ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΦΑΡΜΟΓΗ ANDROID ΓΙΑ ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ - PHISHING

Των φοιτητών

Πάσχου Θεοφάνη

Αρ. Μητρώου:093534,

Μάρκου Κωνσταντίνου **Επιβλέπων καθηγητής**

Αρ. Μητρώου: 093449 **Κλεφτούρης Δημήτριος**

Θεσσαλονίκη 2015

ΠΡΟΛΟΓΟΣ

Στην παρούσα πτυχιακή εργασία η οποία πραγματοποιήθηκε στο Αλεξάνδρειο Τεχνολογικό Ίδρυμα Θεσσαλονίκης, στο τμήμα Πληροφορικής της Σχολής Τεχνολογικών Εφαρμογών αναλύθηκαν και περιγράφονται τεχνικές ανάπτυξης εφαρμογών για smartphones και αναπτύχθηκε εφαρμογή με χρήση της πλατφόρμας Android SDK. Η εφαρμογή είναι ενημερωτική και έχει ως θέμα την ενημέρωση για την κλοπή ταυτότητας στο Διαδίκτυο(Phishing). Σκοπός της είναι η ενήμερωση των χρηστών του Internet για την απάτη του phishing έτσι ώστε να προστατευθούν από αυτή.

Οι λόγοι οι οποίοι μας οδήγησαν στην επιλογή αυτού του θέματος είναι η ανάγκη για ενημέρωση πάνω στο θέμα του Phishing παράλληλα με το μεγάλο ενδιαφέρον μας για την πλατφόρμα του Android του οποίου η ανάπτυξη είναι ραγδαία τα τελευταία χρόνια και καλύπτει ένα πολύ μεγάλο μέρος της αγοράς των smartphones, tablets, τηλεοράσεων και άλλων τεχνολογικών μέσων.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία αφορά την ανάπτυξη εφαρμογής κινητής τηλεφωνίας στην πλατφόρμα Android, με θέμα την ενημέρωση των χρηστών για την κλοπή ταυτότητας στο Διαδίκτυο(Phishing).

Αρχικά γίνεται μια εκτενής αναφορά στην πλατφόρμα του Android όπου δίνεται ο ορισμός του Android, παρουσιάζονται κάποια ιστορικά στοιχεία για την εξέλιξή του με την πάροδο του χρόνου και οι εκδόσεις του με τις δυνατότητές του. Επίσης έχουμε μια αναφορά στα βασικά χαρακτηριστικά της πλατφόρμας, την αρχιτεκτονική και την ασφάλεια την οποία παρέχει.

Στη συνέχεια παρουσιάζονται κάποια συστατικά τα οποία είναι απαραίτητα για να δημιουργηθεί μια ολοκληρωμένη Android εφαρμογή. Επιπρόσθετα, αναλύεται εκτενώς το θέμα της κλοπής ταυτότητας στο Διαδίκτυο(Phishing). Η ανάλυση περιλαμβάνει τους τρόπους εξάπλωσης αυτής της απειλής και προτείνονται μηχανισμοί αντιμετώπισης οι οποίοι καλύπτουν όλα τα επίπεδα προστασίας δήλαδη τη πλευρά προστασίας client-side, τη πλευρά προστασίας server-side και τη πλευρά προστασίας σε επίπεδο επιχειρήσεων.

Τέλος, γίνεται παρουσίαση της εφαρμογής η οποία υλοποιήθηκε περιγράφοντας τις λειτουργίες που χρησιμοποιούνται και της διαδικασίας ανάπτυξής της.

ABSTRACT

This project is about the development of a mobile application on Android platform, on user information about identity theft on the Internet (Phishing).

Initially an extensive report is made on the platform of Android where the definition of Android is given, presented some historical data on its evolution over time and some features of it's versions . Also, a reference is given to the main features of the platform, architecture and the security which it provides.

Afterwards, some features are presented that are necessary to create a complete Android application. In addition, there is an extensive discussion on the issue of the Internet Identity Theft (Phishing). The analysis includes the ways of this threat's spread and suggests response mechanisms that cover all levels of protection, as the protection side client-side, the server-side protection side and side protection at the enterprise level side.

Finally, it presents the application which was implemented by describing the functions used and its development process.

ΠΕΡΙΕΧΟΜΕΝΑ

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

ΚΕΦΑΛΑΙΟ 1

1 ΕΙΣΑΓΩΓΗ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ANDROID

1.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί το λειτουργικό σύστημα Android τα ιστορικά στοιχεία για την εξέλιξη του, οι εκδόσεις του και τα βασικά χαρακτηριστικά του τα οποία είναι απαραίτητα για να γίνει αντιληπτό το πώς λειτουργεί η πλατφόρμα στην οποία βασίζεται η συγκεκριμένη πτυχιακή εργασία.

1.2 Τι είναι το Android

Το Android είναι ένα λειτουργικό σύστημα το οποίο τρέχει τον πυρήνα του λειτουργικού Linux. Αναπτύσσεται από τη Google για smartphones και tablets, αλλά και για User Interfaces για τηλεοράσεις (Android TV), αυτοκίνητα (Android Auto), και ρολόγια χειρός (Android Wear). Επιτρέπει στους προγραμματιστές να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java, κάνοντας χρήση των βιβλιοθηκών λογισμικού που είναι ανεπτυγμένες από την Google. Το Android είναι το πιο ευρέως διαδεδομένο λογισμικό στον κόσμο και το λογότυπο του είναι ένα ρομπότ σε χρώμα πράσινου μήλου.

Σχήμα 1 Το λογότυπο του Android

1.3 Ιστορικά στοιχεία

Η Android Inc ιδρύθηκε το 2003 από τον Andy Rubin (συν-ιδρυτής της Danger), Rich Miner (συν-ιδρυτής της Wildfire Communications, Inc.), Nick Sears (παλαιότερα αντιπρόεδρος της T-Mobile), και Chris White (επικεφαλής του σχεδιασμού και της διασύνδεσης ανάπτυξης στην WebTV) με σκοπό να φτιάξει ένα λειτουργικό με πολλές δυνατότητες για ψηφιακές φωτογραφικές μηχανές. Σύντομα επειδή αυτή η αγορά ήταν ιδιαίτερα περιορισμένη αποφάσισαν να αλλάξουν στρατηγική και να αναπτύξουν ένα λειτουργικό για κινητά τηλέφωνα που θα μπορούσε να ανταγωνιστεί τις άλλες εταιρείες που ανέπτυσσαν λογισμικό για κινητά τηλέφωνα όπως Windows Phone και Symbian.

Η Android Inc σύντομα βρέθηκε να αντιμετωπίζει οικονομικές δυσκολίες και το 2005 η εταιρεία εξαγοράσθηκε από την Google, με σκοπό φυσικά η δεύτερη να μπει στον χώρο της κινητής τηλεφωνίας. Τα βασικά στελέχη της Android Inc παρέμειναν στην εταιρεία μετά την εξαγορά. Η Android Inc. εκείνη την εποχή λειτουργούσε κρυφά, αλλά πολλοί υποθέτανε ότι η Google σχεδιάζει να εισέλθει στην αγορά της κινητής τηλεφωνίας.

Το Νοέμβριο του 2007 ανακοινώθηκε ο συνεταιρισμός Open Handset Alliance, με πολλές εταιρείες στον χώρο της τεχνολογίας να συμμετέχουν σε αυτόν (Google, HTC, Sony, Samsung, Qualcomm, Texas Instruments, T-Mobile κτλ) με σκοπό την ανάπτυξη και εξέλιξη ανοιχτών προτύπων στις συσκευές κινητής τηλεφωνίας και παράλληλα παρουσιάστηκε και το νέο Mobile λειτουργικό "Android" βασισμένο στον πυρήνα του Linux. Επίσης τον Οκτώβριο του 2008 παρουσιάστηκε το πρώτο κινητό τηλέφωνο με λειτουργικό Android το HTC Dream.

Η συνέχεια για τη Google έγινε το 2010 με την ανακοίνωση τις σειράς συσκευών Nexus η οποία περιλαμβάνει κινητά τηλέφωνα αλλά και tablet. Το πρώτο κινητό τηλέφωνο ήταν το Nexus One κατασκευασμένο από την HTC και από τότε η σειρά των συσκευών Nexus χαρακτηρίζεται ως ναυαρχίδα του Android και είναι αυτή που πρώτη λαμβάνει την νέες ενημερώσεις και εκδόσεις του λειτουργικού της Google. Η τελευταία εξέλιξη ήταν το 2014 με το λανσάρισμα του πρώτου κινητού παραγωγής αποκλειστικά από την Google το Android One με λειτουργικό Android Lollipop 5.1.

