Εργασία στο πρόγραμμα επιμόρφωσης εκπαιδευτικών: «ΒΙΩΜΑΤΙΚΕΣ ΔΡΑΣΕΙΣ: Αυτογνωσία - Αυτοεκτίμηση – Λήψη Απόφασης – Διαχείριση Συγκρούσεων»

Κόντος Οδυσσέας ΠΕ12.04

ΕΠΟΠΤΗΣ**: ΑΡΓΥΡΟΠΟΥΛΟΥ ΜΑΡΙΑ** ΣΧΟΛΙΚΟ ΕΤΟΣ**: 2013-2014**

Τίτλος: « Να συστηθώ….» – «Δε χρειάζεται… σε ξέρω!»

Θεματική ενότητα: Οι κίνδυνοι στο διαδίκτυο

Θέμα: έκθεση προσωπικών δεδομένων στο διαδίκτυο

ΣΧΕΔΙΟ ΜΑΘΗΜΑΤΟΣ

1. Προβληματική

Ίσως ο τίτλος της εργασίας να ήταν συνήθης στην περίπτωση ενός επώνυμου προσώπου, όμως σε ότι αφορά τα διαδικτυακά δεδομένα, ισχύει ολοένα και περισσότερο στην περίπτωση «ανώνυμων» προσώπων. Το διαδίκτυο αποτελεί πλέον ένα ευρύ πεδίο γρήγορης εξυπηρέτησης, συναλλαγών, κοινωνικών δικτυώσεων και συνεπώς η ανάρτηση προσωπικών δεδομένων είναι πλέον αναγκαία και απαραίτητη. Όμως η αλματώδης εξέλιξη της μετάδοσης της πληροφορίας επιφέρει παράλληλα και εξέλιξη στους τρόπους υποκλοπής των δεδομένων αυτών. Το πρόβλημα μεγεθύνεται καθώς τα προσωπικά δεδομένα είναι άρρηκτα συνδεμένα με την ίδια μας την αυτοεικόνα ως μέλη μιας κοινωνικής ομάδας και συνεπώς κάθε μορφή υποκλοπής ή διαστρέβλωσης τους, πέρα από εξαπάτηση, ενδεχομένως οδηγήσει ακόμα και σε απαξίωση από τους «σημαντικούς άλλους» που τόσο επιθυμούμε δίπλα μας.

2. Θεωρητικό μέρος

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται και προσδιορίζει ένα άτομο, όπως τα στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κ.λπ.) τα φυσικά χαρακτηριστικά, τα ενδιαφέροντα, οι εργασιακές σχέσεις, οι φωτογραφίες , οι δραστηριότητες, οι συνήθειες, κ.α. Πέρα από τα προσωπικά δεδομένα υπάρχουν και ευαίσθητα δεδομένα όπως η φυλετική προέλευση, το πολιτικό φρόνημα, η θρησκευτική πεποίθηση, η ερωτική ζωή κλπ.

Το να δημοσιοποιεί κανείς προσωπικά δεδομένα θεωρείται ο πιο διαδεδομένος κίνδυνος στις ευρωπαϊκές χώρες *(greukidsonline.blogspot.com 18.07.2009)*. Οι κυριότερες πηγές απειλής προσωπικών δεδομένων

θεωρούνται τα δωμάτια ανοιχτής επικοινωνίας (chat rooms) και οι ιστοσελίδες κοινωνικής δικτύωσης (social networking sites). Στις τελευταίες η απειλή είναι διαρκώς αυξητική, γιατί εύκολα και απλά μπορούν να δημιουργηθούν τεράστιες βάσεις προσωπικών δεδομένων και προτιμήσεων από τις πληροφορίες που δημοσιεύουμε στο προφίλ μας, αλλά και από τη γενικότερη δραστηριότητά μας στην ιστοσελίδα. Τα στοιχεία αυτά χρησιμοποιούνται με πολλούς τρόπους.

Η βασική μορφή υποκλοπής των προσωπικών δεδομένων καλείται '*ψάρεμα'* ή *phishing*. Το phishing είναι η εξαπάτηση των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλειπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί.

