ΥΠΟΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Γεράσιμος Μοσχονάς

Υπεύθυνος Ασφαλείας Πληροφοριών Ομίλου Alpha Bank

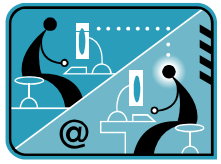
ΔΙΑΔΙΚΤΥΟ

Προσφέρει Πληθώρα Υπηρεσιών

- Αναζήτηση Πληροφοριών, Ανάγνωση ειδήσεων / νέων
- Εταιρική & Ατομική Παρουσίαση
- Ηλεκτρονικό Ταχυδρομείο
- Αγορά Προϊόντων / Ηλεκτρονικές Συναλλαγές
- Κοινωνικά Portals, On-Line συζητήσεις / Blogs

Αλλά ελλοχεύει και κινδύνους

- Απάτες
- Μετάδοση ιών & άλλου κακόβουλου λογισμικού
- Ιστοσελίδες με παράνομο περιεχόμενο
- Παραβίαση πνευματικών δικαιωμάτων
- Υποκλοπή προσωπικών δεδομένων



Στην Ελλάδα, περίπου 2,8 εκ. άτομα (18 ετών και άνω) είναι χρήστες του Διαδικτύου (Στοιχεία Ιουνίου 2008, Πηγή: Metron Analysis)

ΥΠΟΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Προσωπικά Δεδομένα

- Αρ. Τραπεζικών Λογ/σμών & Καρτών, Ταχυδρομικές & Ηλεκτρονικές Διευθύνσεις, Κωδικοί Πρόσβασης, …

↓

Κλοπή Ταυτότητας (Identity Theft)

Πως διαρρέουν

- Οι ίδιοι οι χρήστες τα δίνουν σε sites (π.χ. αγορά προϊόντων, εγγραφή σε ενημερωτικά έντυπα, κοινωνικά Portals). Μπορούν κατόπιν να κλαπούν από εκεί ή νόμιμα να δοθούν σε άλλους τρίτους, με τη συναίνεση του χρήστη
- Υποκλέπτονται εν αγνοία των χρηστών (phishing, malware, pharming, πλαστές ιστοσελίδες, …)

ΥΠΟΚΛΟΠΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σκοπός το οικονομικό όφελος από

- την πώληση των δεδομένων σε τρίτους
  - Αρ. Καρτών $ 0,5 – 5
  - Αρ. Λογ/σμών $ 30 – 400
  - Email passwords $ 1 – 340
  - Email διευθύνσεις $ 2 – 4 / MB

- την ιδία χρήση, προσποιούμενοι τους πραγματικούς χρήστες π.χ. πρόσβαση σε τραπεζικούς λογαριασμούς μέσω e-banking, αγορά προϊόντων.

Τα …. Προβλήματα

Malware

Legitimate Site

Spoof Site

Spam

Pharming

Phishing

Spyware

Virus

Worm

Trojan Horse

Cross Site Scripting

Spam & Phishing …

- Spam : Ανεπιθύμητα Μηνύματα που αποστέλλονται μαζικά με περιεχόμενο σχετικό με διαφημίσεις, αγορά προϊόντων, τυχερά παιχνίδια, οικονομικές υπηρεσίες, τρόπους για αύξηση του εισοδήματος, υλικό για ενήλικες, …
  - Το 2007, το 73% των μηνυμάτων ήταν spam. Κάθε δευτερόλεπτο στέλνονται κατά μ.ο. περίπου 15 spam μηνύματα, 70 ανά χρήστη την ημέρα.
- Phishing : Είδος spam μηνυμάτων που δείχνουν να προέρχονται από αξιόπιστες πηγές και αποσκοπούν στην εξαπάτηση του χρήστη και την υποκλοπή προσωπικών του δεδομένων.
  - Το 95% των στόχων αφορούν Τράπεζες και Οικονομικά Ιδρύματα (στοιχεία 1ου εξαμήνου 2008).