Σχήμα 2 Android One

1.4 Οι εκδόσεις του Android

Η αρχή για τις εκδόσεις του Android έγινε με την beta έκδοση τον Νοέμβριο του 2007 και στη συνέχεια κυκλοφόρησε η πρώτη εμπορική έκδοση Android 1.0 τον Σεπτέμβριο του 2008. Η τελευταία έκδοση Lollipop 5.0 κυκλοφόρησε το Νοέμβριο του 2014 ενώ και η κάθε έκδοση έχει ένα όνομα εμπνευσμένο από ένα είδος γλυκού παρακάτω ακολουθεί μια παρουσίαση όλων των εκδόσεων με τα βασικά τους χαρακτηριστικά.

- Android 1.0 και Android 1.1

Η έκδοση 1.0 κυκλοφόρησε το 2008 με το πρώτο Android smart phone HTC Dream. Η έκδοση περιλάμβανε την εφαρμογή Android Market για την λήψη και αναβάθμιση εφαρμογών, την εφαρμογή Web browser για την προβολή HTML ιστοσελίδων όπως και βασικές εφαρμογές για τις υπηρεσίες της Google(όπως Gmail, Maps, YouTube player κλπ.).

- Android 1.5 “Cupcake”

Κυκλοφόρησε την άνοιξη του 2009 και ήταν το πρώτο που είχε όνομα γλυκού. Η ενημερωμένη έκδοση περιλάμβανε αρκετά νέα χαρακτηριστικά και τροποποιήσεις στο γραφικό περιβάλλον. Παρείχε υποστήριξη για «εικονικό»

πληκτρολόγιο με πρόβλεψη κειμένου και λεξικό για προσθήκη νέων λέξεων. Προστέθηκαν μικρές εφαρμογές που προστίθενται στην αρχική οθόνη και μπορούν να ανανεώνονται τακτικά ώστε να προβάλουν ενημερωμένο περιεχόμενο. Επίσης προστέθηκε η εγγραφή και η αναπαραγωγή βίντεο σε μορφή MPEG-4 και 3GP, η υποστήριξη για Bluetooth, η επιλογή για αυτόματη εναλλαγή προσανατολισμού και η δυνατότητα για upload περιεχομένου σε YouTube και Picasa.

- Android 1.6 “Donut”

Κυκλοφόρησε το φθινόπωρο του 2009 Οι λειτουργίες που περιλάμβανε ήταν η πολύγλωσση μηχανής σύνθεσης ομιλίας ,η βελτίωση της προβολής και της αναζήτησης στο Android Market η εφαρμογή Gallery για τη προβολή φωτογραφιών και βίντεο όπως και ταχύτερη πρόσβαση στη κάμερα, η υποστήριξη για ανάλυση οθόνης WVGA και η δυνατότητα οι προγραμματιστές να συμπεριλάβουν το περιεχόμενό τους στα αποτελέσματα αναζητήσεων.

- Android 2.0“Eclair”

Κυκλοφόρησε μόλις ένα μήνα μετά το Donut (φθινόπωρο 2009). Συμπεριελάμβανε υποστήριξη Bluetooth 2.1,καλύτερη ταχύτητα υλικού και ανανεωμένο UI, υποστήριξη για περισσότερα μεγέθη οθονών και αναλύσεων και ανανεωμένο UI στον Browser και υποστήριξη για HTML5.

- Android 2.2-2.2.3 “Froyo”

Κυκλοφόρησε την άνοιξη του 2010 είναι η πρώτη έκδοση του Android που υποστήριζε Adobe Flash και περιείχε βελτίωση της ταχύτητας μνήμης και της απόδοσης, βελτίωση της απόδοσης των εφαρμογών με χρήση JIT(Just In Time) compilation,βελτιωμένη υποστήριξη Microsoft Exchange,υποστήριξη εγκατάστασης εφαρμογών από εξωτερική μνήμη και υποστήριξη για οθόνες υψηλής πυκνότητας.

- Android 2.3-2.3.7 “Gingerbread”

Κυκλοφόρησε τον Δεκέμβρη του 2010 ήταν πολύ πιο γρήγορο και εύχρηστο από τις προηγούμενες εκδόσεις και έδινε στους δημιουργούς εφαρμογών μεγαλύτερες δυνατότητες όπως η προσθήκη Download Manager για ευκολότερη πρόσβαση στα ληφθέντα αρχεία η υποστήριξη για NFC, η βελτίωση στη διαχείριση της ενέργειας η υποστήριξη υπερμεγεθών διαστάσεων οθονών και αναλύσεων.

- Android 3.0-3.2 “Honeycomb”

Κυκλοφόρησε τον Φεβρουάριο του 2011 και ήταν διαθέσιμη μόνο για tablets. Υποστήριζε επεξεργαστές πολλών πυρήνων και περιλάμβανε τη προσθήκη Μπάρας συστήματος και Μπάρας ενεργειών για να γίνουν πιο εύχρηστες οι λειτουργίες του.

- Android 4.0-4.0.2 “Ice Cream Sandwich”

Κυκλοφόρησε τον Οκτώβρη του 2011 και έφερε πολλές αλλαγές στο λειτουργικό σύστημα. Μερικές από αυτές είναι η δυνατότητα χρήσης κουμπιών πάνω στην οθόνη (πίσω, αρχική, κλπ) ενώ μέχρι τότε όλα τα κινητά είχαν εξωτερικά κουμπιά. Άλλες δυνατότητες ήταν το Face Unlock, καλύτερη χρήση των φωνητικών εντολών, αναδιαμόρφωση του περιβάλλοντος χρήσης, δυνατότητα λήψης βίντεο 1080p και είναι η πρώτη έκδοση με browser Google chrome.

- Android 4.1-4.2 “Jelly Bean”

Κυκλοφόρησε τον Ιούνιο του 2012.Είχε μεγάλη βελτίωση στο γραφικό περιβάλλον χρήσης και η απόκρισή του ήταν πιο γρήγορα και καλοφτιαγμένα, περιλάμβανε βελτιώσεις στην κάμερα στην οθόνη κλειδώματος, υποστήριζε αναλύσεις 4K και Open GLES 3.0.

- Android 4.4 “Kit Kat”

Το Android 4.4 ονομάζεται Kit Kat κυκλοφόρησε τον Οκτωβρίου 2013 και φυσικά θα διαφημίζει το ομώνυμο σοκολατένιο προϊόν. Το Android 4.4 Kit Kat είναι εμφανώς απλούστερο από την προηγούμενη έκδοση, όμως δεν έχει πολύ μεγάλες αλλαγές. Οι αλλαγές εντοπίζονται στη δυνατότητα να αλλαγής τραγουδιού χωρίς ξεκλείδωμα της συσκευής, στα βελτιωμένα γραφικά παιχνιδιών, στη βελτίωση των τεχνολογιών Bluetooth Wi-Fi και NFC .