Υπάρχουν 2 είδη phishing:

- *Social networking phishing*: Αντλώντας πληροφορίες και πολλά προσωπικά δεδομένα από τα προφίλ των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης, οι υποκλοπείς στέλνουν εξατομικευμένα μηνύματα που περιλαμβάνουν συνδέσμους προς ιστοσελίδες .[1]

- *Spear Phishing:* Πρόκειται για στοχευμένα μηνύματα που μοιάζουν αυθεντικά για κάποιες ομάδες ανθρώπων. Για παράδειγμα, στους υπαλλήλους μιας εταιρίας μπορεί να φτάσει μήνυμα με αποστολέα τον εργοδότη τους, στο οποίο τους απευθύνεται προσωπικά και τους ζητά όνομα χρήστη και κωδικούς πρόσβασης. Απαντώντας κανείς σε ένα μήνυμα spear phishing θέτει προσωπικές και συχνά απόρρητες πληροφορίες στη διάθεση των υποκλοπέων.[1]

Η επιτυχία του phishing είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες, το 70% όσων έλαβαν το εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιλαμβανόταν σε αυτό και συμπλήρωσε τα στοιχεία του στην ιστοσελίδα υποκλοπής δεδομένων.[2]

Προφανώς οι λόγοι που οι νέοι σήμερα εκθέτουν τόσο εύκολα τα προσωπικά τους δεδομένα είναι πολλοί. Η εξέλιξη της πληροφορίας , οι γρήγοροι ρυθμοί της ζωής, επιφέρουν έντονες κοινωνικές αλλαγές που οδηγούν τους νέους σε άλλους τρόπους προσωπικής προβολής, αποδοχής και καταξίωσης. Σε κάθε περίπτωση, οι γονείς και οι εκπαιδευτικοί δεν θα πρέπει να απορρίπτουν μια νέα – και καθιερωμένη πλέον – τάση αλλά να προτρέπουν προς τη σωστή ενημέρωση μέσα από συζήτηση και προβληματισμό.

3. Στόχοι

Οι διδακτικοί στόχοι εστιάζονται στο

- να χρησιμοποιούν οι μαθητές τα προσωπικά και τα ευαίσθητα δεδομένα τους ορθολογικά.
- να διαπιστώσουν τους κίνδυνους της αλόγιστης χρήσης προσωπικών δεδομένων ιδιαίτερα σε σελίδες κοινωνικής δικτύωσης.
- να διακρίνουν περιπτώσεις υποκλοπής δεδομένων.
- να αντιμετωπίζουν με σκεπτικισμό κάθε περίπτωση εισαγωγής ή προώθησης προσωπικών δεδομένων.

4. Σχέδιο μαθήματος – περιγραφή βιωματικών δραστηριοτήτων

Η προσπάθεια επίτευξης των παραπάνω διδακτικών στόχων θα γίνει με δύο βιωματικές δραστηριότητες. Η κάθε δραστηριότητα περιλαμβάνεται σε μία σχολική ώρα.

---

[1] *Safe internet- Το αλφαβητάρι του διαδικτύου. Ανασύρθηκε στις 20 Δεκεμβρίου2013 από: http://www.saferinternet.gr*

[2] *Safe internet- Το αλφαβητάρι του διαδικτύου. Ανασύρθηκε στις 20 Δεκεμβρίου2013 από: http://www.saferinternet.gr*

4α. Βιωματική δραστηριότητα Νο1*: Το ταξίδι μιας εικόνας…*

1η σχολική ώρα

Α. Εισαγωγή – χρόνος δημιουργίας κατάλληλου μαθησιακού κλίματος –οδηγίες . *(χρόνος: 3 λεπτά).*

Β. Δραστηριότητα

Αρχική κατάσταση: οι μαθητές κάθονται σε κύκλο.

i. Οι μαθητές καλούνται να ζωγραφίσουν μια εικόνα. Προϋπόθεση στην ζωγραφιά είναι να περιλαμβάνεται και ο εαυτός του μαθητή (υπό μορφή ενός ανθρώπινου σκίτσου). Η εικόνα μπορεί να απεικονίζει μια απλή παραμονή τού μαθητή σε κάποιο τοπίο, μια δραστηριότητά του, ή μπορεί να υποδηλώνει μια προσωπική του στιγμή ή μια πτυχή τού συναισθηματικού του κόσμου. Κάτω από τη ζωγραφιά ο μαθητής γράφει ένα συναίσθημα που χαρακτηρίζει την εικόνα του.

