθρωπικού οργανισμού και βρίσκουμε τρόπους να προσφέρουμε μέσω αυτής, αντί να απαντούμε και να κατευθυνόμαστε από εκκλήσεις-μηνύματα που παραλαμβάνουμε |
|  | Αντιμετώπιση | Δεν ενεργοποιούμε απερίσκεπτα συνδέσμους από μηνύματα αμφιβόλου προελεύσεως και περιεχομένου γιατί αυτά μπορούν να μας οδηγήσουν σε παράνομες ή επιβλαβείς ιστοσελίδες που μπορεί να μοιάζουν νόμιμες |
|  | Αντιμετώπιση | Αποφεύγουμε να δίνουμε προσωπικές πληροφορίες μέσω του Διαδικτύου. Είναι απίθανο μια τράπεζα ή ένας φιλανθρωπικός οργανισμός να ζητά τέτοιες πληροφορίες με αυτόν τον τρόπο |
|  | Αντιμετώπιση | Γνωρίζουμε ότι σοβαρές τράπεζες και επενδυτικοί οργανισμοί χρησιμοποιούν το πρωτόκολλο επικοινωνίας https αντί για http για ασφάλεια των προσωπικών δεδομένων των πελατών τους. Το “S” σημαίνει ασφαλές πρωτόκολλο. Η ασφάλεια αυτή διακρίνεται στη γραμμή διεύθυνσης μιας ιστοσελίδας (https://…… ) |
|  | Αντιμετώπιση | Όταν μας ζητηθεί να πληκτρολογήσουμε ένα ψευδώνυμο συνομιλίας, διαλέγουμε ένα όνομα που δεν προδίδει τα προσωπικά μας στοιχεία όπως το όνομα, το επίθετο, την ημερομηνία γέννησής μας, τον χώρο διαμονής κ.λ.π. |
|  |  |  |

Έλεξε τις γνώσεις σου με το **Tέστ Αυτο-αξιολόγησης**  
(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Ελλάδας)  
[](http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/SELF_ASSESSMENT_TEST/INDEX.HTML)