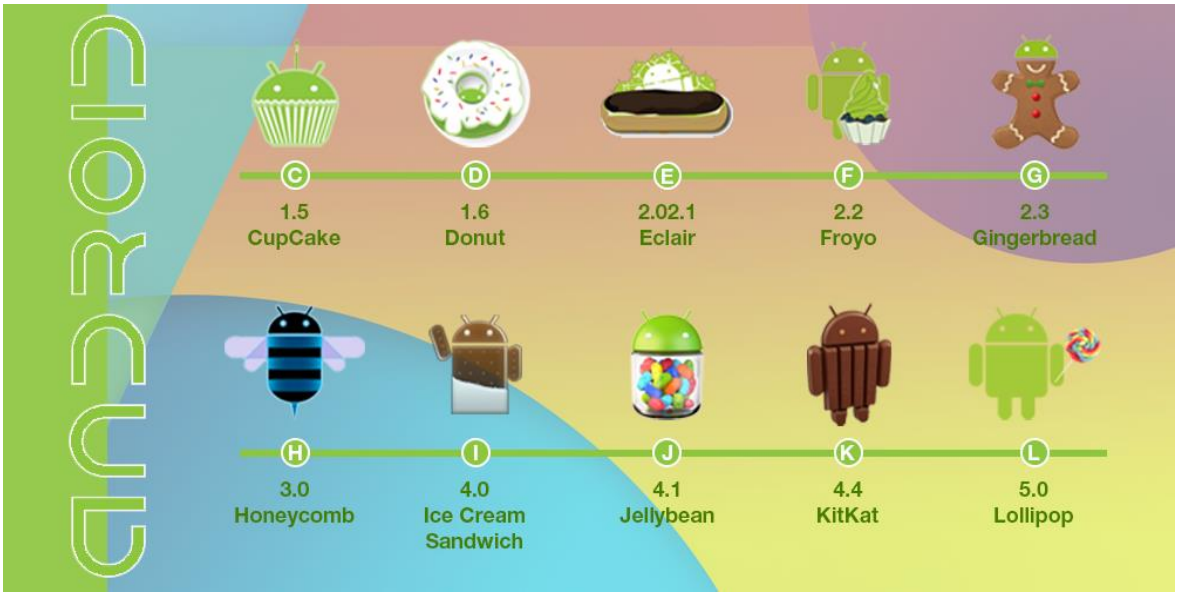
- Android 5.0/5.1 Lollipop

Παρουσιάστηκε υπό την κωδική ονομασία "Android L" τον Ιουνίο του 2014, κατά τη διάρκεια του Google I/O και έγινε διαθέσιμο επίσημα ως ενημέρωση στις 12 του Νοέμβρη 2014, για επιλεγμένες συσκευές με διανομές Android που εξυπηρετούνται από την Google. Η Lollipop διαθέτει ένα επανασχεδιασμένο UI και η Google έκανε εσωτερικές αλλαγές και στην πλατφόρμα, όπου το Android Runtime (ART) να αντικατέστησε το Dalvik για την βελτίωση της απόδοσης των

εφαρμογών και επιπρόσθετα αλλαγές που αποσκοπούν στη βελτίωση και βελτιστοποίηση της χρήσης της μπαταρίας. Επίσης υπάρχει υποστήριξη για επεξεργαστές 64-bit ,ανανεωμένη οθόνη κλειδώματος, δυνατότητα παραμετροποίησης των ειδοποιήσεων από τον χρήστη και είσοδος και έξοδος ήχου μέσω USB συσκευών.

- Android 6.0 MarshMallow

Το Android MarshMallow είναι η ανερχόμενη αναβάθμιση για το λειτουργικό σύστημα του Android η οποία δεν έχει ανακοινωθεί ακόμα πότε θα κυκλοφορήσει. Η έκδοση Marshmallow θα επικεντρωθεί στη βελτίωση της συνολικής εμπειρίας του χρήστη, η οποία θα περιέχει καινούργια χαρακτηριστικά, όπως ένα καινούργιο σχέδιο ενέργειας, το Doze,για την επέκταση της διάρκειας αυτονομίας της μπαταρίας και υποστήριξη αναγνώρισης δαχτυλικού αποτυπώματος.



Σχήμα 3 Οι εκδόσεις του Android

Πίνακας 1 Λεπτομέρειες εκδόσεων Android

Έκδοση	Κωδικό Όνομα	Ημερομηνία Έκδοσης	API level
5.1.x	Lollipop	9 Μαρτίου 2015	22
5.0-5.0.2		3 Νοεμβρίου 2014	21
4.4-4.4.4	KitKat	31 Οκτωβρίου 2013	19
4.3.x	Jelly Bean	24 Ιουλίου 2013	18
4.2.x		13 Νοεμβρίου 2012	17
4.1.x		9 Ιουλίου 2012	16
4.0.3-4.0.4	Ice Cream Sandwich	16 Δεκεμβρίου 2011	15
2.3.3-2.3.7	Gingerbread	9 Φεβρουαρίου 2011	10
2.2-2.2.3	Froyo	20 Μαΐου 2010	8

1.5 Βασικά Χαρακτηριστικά

1.5.1 Διεπαφή(Interface)

Το βασικό περιβάλλον χρήστη του Android βασίζεται στον άμεσο χειρισμό, χρησιμοποιώντας την οθόνη αφής για είσοδο, με κινήσεις που αντιστοιχούν σε πραγματικές, όπως το σύρσιμο, το πάτημα, το τσίμπημα, και το αντίστροφο του τσιμπήματος για να χειριστεί αντικείμενα που εμφανίζονται στην οθόνη, και επίσης συμπληρώνεται από ένα εικονικό πληκτρολόγιο. Η αντίδραση στις κινήσεις του χρήστη είναι σχεδιασμένο να είναι άμεση και να παρέχει ένα εύχρηστο interface αφής που σε συνδυασμό με τη δόνηση της συσκευής δίνει στο χρήστη ένα πολύ καλό αποτέλεσμα επικοινωνίας μεταξύ της συσκευής και του χρήστη. Παράλληλα οι αισθητήρες, τα γυροσκόπια και τα επιταχυνσιόμετρα της συσκευής χρησιμοποιούνται από κάποιες εφαρμογές για να ανταποκριθούν σε άλλες κινήσεις του χρήστη όπως η αντιστροφή της οθόνης από οριζόντια σε κάθετη ανάλογα με το πώς κρατά τη συσκευή ο χρήστης. Το λειτουργικό Android όταν εκκινεί μας παρουσιάζει την οθόνη κλειδώματος και στη συνέχεια εφόσον ξεκλειδωθεί είτε με ένα απλό σύρσιμο είτε με έναν κωδικό ή μοτίβο το οποίο έχει ορίσει ο χρήστης παρουσιάζεται η αρχική οθόνη. Η αρχική οθόνη αποτελείται από εικονίδια τα οποία εκκινούν εφαρμογές και από widgets δηλαδή δυναμικά εικονίδια τα οποία ενημερώνονται συνεχώς ,χαρακτηριστικό παράδειγμα το widget με την πρόβλεψη καιρού, επίσης υπάρχει και η status bar η οποία μας δίνει τις βασικές πληροφορίες της συσκευής όπως την κατάσταση της μπαταρίας ,την ώρα και τις καταστάσεις

συνδεσιμότητας. Η αρχική οθόνη μπορεί να αποτελείτε από παραπάνω από μια επιφάνειες εργασίας τις οποίες ο χρήστης μπορεί να διαμορφώσει όπως θέλει και όπως ταιριάζει στις ανάγκες του. Τέλος το λειτουργικό Android επιτρέπει την εγκατάσταση εφαρμογών οι οποίες αλλάζουν την προκαθορισμένη εμφάνιση και την αρχικής οθόνης αλλά και γενικά όλων των χαρακτηριστικών του interface.

1.5.2 Εφαρμογές(Applications) και το Google Play

Οι εφαρμογές του Android δημιουργούνται κατά κύριο λόγο με το Android software development kit(SDK) σε γλώσσα Java η οποία έχει πλήρη πρόσβαση στα Android API. Οι προγραμματιστές χρησιμοποιούν για να δημιουργήσουν τις εφαρμογές με Java ολοκληρωμένα περιβάλλοντα ανάπτυξης(IDE) τα πιο διαδεδομένα είναι το Eclipse και το Android Studio τα οποία προτείνει και η Google για την ανάπτυξη των εφαρμογών. Εκτός της Java όμως η Google παρέχει το Native Development Kit (NDK) το οποίο επιτρέπει στους developer να γράψουν σημαντικό μέρος των εφαρμογών τους σε native γλώσσες όπως είναι η C και η C++. Αυτό είναι ιδιαίτερα χρήσιμο καθώς επιτρέπει να επαναχρησιμοποιηθεί ο υπάρχων κώδικας (δηλαδή κάποιες γνωστές βιβλιοθήκες) ή να βελτιωθεί η κατανάλωση πόρων της εφαρμογής κάνοντας το μέγιστο δυνατό optimization (βελτιστοποίηση) στα σημεία που χρειάζεται. Υπάρχουν κάποια εργαλεία τα οποία μας επιτρέπουν να γράψουμε εφαρμογές χρησιμοποιώντας και web γλώσσες όπως η HTML, η CSS και η JavaScript. Με αυτά μπορούμε να δημιουργήσουμε εφαρμογές που θα τρέχουν μέσα σε ένα Web View, δηλαδή μία πλήρης web page που τρέχει μέσα σε μία εφαρμογή αντί στον browser. Εργαλεία όπως τα Phone Gap και Appcelerator Titanium μας βοηθούν να γράψουμε κώδικα ο οποίος μεταγλωττίζεται στο παρασκήνιο σε native code. Υπάρχουν μειονεκτήματα και πλεονεκτήματα σ' αυτή την προσέγγιση και θα πρέπει να έχουμε πάντα υπόψη μας ότι χρησιμοποιώντας Java παίρνουμε τα καλύτερα αποτελέσματα, αλλά μπορούμε να φτιάξουμε εξίσου δυνατές εφαρμογές με όποιο εργαλείο μας βολεύει. Ένα ακόμη μειονέκτημα των άλλων γλωσσών προγραμματισμού είναι ότι τα 3rd party εργαλεία που χρησιμοποιούμε θα βρίσκονται πάντα ένα βήμα πίσω από τις τελευταίες εξελίξεις στον χώρο του Android development.