(χρόνος: 5 λεπτά).

ii. Οι μαθητές στη συνέχεια σηκώνονται και περπατούν άτακτα στο χώρο. Με εντολή του εκπαιδευτικού καλούνται να κάνουν ζευγάρι με αυτόν που εμπιστεύονται περισσότερο ή θεωρούν φίλο. Το ζευγάρια που δημιουργούνται, συζητούν μεταξύ τους τις εικόνες που κατασκεύασαν και στη συνέχεια τις ανταλλάσουν. Επίσης καλούνται να γράψουν ένα δεύτερο συναίσθημα για την εικόνα του φίλου τους ακριβώς κάτω από το πρώτο.

(χρόνος: 5 λεπτά).

iii. Οι μαθητές σηκώνονται πάλι και περπατούν άτακτα στο χώρο με τη διαφορά ότι κάθε ένας που ακουμπά κάποιον άλλον, είναι υποχρεωμένος να του δώσει την εικόνα που μέχρι τώρα κρατούσε, παίρνοντας παράλληλα αυτή του άλλου. Με τον τρόπο αυτό οι εικόνες ανταλλάσουν πολλούς παραλήπτες (ο εκπαιδευτικός μπορεί να περιορίσει το χώρο αν κρίνει ότι δεν υπάρχει ικανοποιητική ανταλλαγή).

(χρόνος: 2 λεπτά).

iv. Οι μαθητές κάθονται πάλι σε κύκλο. Κάθε μαθητής γράφει δύο συναισθήματα ή μια κριτική στην εικόνα που έλαβε, κάτω από τις δύο προηγούμενες γραφές. Κατόπιν, σηκώνεται όρθιος δείχνει την εικόνα στην ολομέλεια, ασκώντας κριτική. Σε κάθε περίπτωση (θετικής ή αρνητικής κριτικής) ο δημιουργός της εικόνας έχει δικαίωμα να προβάλει ή να αντιπαραβάλλει τα επιχειρήματα του στον ‘άγνωστο παραλήπτη’.

(χρόνος: 10 λεπτά).

Γ. Συζήτηση (βλ παρακάτω): *(χρόνος: 10 λεπτά).*

4β. Βιωματική δραστηριότητα Νο2: *Το παιχνίδι των διαδικτυακών… θυμάτων*

2η σχολική ώρα

Α. Εισαγωγή – χρόνος δημιουργίας κατάλληλου μαθησιακού κλίματος –οδηγίες . *(χρόνος: 3 λεπτά).*

Β. Δραστηριότητα

Αρχική κατάσταση: οι μαθητές κάθονται σε κύκλο εκτός από έναν που και κάθεται στο κέντρο και παίζει το ρόλο του ‘κεντρικού server’

Απαιτούμενα εργαλεία: Ο εκπαιδευτικός έχει προκατασκευάσει κάρτες – ενέργειες με σκοπό την εισαγωγή προσωπικών δεδομένων για διαφορές κακόβουλες περιπτώσεις, καθώς και κάρτες απαντήσεων – συνεπειών για κάθε ενέργεια (βλ. παράρτημα). Σε κάθε κάρτα – ενέργεια και την απάντησή της, αναγράφεται ένας κοινός κωδικός για ευκολία στην αντιστοίχηση. Προφανώς οι κάρτες με τις απαντήσεις τους, πρέπει να καλύπτουν τον αριθμό των μαθητών του τμήματος .

Το παιχνίδι

i. Οι μαθητές υποτίθεται ότι ‘σερφάρουν ’ στο διαδίκτυο. Ο ‘server’ τους μοιράζει από μια κάρτα – ενέργεια στην οποία περιγράφεται μια κατάσταση που οδηγεί κάθε φορά σε μια φόρμα εισαγωγής δεδομένων (π.χ. όνομα, διεύθυνση, e mail, αριθμός τραπεζικού λογαριασμού, κωδικός μέλους ιστότοπων κοινωνικής δικτύωσης ή διαδικτυακών συναλλαγών κλπ). Οι μαθητές εισάγουν τα δεδομένα τους συμφώνα με τη φόρμα.

(χρόνος: 5 λεπτά).

ii. Στη συνέχεια, κάθε μαθητής σηκώνεται και ‘στέλνει’ την πληροφορία στο μαθητή – server, ο οποίος του δίνει επιπλέον την αντίστοιχη κάρτα – συνέπεια διπλωμένη. Αυτό γίνεται μέχρι όλοι οι μαθητές λάβουν τις κάρτες – συνέπειες. Ο μαθητής διαβάζει την κάρτα – συνέπεια και καταγράφει 2 - 3 συναισθήματα που ένιωσε από αυτή.