Phishing …

Είδη Phishing :

- Μηνύματα που εμφανίζονται να προέρχονται από Τράπεζες και ζητούν από το χρήστη για λόγους ασφαλείας να επιβεβαιώσει / δώσει προσωπικά του στοιχεία, οδηγώντας τον μέσω ενός συνδέσμου σε πλαστό site.
- Μηνύματα που προσφέρουν στο χρήστη κέρδη από λοταρίες, μέρος κληρονομιάς, αποδέσμευση χρημάτων από τραπεζικούς λογαριασμούς, συμμετοχή σε επενδύσεις κ.λπ.
- Μηνύματα που αποστέλλονται από «φίλους» ή «εταιρίες» και προτρέπουν το χρήστη να πατήσει ένα link ή να ανοίξει / εκτελέσει το αρχείο που επισυνάπτεται σε αυτά (mp3 ή video γνωστού καλλιτέχνη, ένα report για θέματα ασφαλείας κ.λπ.).

Phishing …

Δείγμα μηνύματος

<<Dear Customer,

During the last maintenance on our systems, we lost some data which caused errors on the account of some of our customers, which you appear to be one of them.
In order to prevent you from having problems in accessing your account and also in order to ensure that these errors are fixed, we have decided to recollect your data so as to enable us fix the problem and update our database(s) with your correct information.
You are required to follow the link below and provide us with all required information(s)

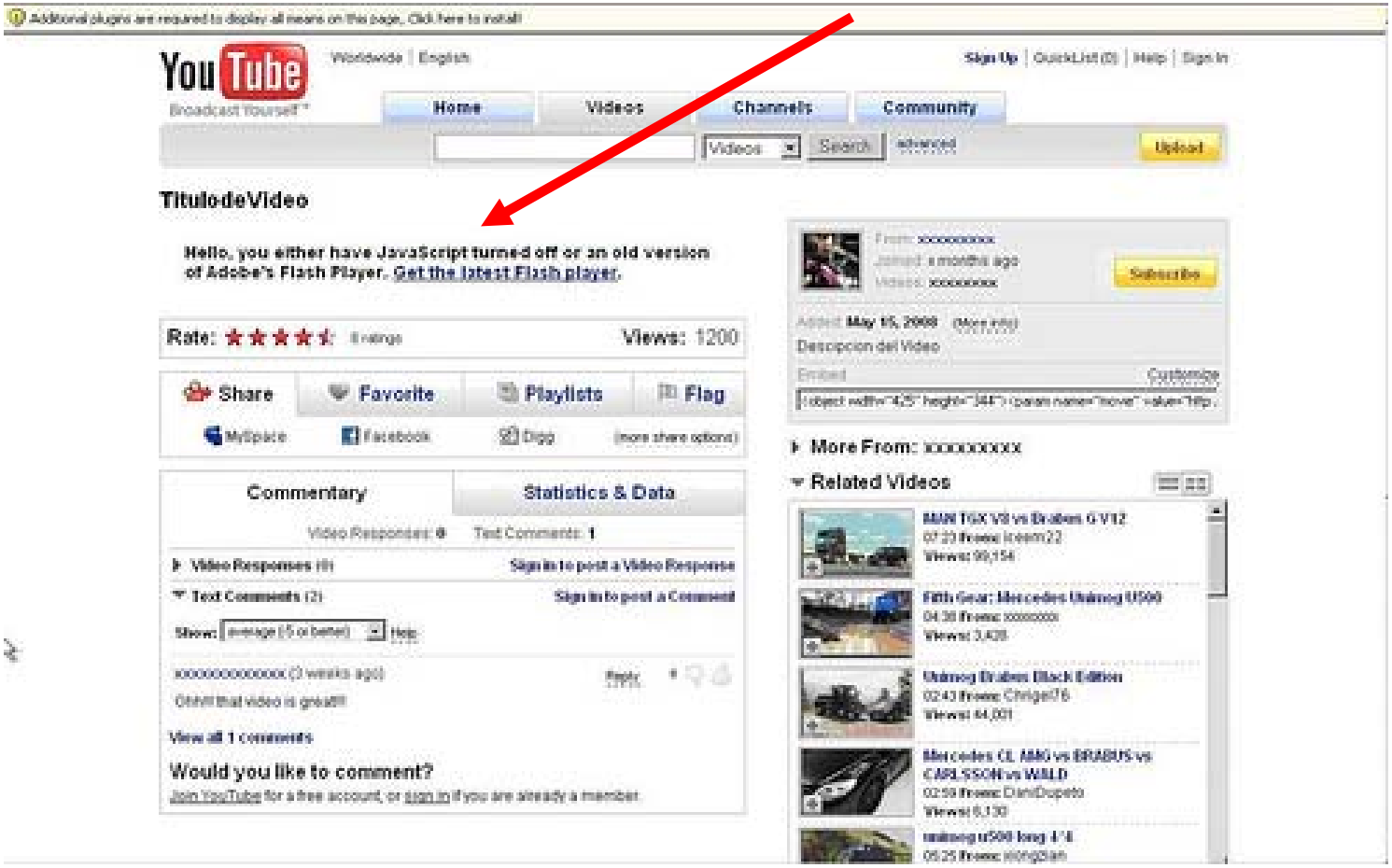
Click here

We apologise for any inconvenience this might have caused you. Thank you for your co-operation.
On-line Banking Service
Prime Bank>>