Όλες αυτές οι εφαρμογές οι οποίες δημιουργούνται μπορούν να γίνουν άμεσα διαθέσιμες στους χρήστες οι οποίοι χρησιμοποιούν λειτουργικό Android.Για να γίνει αυτό οι χρήστες μπορούν να κατεβάσουν και να εγκαταστήσουν το APK(Android

Application Package) αρχείο της εφαρμογής στη συσκευή τους η εναλλακτικά μπορούν να κατεβάσουν την εφαρμογή από ένα κατάστημα εφαρμογών (application store) το οποίο προσφέρει στους χρήστες τις δυνατότητες κατεβάσματος, εγκατάστασης, απεγκατάστασης αλλά και ενημέρωσης των εφαρμογών. Υπάρχουν διάφορα καταστήματα εφαρμογών από οποία ο χρήστης μπορεί να χρησιμοποιήσει αλλά το επίσημο κατάστημα της Google είναι το Google Play Store(ή παλιότερα Market). Από εκεί ο χρήστης μπορεί να κατεβάσει τις εφαρμογές της Google αλλά και εφαρμογές από άλλους προγραμματιστές οι οποίες θα πληρούν τις προϋποθέσεις της Google. Εκτός από εφαρμογές ο χρήστης μπορεί να κατεβάσει από το Google Play Store μουσική, περιοδικά, βιβλία, ταινίες και τηλεοπτικά προγράμματα. Οι χρήστες μπορούν επίσης να αγοράσουν υλικό, όπως Chromebooks, το Google Nexus branded κινητών συσκευών, Chromecasts, και αξεσουάρ. Το πλεονέκτημα του Google Play Store έναντι των άλλων καταστημάτων είναι η ασφάλεια καθώς η Google εγγυάται για την ασφάλεια των εφαρμογών τις οποίες διαθέτει στο Google Play Store ενώ οι άλλες εφαρμογές από άγνωστες πηγές μπορεί να είναι διαθέτουν κάποιο κακόβουλο λογισμικό το οποίο θα προσβάλει τη συσκευή. Ακόμη υπάρχει δυνατότητα για τον οποιονδήποτε να δημιουργήσει μια Android εφαρμογή και να την ανεβάσει στο Google Play Store χωρίς να είναι απαραίτητα προγραμματιστής η εταιρεία πληροφορικής αρκεί να πληρώσει ένα αντίτιμο στη Google το οποίο δεν χρειάζεται να το πληρώνει για κάθε εφαρμογή μου ανεβάζει αλλά μόνο για την πρώτη.

1.5.3 Open source λογισμικό

Το Android είναι ένα λογισμικό ανοιχτού κώδικα. Αυτό σημαίνει ότι:

- Επιτρέπεται η δωρεάν πρόσβαση στον κώδικα του συστήματος έτσι ώστε να είναι εφικτή η ανάπτυξη επιπρόσθετων λειτουργιών από άλλους προγραμματιστές.
- Επιτρέπεται η επανασχεδίαση ορισμένων λειτουργιών και η αντικατάσταση αυτών ή ολόκληρου του συστήματος.
- Ευθυγραμμίζεται με διεθνή πρότυπα λειτουργίας έτσι ώστε να εγγυηθεί τόσο την ορθή λειτουργία αλλά και το επίπεδο ποιότητας αυτής
- Επιτρέπεται η δωρεάν χρήση του συστήματος, η ανάπτυξη νέων εφαρμογών και η δημοσίευση αυτών.

- Χρησιμοποιείται γλώσσα προγραμματισμού με ανοικτό πρότυπο.
- Μπορεί να εγκατασταθεί και να χρησιμοποιηθεί σε οποιαδήποτε πλατφόρμα υλικού.

1.6 Αρχιτεκτονική

Η Αρχιτεκτονική του Android χωρίζεται σε 4 επίπεδα όπως αυτά περιγράφονται παρακάτω:

- Linux Kernel (Πυρήνας Linux)

Ο Linux Kernel είναι αυτός στον οποίο βασίζεται το λειτουργικό σύστημα Android.Σε αυτόν περιέχονται όλοι οι οδηγοί της συσκευής που χρειάζονται για τα διάφορα υλικά μέρη της συσκευής. Επίσης το Android βασίζεται στον πυρήνα Linux για εργασίες όπως η ασφάλεια, η διαχείριση μνήμης, η διαχείριση διεργασιών και άλλες υπηρεσίες συστήματος.

- Βιβλιοθήκες (Libraries)

Οι βιβλιοθήκες περιλαμβάνουν όλο τον κώδικα ο οποίος παρέχει τα βασικά χαρακτηριστικά ενός λειτουργικού συστήματος Android.Ο κώδικας είναι γραμμένος σε C και C++ και χρησιμοποιούνται μέσω του κατάλληλου interface της java.Μερικές από τις κυριότερες είναι η Surface manager για δημιουργία γραφικών, η Media framework για πολυμέσα , η SQLite για βάσεις δεδομένων και η Webkit για την υποστήριξη του browser.

- Android Runtime

Μαζί με τις βιβλιοθήκες υπάρχει και ο τομέας Android run time που προσφέρει με ένα σύνολο από βασικές βιβλιοθήκες τη δυνατότητα στους προγραμματιστές να δημιουργήσουν εφαρμογές Android σε γλώσσα προγραμματισμού Java. Επιπλέον, ο τομέας αυτός περιλαμβάνει την εικονική μηχανή (virtual machine) Dalvik. Η Dalvik είναι μια ειδική εικονική μηχανή η οποία είναι υπεύθυνη για την δημιουργία των εκτελέσιμων αρχείων και είναι ειδικά σχεδιασμένη για Android για χρήση με κινητές συσκευές που λειτουργούν με μπαταρία και διαθέτουν περιορισμένες δυνατότητες σε μνήμη και CPU.

- Πλαίσιο Εφαρμογών (Application Framework)

Λόγο του ότι το Android είναι ανοιχτή πλατφόρμα ανάπτυξης εφαρμογών οι εφαρμογές που παράγονται είναι ιδιαίτερα προχωρημένες έτσι λοιπόν μπορούν να έχουν πρόσβαση σε βασικές βιβλιοθήκες του συστήματος και μέσω του Application Framework μπορούν να παρέχουν λειτουργίες ή υπηρεσίες προς άλλες εφαρμογές. Το Application Framework περιλαμβάνει ένα πακέτο από υπηρεσίες μερικές από τις οποίες είναι:

- View System

  Περιλαμβάνει γραφικά περιβάλλοντος όπως κουμπιά(buttons) λίστες(lists), πλέγματα (grids), κουτιά κειμένου (text boxes) και άλλα.
- Content Providers

  Μέσω αυτού οι εφαρμογές έχουν πρόσβαση στα δεδομένα άλλων εφαρμογών η μπορούν να διαμοιράσουν τα δικά τους δεδομένα σε άλλες εφαρμογές.
- Resource Manager