(χρόνος: 7 λεπτά).

iii. Ο κάθε μαθητής διαβάζει τόσο την ενέργεια του όσο και τη συνέπεια στην ολομέλεια. Ο εκπαιδευτικός καταγράφει τα συναισθήματα στον πίνακα. Ακολουθεί συζήτηση και σχολιασμός της κάθε κατάστασης.

(χρόνος:15 λεπτά).

Γ. Ανακεφαλαίωση – κλείσιμο – αυτοαξιολόγηση

(χρόνος:10 λεπτά).

5. Ώρα για συζήτηση

Θεωρείται σκόπιμο η συζήτηση να γίνεται μετά το τέλος κάθε βιωματικής δραστηριότητας και όχι μετά το τέλος όλων ώστε να εκφράζεται άμεσα κάθε προβληματισμός.

Η πρώτη δραστηριότητα στοχεύει στην διασπορά προσωπικών και ευαίσθητων δεδομένων (ζωγραφιά) σε σελίδες κοινωνικής δικτύωσης, ξεκινώντας από ένα φίλο (ζευγάρι) και καταλήγοντας σε άγνωστους παραλήπτες. Η κατά αντιπαράθεση συζήτηση αποστολέα – παραλήπτη με ταυτόχρονή καταγραφή - δημοσιοποίηση των συναισθημάτων, οδηγεί στην βέλτιστη δυνατή κατανόηση της έννοιας του ‘ιδεατού εαυτού’ μέσα από τα σχόλια και τις αποτιμήσεις των άλλων. Ο μαθητής με τον τρόπο αυτό αντιλαμβάνεται το μέγεθος που κάθε προσωπικό δεδομένο, με τη διάδοση του, μπορεί να επηρεάσει την αυτοεικόνα του και να αυξήσει ή να μειώσει την αυτοεκτίμηση του. Ερωτήματα που μπορούν να τεθούν στην ολομέλεια είναι μεταξύ άλλων:

- πώς νιώσατε με το «μοίρασμα» της προσωπικής σας εικόνας με ένα φίλο;
- πώς χαρακτηρίζετε τη μεταφορά της προσωπικής σας εικόνας σε έναν τυχαίο αποδέκτη;
- δεδομένου ότι εν γνώση σας η εικόνα σας έφτασε σε έναν ‘άγνωστο τρίτο’ γιατί ίσως σας ενοχλήσει μια αρνητική κριτική του;
- πιστεύετε ότι αυτός ο αποδέκτης θα χρησιμοποιήσει και με διαφορετικό τρόπο την εικόνα σας, πέρα από μια αρνητική κριτική;

Η δεύτερη βιωματική δραστηριότητα επικεντρώνεται περισσότερο στον έλεγχο της εισαγωγής προσωπικών δεδομένων ιδιαίτερα σε περιπτώσεις phishing. Η ερμηνεία κάθε διαφορετικού περιστατικού στην ολομέλεια, έχει σα σκοπό την απευθείας παροχή της σχετικής γνώσης στο μαθητή και στη συνέχεια τον προβληματισμό του, την ευαισθητοποίηση του και την αλλαγή της στάσης κα συμπεριφοράς του σε παρόμοιες καταστάσεις.

Οι ερωτήσεις που μπορούν να τεθούν στη συζήτηση είναι:

- Πως κρίνετε το κάθε περιστατικό phishing
- Πως νιώσατε ως θύμα;
- Τι διαφορετικό θα έπρεπε να κάνετε;

Κάτω από αυτό το πρίσμα μπορούν να προκύψουν νέες ερωτήσεις και θέματα προς συζήτηση όπως:

- Τι πρέπει να ελέγχουμε και με ποιον τρόπο ώστε να είμαστε σίγουροι για την ασφάλεια της ενέργειάς μας;

- Ποια είναι τα χαρακτηριστικά ενός ιστότοπου, από τα οποία μπορούμε να καταλάβουμε πόσο ασφαλής είναι;
- Πού μπορούμε να βρίσκουμε πληροφορίες για το τι είναι επικίνδυνο και τι όχι;
- Ποια από τα προσωπικά μας στοιχεία πρέπει να προστατεύουμε περισσότερο;
- Ποιες ενέργειες πρέπει να αποφεύγουμε στα περιβάλλοντα κοινωνικής δικτύωσης;
- Πώς μπορούμε να ενημερώσουμε και να ευαισθητοποιήσουμε τους φίλους μας και την οικογένειά μας;

6. Χρόνος υλοποίησης (σε διδακτικές ώρες)

Ο χρόνος υλοποίησης του σχεδίου μαθήματος ανέρχεται σε δύο διδακτικές ώρες με απαραίτητη προϋπόθεση να είναι διαδοχικές ώστε να υπάρχει συνέχεια στην όλη διαδικασία.