- Τα Phishing πλέον γίνονται πιο έξυπνα, χρησιμοποιούνται εξελιγμένες τεχνικές, προσομοιώνουν τον πραγματικό αποστολέα και είναι στοχευμένα
  - Σε ομάδες χρηστών (π.χ. σε μέλη ενός κοινωνικού portal)
  - Σε συγκεκριμένες χώρες (το ίδιο μήνυμα αυτόματα στην κάθε τοπική γλώσσα, αναλόγως από που προέρχεται ο χρήστης).
- Το 1ο τρίμηνο του 2008 εμφανίστηκαν >80.000 νέα phishing sites.

Phishing

Το παράδειγμα με το YouTube (Σεπτ. 2008)



Pharming

- Είδος απάτης με σκοπό να οδηγήσει / εκτρέψει το χρήστη σε πλαστή σελίδα, ενώ αυτός νομίζει ότι βρίσκεται στην πραγματική.
- **Traffic redirectors**
  - Αλλάζουν τις παραμέτρους στον DNS Server ή τις παραμέτρους στο τερματικό του χρήστη και για επιλεγμένα sites, ο χρήστης οδηγείται σε αντίστοιχα πλαστά.
- **Banker Trojans**
  - Εγκατάσταση Trojan στο τερματικό του χρήστη & λίστας με τραπεζικά sites
  - Όταν ο χρήστης πληκτρολογήσει ένα από αυτά, ενεργοποιείται το Trojan και εκτρέπει το χρήστη σε πλαστό site
  - Ακόμα και η διεύθυνση στον browser δείχνει π[illegible]στή
  - Κατόπιν στο πλαστό site ο χρήστης δίνει τα [illegible]εία του τα οποία και υποκλέπτονται.

Τα πιο εξελιγμένα Banker Trojans αν[illegible]
πιο δύσκολα.

Παραβίαση σε ιστοσελίδες …

iFrame

- Εκμεταλλευόμενοι οι κακόβουλοι κενά ασφαλείας, εγκαθιστούν κώδικα (iFrame) σε σελίδες ενός νόμιμου site.
- Κάθε φορά που το επισκέπτεται κάποιος χρήστης, ο κώδικας ενεργοποιείται και μπορεί να
  - εκτρέπει το χρήστη σε πλαστή σελίδα
  - αντιγράφει τα στοιχεία που δίνει ο χρήστης και τα αποστέλλει σε κακόβουλο site
  - εκτελεί πρόγραμμα που κατεβάζει malware στο τερματικό του χρήστη (π.χ. Italian Job)
  - οδηγεί σε παράνομο site που ελέγχει το τερματικό του χρήστη και, αναλόγως των κενών ασφαλείας που ανιχνεύει, του εγκαθιστά το ανάλογο malware.
- Τον Μάιο 2008, 200.000 σελίδες μολύνθηκαν μαζικά με τύπου iFrame κώδικα.

Παραβίαση σε ιστοσελίδες …

Κοινωνικά Portals (Social Networking)

MySpace

- Διαφημιστικό Banner στο MySpace περιείχε κώδικα που εκμεταλλευόταν κενό ασφαλείας του Internet Explorer.
- Video καλλιτέχνη περιείχε κώδικα που οδηγούσε το χρήστη σε πλαστό site και κατέβαζε malware στο τερματικό του.

Facebook

- Στο Wall του Facebook, που χρησιμοποιείται από μέλη για ανταλλαγή μηνυμάτων, video, φωτογραφιών κ.λπ., τοποθετήθηκε μήνυμα από «φίλο» που καλεί τα μέλη να πατήσουν το link και να δουν σχετικό video από το Google.
- Ο χρήστης οδηγείται σε ένα πλαστό site που τον καλεί να κατεβάσει μία νέα έκδοση του Flash Player.
- Αντί αυτού, ένα malware κατεβαίνει στο τερματικό του.