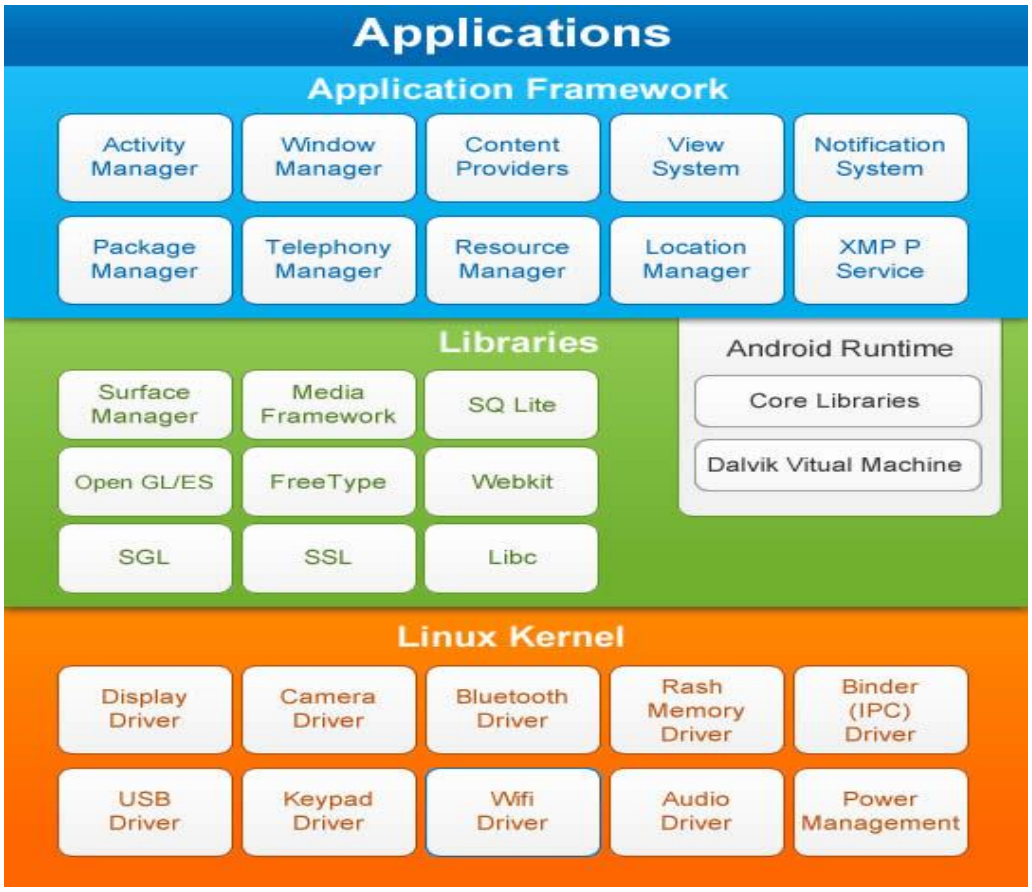
  Παρέχει πρόσβαση σε άλλους πόρους εκτός κώδικα όπως αρχεία και γραφικά.
- Notification Manager

  Διαχειρίζεται να μηνύματα που εμφανίζονται στο status bar.
- Activity Manager

  Διαχειρίζεται τον κύκλο ζωής των εφαρμογών και δίνει την δυνατότητα επιστροφής σε προγενέστερες καταστάσεις

- Εφαρμογές (Applications)

Τέλος στο υψηλότερο στρώμα βρίσκονται οι εφαρμογές οι οποίες διατίθενται μαζί με την συσκευή όπως οι επαφές (Contacts), το Τηλέφωνο (Phone), ο Περιηγητής (Browser κλπ) και οι εφαρμογές που μπορεί να κατεβάσει ο χρήστης από το Google Play.



Σχήμα 4 Διάγραμμα αρχιτεκτονικής του συστήματος Android

1.7 Ασφάλεια

Οι Android εφαρμογές τρέχουν σε ένα sandbox, δηλαδή μια απομονωμένη περιοχή του συστήματος που δεν έχει πρόσβαση στους υπόλοιπους πόρους του συστήματος, εκτός εάν τους έχουν δοθεί τα δικαιώματα πρόσβασης που χορηγούνται ρητώς από το χρήστη όταν έχει εγκατασταθεί η εφαρμογή. Πριν από την εγκατάσταση μιας εφαρμογής, το Google Play Store εμφανίζει όλες τις απαιτούμενες άδειες, για παράδειγμα ένα παιχνίδι μπορεί να χρειαστεί να ενεργοποιηθεί η δόνηση ή να αποθηκεύσει τα δεδομένα σε μια κάρτα SD αλλά δεν θα χρειαστεί να διαβάσει τα μηνύματα SMS ή να έχει πρόσβαση στον τηλεφωνικό κατάλογο. Μετά την εξέταση αυτών των δικαιωμάτων, ο χρήστης μπορεί να επιλέξει να δεχθεί ή να αρνηθεί την εγκατάσταση της εφαρμογής μόνο σε περίπτωση που τα αποδέχεται. Το σύστημα αυτό με τις άδειες μειώνει τον κίνδυνο για τρωτά σημεία και σφάλματα σε εφαρμογές, αλλά λόγο της δυσκολίας των προγραμματιστών να καταλάβουν το σύστημα και λόγο της περιορισμένης γραπτής τεκμηρίωσης των εφαρμογών, έχει οδηγήσει οι εφαρμογές να ζητούν περιττά δικαιώματα, μειώνοντας την αποτελεσματικότητά τους. Επίσης η Google

προχώρησε σε μια ενημέρωση την Android Verify Apps, η οποία θα εκτελείται τώρα στο παρασκήνιο θα εντοπίζει κακόβουλα λογισμικά και αφού τα τερματίζει θα τα διαγράφει.

1.8 Επίλογος

Συνοψίζοντας, σε αυτό το κεφάλαιο παρουσιάζεται το λειτουργικό σύστημα Android, γίνεται μια αναδρομή στην ιστορία του και στην εξέλιξή του μέσα από τις εκδόσεις του, γίνεται μια αφορά στα βασικά χαρακτηριστικά του και στην αρχιτεκτονική σύμφωνα με την οποία είναι δομημένο αλλά και στην ασφάλεια που είναι πολύ βασική αλλά και πολύ ισχυρή με αυτό το λειτουργικό σύστημα. Όλα αυτά θα βοηθήσουν για να καταλάβουμε πιο εύκολα την διαδικασία ανάπτυξης της εφαρμογής μας με το λειτουργικό σύστημα Android.

ΚΕΦΑΛΑΙΟ 2

2 Ανάπτυξη Εφαρμογής σε Android

2.1 Εισαγωγή

Η ανάπτυξη μιας Android εφαρμογής βασίζεται σε τέσσερα θεμελιώδη συστατικά. Τα συστατικά αυτά παρέχουν τις απαραίτητες διασυνδέσεις με το σύστημα, έχοντας καθένα από αυτά συγκεκριμένο ρόλο καθόλη τη διάρκεια ζωής της εφαρμογής. Δεν είναι απαραίτητη η χρήση όλων αυτών των συστατικών σε κάθε εφαρμογή και κάποια από αυτά δεν είναι απαραίτητα για τη διασύνδεση με το χρήστη, όμως κάθε ένα από αυτά εξυπηρετεί μοναδικό σκοπό με τον διαφορετικό κύκλο ζωής του.

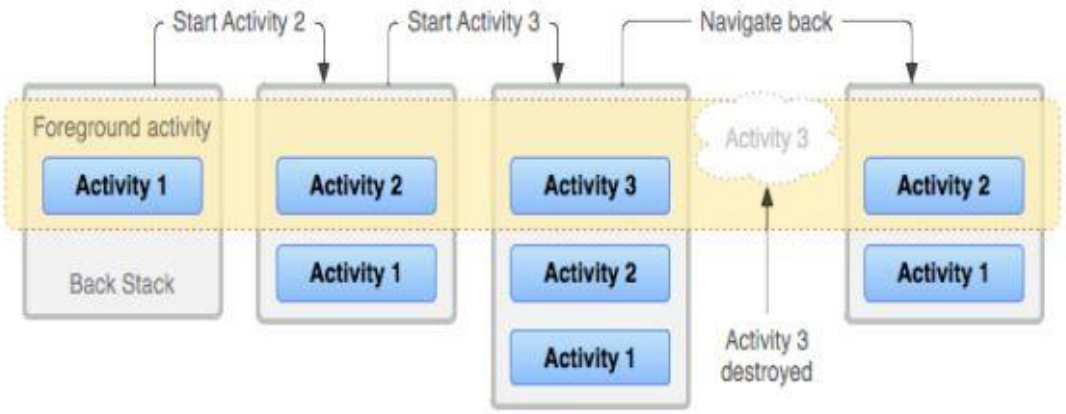
Σε αυτό το κεφάλαιο, περιγράφονται τα βασικά στοιχεία μιας εφαρμογής Android,ενώ γίνεται αναφορά και σε επιμέρους, πιο εξειδικευμένα στοιχεία

2.2 Βασικά συστατικά Android εφαρμογής

2.2.1 Activities

Μια δραστηριότητα αφορά πάντα την οπτική αναπαράσταση της εφαρμογής μας(User Interface).Όλες οι εφαρμογές έχουν υποχρεωτικά τουλάχιστον μια δραστηριότητα για να λειτουργήσουν. Μέσα από μια δραστηριότητα μπορούμε να ξεκινήσουμε και μια δεύτερη και πάει λέγοντας, αναστέλλοντας την προηγούμενη. Στην ουσία αυτές που αναστέλλονται, δεν χάνονται αλλά κρατιούνται σε μια στοίβα(LIFO) δραστηριοτήτων με τις τρέχουσες καταστάσεις τους, ώστε όταν τις ξανακαλέσουμε να συνεχίσουμε από εκεί που ήμασταν.