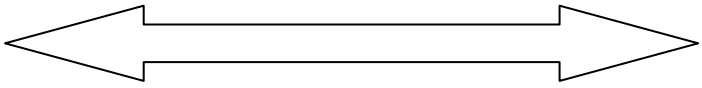
7. Απαιτούμενα υλικά

Τα υλικά που απατούνται είναι χαρτόνι, μαρκαδόροι, εκτυπωτής , φύλλα εκτύπωσης.

8. Ανακεφαλαίωση – αξιολόγηση

Είναι φανερό ότι σε κάθε προσπάθεια εφαρμογής βιωματικών δραστηριοτήτων υπάρχουν εμπόδια όπως χρονικοί περιορισμοί, έλλειψη εποπτικών μέσων ή πόρων κλπ. Το πιο σημαντικό όμως είναι το ισχύον μαθητικό δυναμικό δεν είναι εξοικειωμένο με αυτόν τον τρόπο διδασκαλίας. Το εκπαιδευτικό μας σύστημα παρ όλες τις προσπάθειες αλλαγής του έχει παγιωθεί στο τρίπτυχο καθηγητής – βιβλίο –αναλυτικό πρόγραμμα, μην αφήνοντας περιθώριο για εναλλακτικές δράσεις . Χρειάζεται αρκετή προσπάθεια από τον εκπαιδευτικό ώστε να απαγκιστρωθούν οι μαθητές, να αποκτήσουν ομαδοσυνεργατικό πνεύμα και να γίνουν μέρος της διδασκαλίας και όχι απλοί θεατές της. Όταν όμως γίνει αυτό το ενδιαφέρον είναι πλέον έκδηλο.

Αυτό ακριβώς φάνηκε και στην εν λόγω εκπαιδευτική διαδικασία. Αρχικά υπήρχε δυσκολία στην νέα προσαρμογή αλλά στη συνέχεια υπήρχε πνεύμα συμμετοχικότητας , δεκτικότητας και θετικών συναισθημάτων, ιδιαίτερα στην δεύτερη δραστηριότητα. Οι μαθητές έγιναν ενεργά μέλη εικονικών δρωμένων με αποτέλεσμα οι ίδιοι να οδηγηθούν στην επίτευξη των μαθησιακών στόχων μέσα από την ίδια τη συζήτηση και τη συμμετοχή. Το πνεύμα αυτό της αποδοχής στο νέο, στο καινοτόμο είναι που πρέπει να καλλιεργηθεί. Και εδώ ο εκπαιδευτικός καλείται να παίξει τον πραγματικό του ρόλο.



« Να συστηθώ….» – «Δε χρειάζεται… σε ξέρω!»

(έκθεση προσωπικών δεδομένων στο διαδίκτυο)

ΠΑΡΑΡΤΗΜΑ

Κωδικός: 01 /ενέργεια

Παρακαλούμε πατήστε στον παρακάτω σύνδεσμο και εισάγετε τα παρακάτω στοιχεία:

Επώνυμο: *Όνομα:*
Διεύθυνση: *ΤΚ:* *Πόλη /Χώρα*
Τηλ:
Αριθμός πιστωτικής κάρτας:

Κωδικός: 01 / συνέπεια

Ο λογαριασμός σας χρεώνεται μια ένα αρκετά μεγάλο ποσό αγνώστου παραλήπτη και κάθε προσπάθεια ανάκτησης είναι αδύνατη. Επιπλέον η Τράπεζα δεν αναλαμβάνει την ευθύνη, καθώς το προϊόν δεν είναι δικό της, επιφυλασσόμενη όμως να προσφύγει νομικά για υποκλοπή και παραχάραξη δεδομένων.