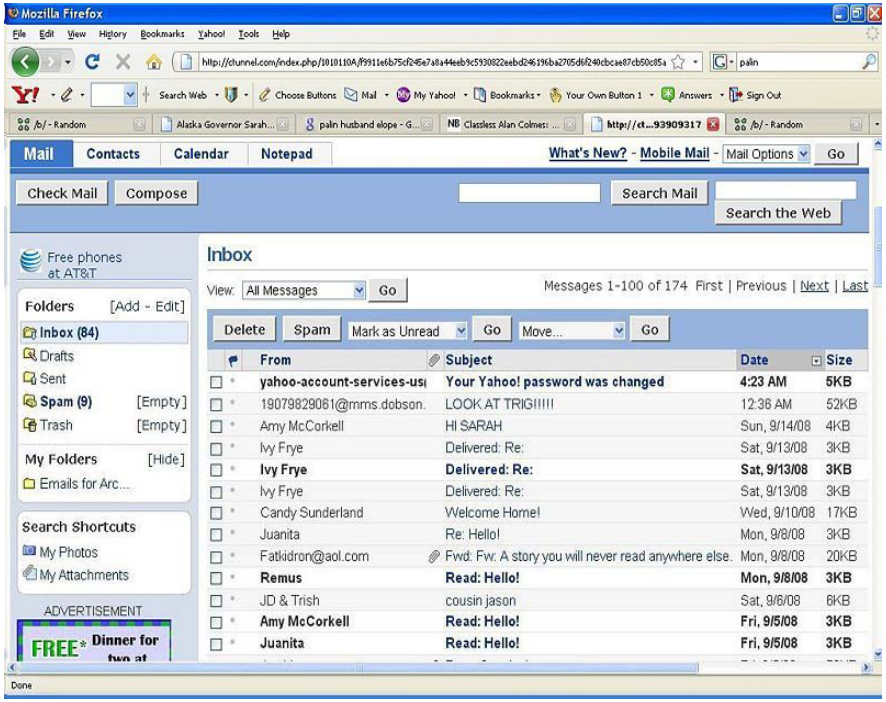
Webmail (Google, Hotmail, Yahoo)

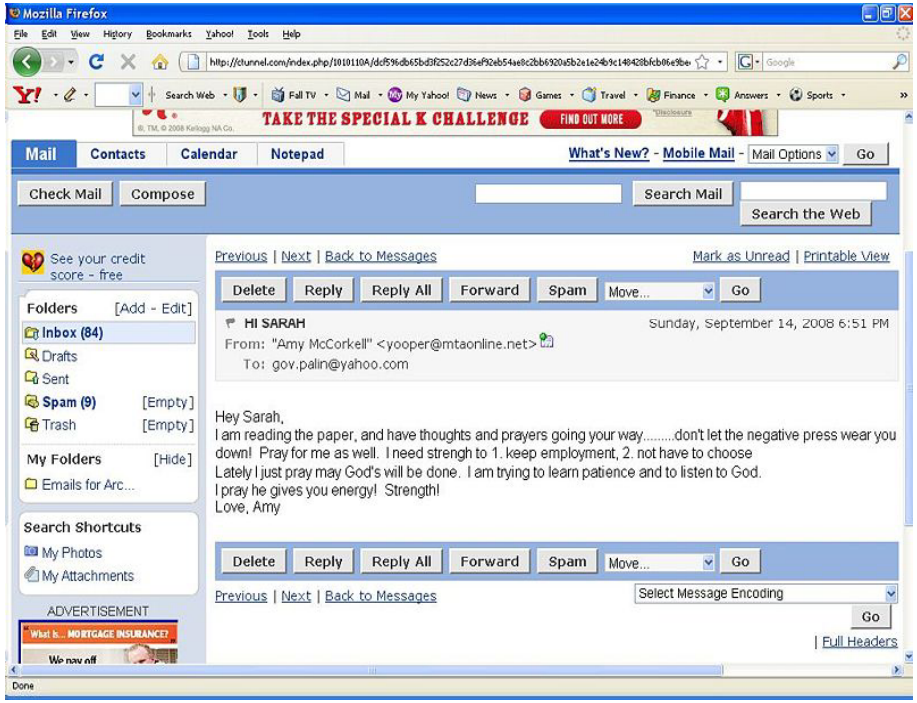
- Εύκολο να γίνει reset το password και να αποκτήσει κάποιος πρόσβαση στο λογαριασμό e-mail του χρήστη.
- Πρόσφατα, παραβιάστηκε το webmail της κ. Palin.