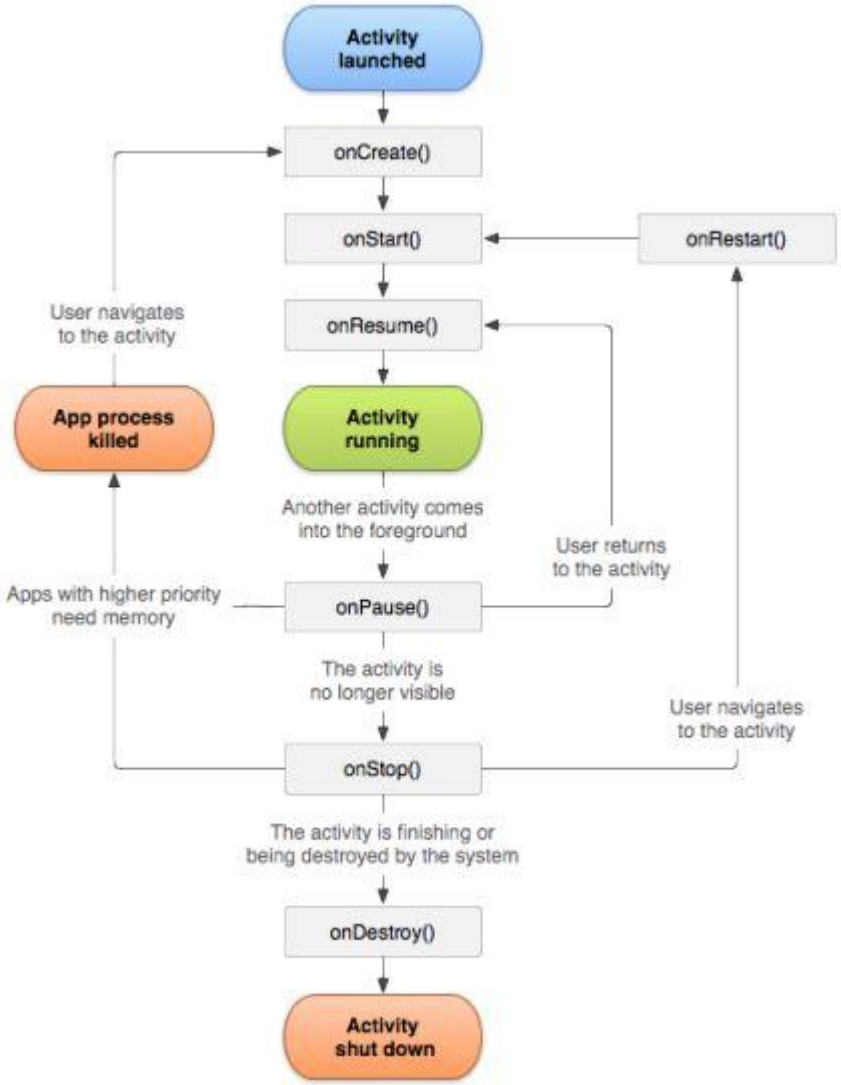
Στο επόμενο σχήμα φαίνεται η συγκεκριμένη διαδικασία στη στοίβα :



Σχήμα 5 Διάγραμμα στοίβας δραστηριοτήτων

Κάθε δραστηριότητα έχει έναν κύκλο ζωής, ο οποίος ξεκινά με την δημιουργία της onCreate() και τελειώνει με την καταστροφή της onDestroy().

Στην επόμενη εικόνα, υπάρχει στο διάγραμμα ολόκληρος ο κύκλος ζωής μιας δραστηριότητας τον οποίο και θα εξηγήσουμε :



Σχήμα 6 Διάγραμμα κύκλου ζωής δραστηριοτήτων

Στον ακόλουθο πίνακα, αναγράφονται οι κύκλοι ζωής των δραστηριοτήτων, μαζί με την λειτουργία τους και την δραστηριότητα που ακολουθεί μετά την ολοκλήρωση της τρέχουσας δραστηριότητας :

Τρέχουσα μέθοδος	Περιγραφή	Επόμενη μέθοδος
onCreate()	Η πρώτη μέθοδος που φορτώνεται με το που ξεκινάμε μια δραστηριότητα. Εδώ ορίζονται για πρώτη φορά όλα τα αντικείμενα που χρειάζονται με τις κατάλληλες αρχικές τιμές.	OnStart()
onStart()	Καλείται ακριβώς πριν γίνει εμφανίσιμη η δραστηριότητα στον χρήστη. Οπότε προσθέτουμε ότι λειτουργικότητα θέλουμε για αυτή την περίπτωση.	onResume()
onResume()	Καλείται πριν η δραστηριότητα αρχίσει να αλληλοεπιδρά με τον χρήστη. Βρίσκεται στην κορυφή της στοίβας, περιμένοντας για κάποιο user input.	onPause()
onPause()	Καλείται όταν πάει να γίνει resume μιας άλλης δραστηριότητας. Συνήθης χρήση είναι όταν θέλουμε να αποθηκεύσουμε της αλλαγές μας για να μην απασχολούμαι άσκοπα πόρους cpu	onResume() , αν επιστρέψει στο προσκήνιο αλλιώς onStop()
onStop()	Καλείται όταν η δραστηριότητα δεν είναι εμφανίσιμη πλέον στο χρήστη. Αυτό συμβαίνει είτε γιατί πρόκειτε να τερματιστεί η δραστηριότητα είτε γιατί ξεκινά νέα και την καλύπτει.	OnDestroy()
onDestroy()	Καλείται είτε επειδή τελείωσε η εφαρμογή από το χρήστη ηθελημένα είτε επειδή πρέπει να τερματιστεί βίαια (force closing) για να εξοικονομήσει πόρους συστήματος.	----

2.2.2 Services

Είναι άλλο ένα δομικό στοιχείο των εφαρμογών Android. Έχει διαφορές ως προς τον τρόπο λειτουργίας του σε σχέση με τις δραστηριότητες. Πιο συγκεκριμένα τρέχει πάντα στο παρασκήνιο και ποτέ δεν αλληλοεπιδρά άμεσα με τον χρήστη , και κατά δεύτερο έχει μεγαλύτερη διάρκεια ζωής από τις δραστηριότητες. Για παράδειγμα ένα service μπορεί να διαχειρίζεται συνδέσεις δικτύου, βάσεων δεδομένων , ενημέρωση τοποθεσίας ανά διαστήματα , λήψη mail κ.α

Ένα service θα μπορούσαμε να πούμε ότι έχει δύο μορφές λειτουργίας , Started (ξεκίνημα) και Bound (δέσμευση).

Started

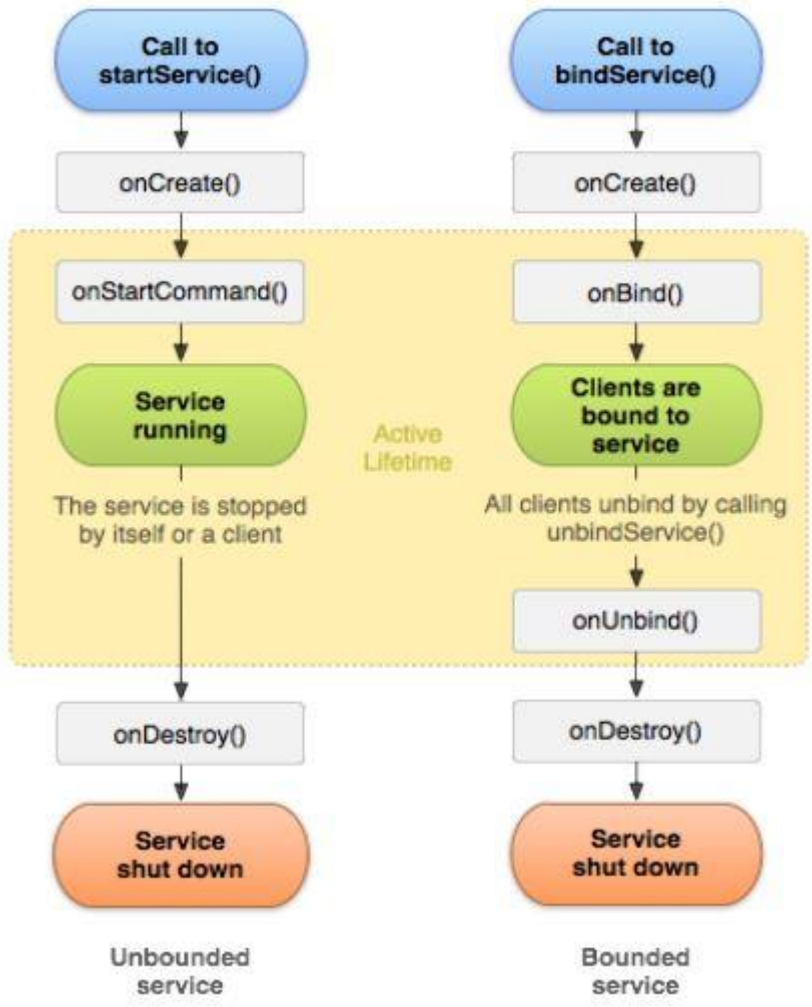
Ξεκινά από κάποια δραστηριότητα συνήθως με τη μέθοδο startService(). Εφόσον ξεκινήσει διατηρείται μακροχρόνια ακόμα και αν το συστατικό που την ξεκίνησε καταστραφεί. Αυτή η μορφή λειτουργίας είναι ιδανική όταν δεν περιμένουμε από το service να μας επιστρέψει κάτι , απλά θέλουμε να γίνει μια διαδικασία και μετά να σταματήσει. Πχ Το ανέβασμα κάποιου αρχείου σε server.