Κωδικός: 02 /ενέργεια

Σε email που λάβατε αναφέρεται ότι ο λογαριασμός σας στο PayPal θα διαγραφεί λόγω αλλαγής στους όρους χρήσης. Πατήστε : "get verified" ώστε να δώσετε τα παρακάτω στοιχεία:

E mail:

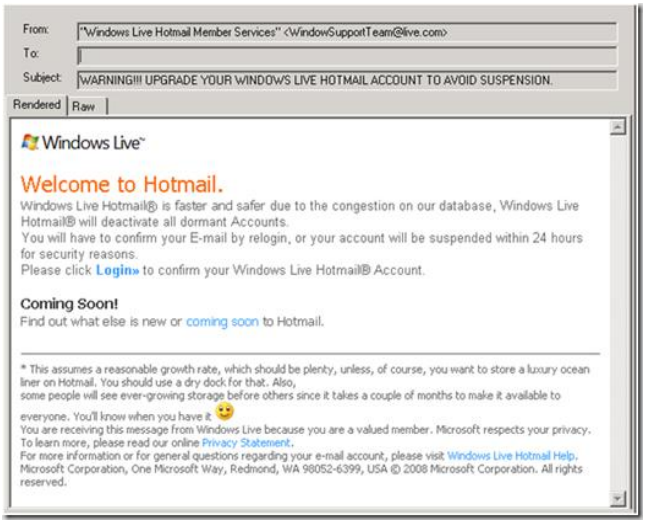
Pay Pal password:

Κωδικός: 02 /συνέπεια:

Ο τραπεζικός σας λογαριασμός είναι πλέον άμεσα προσβάσιμος σε κακόβουλο χρήστη και κάθε συναλλαγή σας μέσω PayPal είναι άκρως εκτεθειμένη με ότι αυτό συνεπάγεται.

Πηγή: http://howto.cnet.com/8301-11310_39-10396786-285/how-to-recognize-phishing-e-mails/

Κωδικός: 03 /ενέργεια



Λόγω αλλαγής στη βάση δεδομένων του windows mail θα πρέπει να πιστοποιήσετε εκ νέου το λογαριασμό σας. Παρακαλούμε κάνετε login και στη συνέχεια εισάγετε τα παρακάτω στοιχεία

E mail:

password:

Κωδικός: 03 /συνέπεια

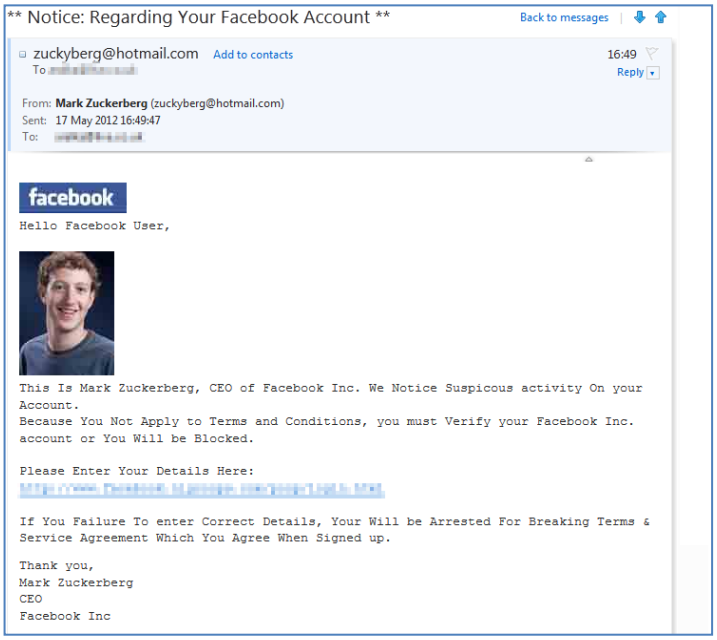
Το e mail σας στο windows life είναι πλέον προσβάσιμο σε κακόβουλο χρήστη. Αυτό σημαίνει ότι μπορεί όχι μόνο ότι είναι ορατό το περιεχόμενο της αλληλογραφίας σας, αλλά το e mail σας χρησιμοποιείται σε περιπτώσεις που προφανώς εσείς αγνοείτε.