Παραβίαση σε ιστοσελίδες

Οθόνες από το ηλεκτρονικό ταχυδρομείο της Palin….

δημοσιευμένες ελεύθερα στο site WIKILEAKS





Συμβουλές για την προστασία μας ….

- ☑ Προσέχουμε που δίνουμε προσωπικά μας στοιχεία και που συναινούμε να δοθούν.
- ☑ Αγνοούμε και διαγράφουμε αμέσως «ύποπτα» e-mail που μας προτρέπουν να δώσουμε προσωπικά μας στοιχεία, περιέχουν συνδέσμους (links) ή συνημμένα αρχεία. Ενημερώνουμε άμεσα την Τράπεζά μας για τέτοια γεγονότα.
- ☑ Δεν αποκαλύπτουμε τους προσωπικούς μας κωδικούς σε άλλους τρίτους (στη Τράπεζά μας, σε φορείς κ.λπ.) για κανένα λόγο.
- ☑ Δεν επιλέγουμε εύκολα προβλέψιμους κωδικούς, τους φυλάσσουμε δε με τρόπο που να μην είναι δυνατή η υποκλοπή τους και βεβαίως όχι στον browser.
- ☑ Δεν χρησιμοποιούμε κοινό κωδικό σε όλο το Διαδίκτυο, ούτε τους ίδιους κωδικούς με αυτούς που χρησιμοποιούμε στην εργασία μας ή για πρόσβαση σε υπηρεσίες (π.χ. ATM), ενώ φροντίζουμε να τους αλλάζουμε συχνά.

Συμβουλές για την προστασία μας

- ☑ Πληκτρολογούμε οι ίδιοι την ιστοσελίδα που θέλουμε να πάμε και όχι να οδηγούμαστε μέσω συνδέσμων που βρίσκονται σε sites ή σε e-mail.
- ☑ Χρησιμοποιούμε προγράμματα προστασίας (antivirus, antispyware, firewall) στον υπολογιστή μας και τα ενημερώνουμε με τις πιο πρόσφατες εκδόσεις τους.
- ☑ Εγκαθιστούμε τις τελευταίες εκδόσεις του λειτουργικού συστήματος στον υπολογιστή μας.
- ☑ Αποφεύγουμε να χρησιμοποιούμε για ηλεκτρονικές συναλλαγές υπολογιστές σε Internet Cafe, δημόσιους χώρους ή τρίτων.
- ☑ Βεβαιωνόμαστε για την ασφάλεια του site, ελέγχοντας τη διεύθυνσή του (να είναι σωστά γραμμένη και να αρχίζει με *HTTP**S)*** και το λουκετάκι στον browser.
- ☑ Ενεργοποιούμε το φίλτρο προστασίας για το phishing στον browser.
- ☑ Κατεβάζουμε προγράμματα & αρχεία μόνο από γνωστά sites.

Η Ασφάλεια είναι Υπόθεση Όλων μας

Πρόσφατη έρευνα στις ΗΠΑ & Βρετανία έδειξε ότι το 88% των ερωτηθέντων θεωρούν ως κύρια αιτία της υποκλοπής των δεδομένων τους την προσωπική ανευθυνότητα. Πολλοί χρήστες δεν αντιλαμβάνονται την αυξανόμενη απειλή του οργανωμένου εγκλήματος στο Διαδίκτυο, ενώ ένας στους δύο χρησιμοποιεί τον ίδιο κωδικό για όλες τις υπηρεσίες στο Διαδίκτυο.

- Πάροχοι Υπηρεσιών Διαδικτύου (ISPs)
- Εταιρίες / Οργανισμοί που προσφέρουν διαδικτυακές υπηρεσίες προς την πελατεία τους (Τράπεζες, Δημόσιος Τομέας, Έμποροι κ.λπ.)
- Χρήστες

ΠΡΟΛΗΨΗ

Ανάλογα με το ρόλο μας, όλοι έχουμε ευθύνη να ενημερωνόμαστε για τις νέες απειλές και να λαμβάνουμε τα κατάλληλα μέτρα.