Bound

Μια υπηρεσία δεσμεύεται από το καλούμενο συστατικό (Activity) με την μέθοδο bindService(). Έτσι μας δίνεται η δυνατότητα να στέλνουμε αιτήσεις σε αυτό και να μας επιστέφει αποτελέσματα. Όταν το αποδεσμεύσουμε θα σταματήσεις τη λειτουργία του.

ΠΡΟΣΟΧΗ : Να σημειώσουμε ότι οι υπηρεσίες και οι δραστηριότητες από προεπιλογή τρέχουν στην ίδιο νήμα συνεπώς έχουμε μια διεργασία για όλα μαζί. Αν θέλουμε να δημιουργήσουμε κάποια βαριά υπηρεσία είναι καλό να έχουμε και ξεχωριστή διεργασία διαφορετικά μειώνεται η απόδοση της δραστηριότητας και κατ’ επέκταση της εφαρμογής.

Στο επόμενο σχήμα, υπάρχουν οι κύκλοι ζωής ενός service,και στις δύο του μορφές :



Σχήμα 7 Διάγραμμα κύκλου ζωής ενός service

Όπως παρατηρούμε ολόκληρος ο ενεργός κύκλος ζωής ξενικά με τις μεθόδους onStartCommand() ή onBind() και τελειώνει με την onDestroy().

2.2.3 Content Provider

Οι content providers ή αλλιώς πάροχοι περιεχομένου, είναι υπεύθυνοι για τη διαχείριση του αποθηκευτικού χώρου των δεδομένων. Στην ουσία αποθηκεύονται τα δεδομένα στο file system του κινητού έτσι ώστε και άλλες εφαρμογές να μπορούν τα έχουν πρόσβαση σε αυτά τα κοινά δεδομένα, μεταβάλλοντας τα αν χρειαστεί κιόλας. Για παράδειγμα το σύστημα Android χρησιμοποιεί έναν content

provider που διαχειρίζεται τα δεδομένα μιας επαφής χρήστη, έτσι κάθε άλλη εφαρμογή που έχει τα κατάλληλα δικαιώματα μπορεί να τροποποιήσει αυτά τα δεδομένα.

2.2.4 Broadcast Receiver

Οι broadcast receivers είναι ένας μηχανισμός που παρέχει ενημέρωση στην εφαρμογή όταν κάποιο γεγονός πραγματοποιηθεί. Τέτοια γεγονότα είναι για παράδειγμα όταν η στάθμη της μπαταρίας είναι πολύ χαμηλή ή όταν είμαστε εκτός δικτύου κ.α . Δεν παρέχουν user interface συνεπώς αν θέλουμε να ενημερώσουμε τον χρήστη ότι κάτι από αυτά συνέβη , το κάνουμε μέσω notifications.

Όσο αφορά την ενεργοποίηση αυτών των συστατικών , τα 3 από αυτά (activity, service,broadcast receiver) ενεργοποιούνται ασύγχρονα μέσω μηνυμάτων intent ή αλλιώς προθέσεις .(intent είναι η περιγραφή για το τι θα συμβεί, μεταφέροντας αυτή την εντολή, δηλαδή κάτι σαν messenger για την εφαρμογή). Μια πρόθεση (intent) δημιουργείται με το ανάλογο αντικείμενο Intent object στο οποίο ορίζεται η πράξη που θα εκτελεστεί. Για παράδειγμα στις εφαρμογές χρησιμοποιείται κατά κόρων το intent για να ξεκινήσουμε νέες activities.

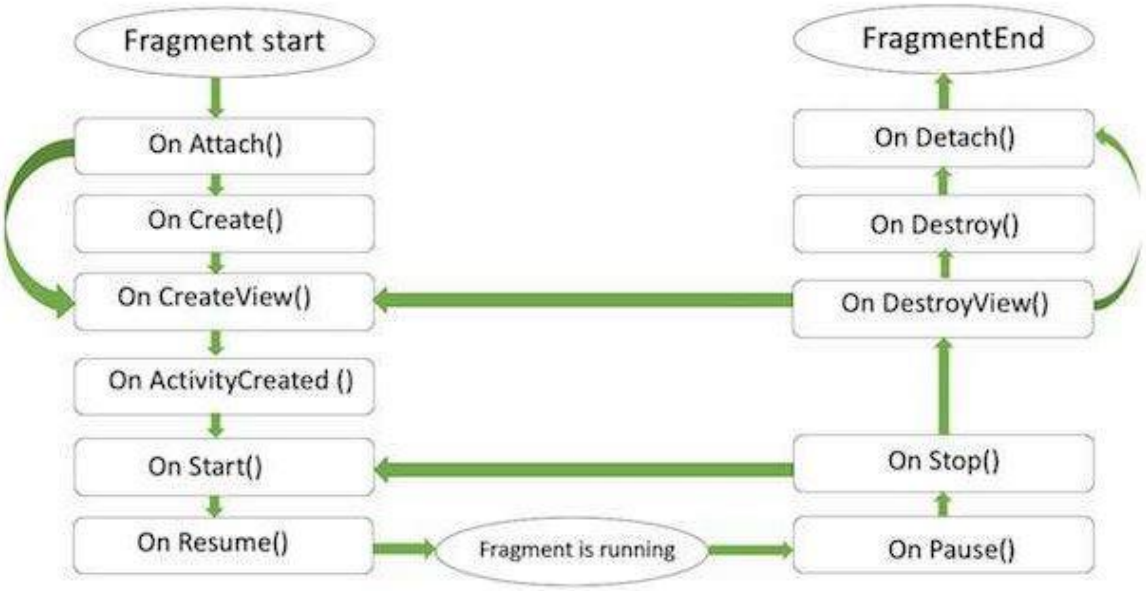
2.3 Επιπρόσθετα χαρακτηριστικά

2.3.1 Fragments

Το Fragment είναι ένα κομμάτι από μια δραστηριότητα το οποίο επιτρέπει πιο εύκολη τροποποίηση στη σχεδίαση μιας δραστηριότητας. Ένα fragment δηλαδή, αποτελεί ένα είδος υπο-δραστηριότητας. Παρακάτω ακολουθούν μερικά βασικά χαρακτηριστικά των fragments:

- Ένα fragment έχει τη δικιά του εμφάνιση μαζί με την δικιά του συμπεριφορά και τον δικό του κύκλο ζωής.
- Μπορούμε να προσθέσουμε η να αφαιρέσουμε ένα fragment από μια δραστηριότητα ,ενώ η δραστηριότητα εκτελείτε.
- Μπορούμε να συνδυάσουμε πολλά fragments σε μια δραστηριότητα για να χτίσουμε ένα μοναδικό user interface

- Ένα fragment μπορεί να χρησιμοποιηθεί σε πολλές δραστηριότητες
- Ο κύκλος ζωής ενός fragment είναι άρρηκτα συνδεδεμένος με τον κύκλο ζωής της δραστηριότητας στην οποία εμπεριέχεται. Αυτό σημαίνει, ότι όταν η δραστηριότητα κάνει παύση, τότε και όλα τα fragments της συγκεκριμένης δραστηριότητας θα σταματήσουν επίσης
- Ένα fragment μπορεί να εμπεριέχει μια συμπεριφορά, η οποία δεν έχει User Interface
- Τα fragments προστέθηκαν στο Android API 11,στην έκδοση του Honeycomb