Επίσης μερικές φράσεις που χρησιμοποιούνται με σκοπό να σας προτρέψουν για καταγραφή προσωπικών δεδομένων είναι: **"Verify your account." (πιστοποιήστε το λογαριασμό σας)** ή **"You have won the lottery." (Έχετε κερδίσει....)**ή **"If you don't respond within 48 hours, your account will be closed."(αν δεν απαντήσετε εντός48 ωρών ο λογαριασμός σας θα απενεργοποιηθεί)**

Αξίζει να σημειωθεί πως ένας καλός τρόπος να ανακαλύψετε αν πρόκειται για κακόβουλη διεύθυνση να σύρετε (προσοχή χωρίς να κάνετε κλικ) το ποντίκι του υπολογιστή σας πάνω στην «ψεύτικη επικαλυμμένη διεύθυνση και να δείτε την πραγματική που προφανώς ουδεμία σχέση έχει με αυτή που βλέπετε (βλ σχήμα).

Πηγή: http://www.microsoft.com/en-gb/security/online-privacy/phishing-symptoms.aspx

Κωδικός: 04



Ονομάζομαι Mark Zuckerberg και ως γνωστό είμαι ο κύριος ιδρυτής του Facebook. Έχουμε εντοπίσει ύποπτη δραστηριότητα στο λογαριασμό σας. Θα πρέπει να επιβεβαιώσετε το λογαριασμό σας στο Facebook αλλιώς ο λογαριασμός σας θα μπλοκαριστεί.
Παρακαλούμε πατήστε στον παρακάτω σύνδεσμο για να εισάγετε τα στοιχεία σας:
Όνομα:
Επώνυμο:
Διεύθυνση:
Πόλη /Χώρα
Τηλ:
e mail:
Facebook password:

Κωδικός: 04 / συνέπεια:

Ο κακόβουλος χρήστης (phisher) αποκτά πλέον πρόσβαση σε όλα σας τα προσωπικά δεδομένα στο Facebook. Επιπλέον οι χρήστες αυτοί αποκτούν κάθε δικαίωμα προώθησης των δεδομένων αυτών σε οποιονδήποτε άλλο χρήστη του facebook και για οποιονδήποτε σκοπό

Προσέξτε ότι ο ίδιος ο ιδρυτής του Facebook έχει στο e mail του επέκταση @hotmail.com !

Πηγή: http://edgis-security.org/spam-scams-and-social-engineering/phishing-email-from-zucky/

Κωδικός: 05 /ενέργεια

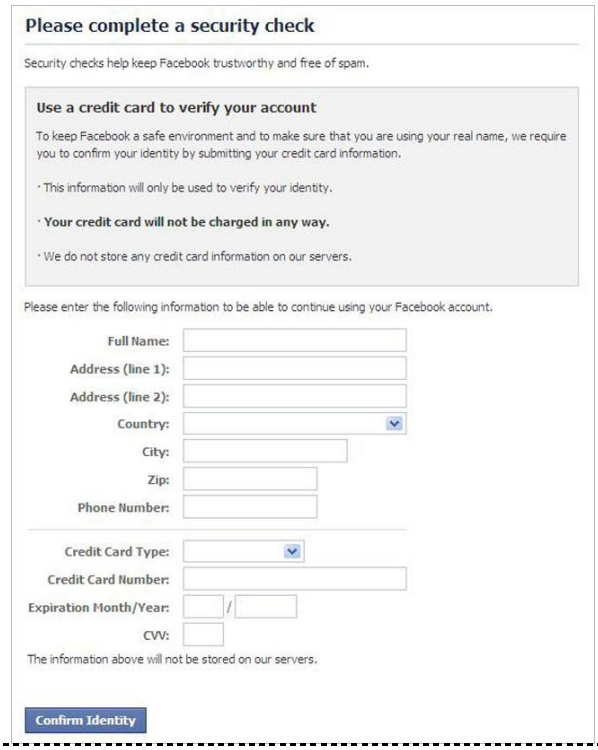
Ο Eric σας πρόσθεσε ως φίλο. Για να αποδεχτείτε ως φίλο πατήστε “add friend”

Εισάγετε τα στοιχεία σας
username:
password:

Κωδικός: 05 /συνέπεια:

Αν πατήσατε “add friend” θα οδηγηθείτε σε ένα περιβάλλον που μοιάζει με αυτό του Facebook και εισάγοντας τα δεδομένα σας (username and password), ο χρήστης (phisher) αυτόματα εγκαθιστά κακόβουλο λογισμικό στον υπολογιστή σας, το οποίο αποκτά πρόσβαση στα προσωπικά σας δεδομένα σε ότι αφορά κωδικούς εισαγωγής σε κάθε ιστοσελίδα που είστε μέλος (ακόμα και σε τράπεζες μέσω e banking)

Πηγή: http://ericallison.info/blog.php?article=phishing_identity_theft



Κωδικός: 06 /ενέργεια

Στην προσπάθεια μας να κρατήσουμε το Facebook εμπιστευτικό, και πέρα από κάθε κακόβουλη αλληλογραφία, θα θέλαμε να πιστοποιήσουμε την αυθεντικότητα της ταυτότητας σας, με τη εισαγωγή των παρακάτω στοιχείων της πιστωτικής σας κάρτας: (η πιστωτική σας δεν θα χρεωθεί για κανένα λόγο)

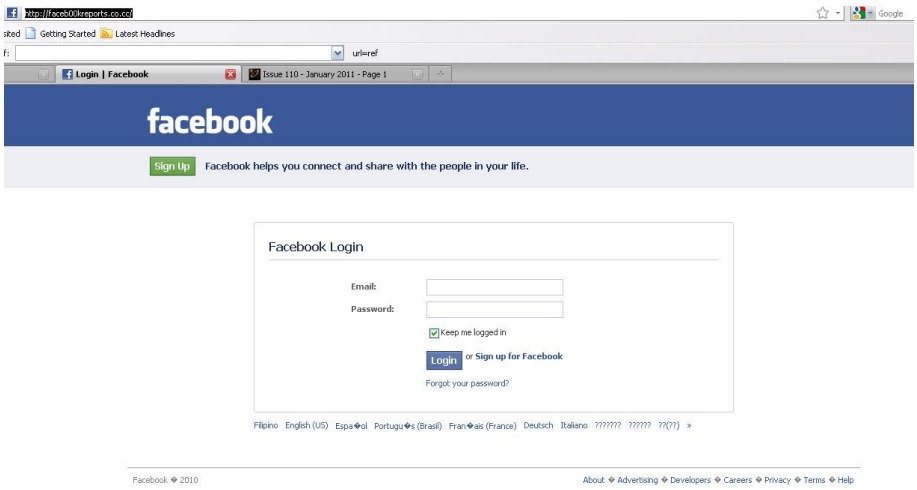
Όνομα:
Επώνυμο:
Διεύθυνση 1:
Διεύθυνση 2:
Πόλη /Χώρα
ΤΚ
Τηλ:
Αριθμός πιστωτικής κάρτας:
Ημερ/νία λήξης:
CVV:

Κωδικός: 06 / συνέπεια:

Με την εισαγωγή των παραπάνω δεδομένων η πιστωτική σας κάρτα θα χρησιμοποιηθεί για συναλλαγές εν αγνοία σας.

Πηγή: http://businesstoday.intoday.in/story/fake-facebook-security-page-phishing-scam-for-credit-card-info/1/194603.html

Κωδικός: 07 /ενέργεια



Σας έρχεται e mail που σας προτρέπει να μπείτε στο λογαριασμό σας στο Facebook.

Εισάγετε τα στοιχεία σας
username:
password:

Κωδικός: 07 /συνέπεια

Πρόκειται για μια προσπάθεια εισαγωγής δεδομένων (username και password), μέσω μια διαφορετικής διεύθυνσης (url) , με σκοπό την συλλογή του λογαριασμού σας στο facebook και κατ επέκταση των προσωπικών σας δεδομένων.
Προφανώς ο μόνος τρόπος εισαγωγής δεδομένων (username και password), είναι η κανονική διεύθυνση της ιστοσελίδας.

Πηγή: http://www.scamsniper.info/2010/12/another-facebook-phishing-attempt-going.html

Κωδικός: 08/ενέργεια

Λαμβάνετε e mail από ένα γνωστό σας φίλο ή οικογενειακό σας μέλος το οποίο σας στέλνει ένα αρχείο το οποίο ανοίγετε και έχει την παρακάτω φόρμα. Εισάγετε :

e mail:
password:

για να δείτε το αρχείο που σας εστειλαν

Κωδικός: 08 / συνέπεια:

Με την εισαγωγή των στοιχείων σας υποκλέπτονται οι λογαριασμοί του e mail σας, η αλληλογραφία σας είναι πλέον εκτεθειμένη και το e mail σας επιπλέον μπορεί ακόμα και να πωληθεί σε άλλους spammers.

Πηγή: http://www.onlinethreatalerts.com/article/2013/4/25/google-docs-phishing-email-scam/