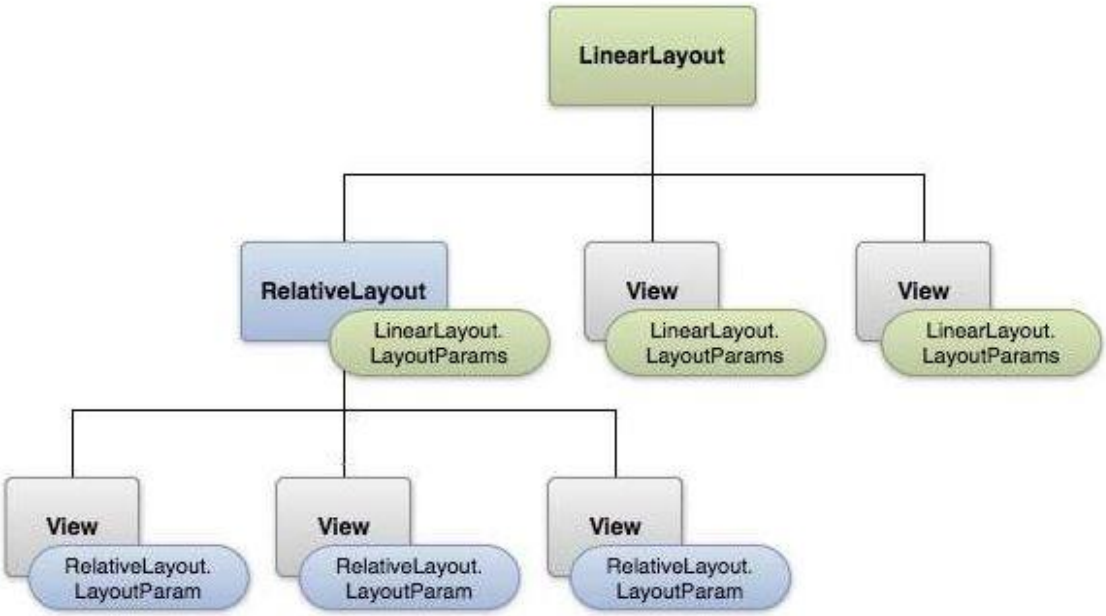


Σχήμα 8 Διάγραμμα κύκλου ζωής ενός fragment

2.3.2 Views & ViewGroup

Το βασικό πεδίο 'χτισίματος' ενός User Interface,είναι το αντικείμενο View. Δημιουργείται από την κλάση View και καταλαμβάνει μια περιοχή στην οθόνη η οποία είναι υπεύθυνη για την σχεδίαση και τη διαχείριση των γεγονότων. Η View είναι η βασική κλάση των widgets, τα οποία χρησιμοποιούνται για να παράγουν τα διαδραστικά στοιχεία μιας Android εφαρμογής, όπως κουμπιά, πεδία κειμένου κτλ.

Η ViewGroup είναι μια υποκλάση της View και παρέχει ένα αόρατο container,που είναι υπεύθυνο να κρατάει άλλα Views ή ViewGroups και να ορίζει τις ιδιότητες της εμφάνισής τους. Στο 3ο επίπεδο έχουμε διαφορετικά layouts,τα οποία είναι υποκλάσεις της ViewGroup που ένα κλασσικό layout ορίζει την δομή για ένα Android user interface. Μπορεί να δημιουργηθεί είτε σε χρόνο εκτέλεσης, χρησιμοποιώντας αντικείμενα τύπου View /ViewGroup ή μπορούμε να τα ορίσουμε χρησιμοποιώντας ένα απλό XML αρχείο, το main_layout.xml το οποίο βρίσκεται στον κατάλογο res/layout του project.



Σχήμα 9 Views

2.3.3 Layouts

Υπάρχει ένας μεγάλος αριθμός από Layouts που παρέχει η πλατφόρμα του Android,τα οποία θα χρησιμοποιηθούν στις περισσότερες από τις Android εφαρμογές, έτσι ώστε να παρέχουν διαφορετική εμφάνιση, όψη και αίσθηση στην εφαρμογή. Τα υπάρχοντα είδη Layout,παρουσιάζονται στον παρακάτω πίνακα :

	Layout & Περιγραφή
1	Linear Layout Linear Layout είναι ένα view group το οποίο στοιχίζει όλα τα ‘παιδιά’ του σε μια συγκεκριμένη κατεύθυνση, οριζόντια ή κάθετα.
2	Relative Layout Relative Layout είναι ένα view group που εμφανίζει τα ‘παιδιά’ του σε σχετικές θέσεις.
3	Table Layout Table Layout είναι ένα view group που ομαδοποιεί τα views σε στήλες και γραμμές.
4	Absolute Layout Absolute Layout είναι ένα view group που μας δίνει την δυνατότητα να ορίσουμε τη θέση ακριβή θέση των ‘παιδιών’ του.
5	Frame Layout Frame Layout είναι ένα view group που δεσμεύει μια συγκεκριμένη θέση στην οθόνη η οποία χρησιμοποιείται για να εμφανιστεί ένα μόνο view.
6	List Layout List Layout είναι ένα view group που εμφανίζει μια λίστα από αντικείμενα.
7	Grid Layout Grid Layout είναι ένα view group που εμφανίζει αντικείμενα σε ένα πλέγμα δύο διαστάσεων.

2.3.4 Intents

Ένα intent είναι μια δομή δεδομένων που περιέχει τις απαραίτητες πληροφορίες για μια ενέργεια που θέλουμε να εκτελέσουμε. Το στιγμιότυπο της κλάσης Intent μπορεί να περιέχει διάφορες πληροφορίες που χρειάζονται για την επιτυχή εκτέλεση της περιγραφόμενης ενέργειας. Στον παρακάτω πίνακα βλέπουμε τι είδους πληροφορίες μπορεί να περιέχει ένα intent.

Πληροφορία	Περιγραφή
Όνομα Στοιχείου	Ένα intent μπορεί να περιέχει το όνομα του στοιχείου (πλήρες όνομα κλάσης) που προορίζεται να χειριστεί την ενέργεια που επιθυμούμε να εκτελεστεί. Το πεδίο αυτό είναι προαιρετικό. Αν είναι ορισμένο τότε το intent παραδίδεται σε ένα στιγμιότυπο της κλάσης που έχουμε καθορίσει, αλλιώς το Android αναζητά κάποιον κατάλληλο στόχο για να χειριστεί το intent αυτό βασιζόμενο σε άλλες πληροφορίες μέσα στο στιγμιότυπο της intent.
Ενέργεια	Περιγράφει την ενέργει που πρέπει να εκτελεστεί (ή το μήνυμα που μεταδίδεται , σε περίπτωση που κάνουμε broadcast κάποιο συμβάν). Η κλάση intent περιλαμβάνει έναν αριθμό από σταθερές που καθορίζουν διάφορες προκαθορισμένες ενέργειες. Ο προγραμματιστής μπορεί να ορίσει και δικές του ενέργειες και στην συνέχεια να αναπτύξει εφαρμογές που αποκρίνονται σε αυτές.
Δεδομένα	Τα δεδομένα πάνω στα οποία θα εκτελεστεί η ενέργεια. Για κάθε ενέργει απαιτούνται και διαφορετικής μορφής δεδομένα.
Κατηγορία	Το πεδίο αυτό παρέχει επιπλέον λεπτομέρειες για την οντότητα που θέλουμε να χειριστεί το intent. Όπως και στην περίπτωση των ενεργειών ,έτσι και εδώ η κλάση intent παρέχει σταθερές που περιγράφουν διάφορες προκαθορισμένες κατηγορίες.
Extra	Επιπλέον δεδομένα που θέλουμε να μεταφέρουμε στο intent. Τα δεδομένα αυτά αποθηκεύονται και ανακτώνται από το

	intent με τις μεθόδους putExtras() και getExtras() σε μορφή ζευγαριών κλειδιού/τιμής.
Flags	Τιμές που καθορίζουν τον τρόπο που το Android πρέπει να εκτελέσει ένα activity καθώς και πως θα το χειριστεί μετά την εκκίνηση του,

Τα intents μπορεί να είναι explicit ή implicit. Σε ένα explicit intent το activity (ή το service κ.λπ) που θα εκτελεστεί είναι καθορισμένο. Ο καθορισμός αυτός γίνεται από το πεδίο Όνομα Στοιχείου του intent και επειδή απαιτεί να γνωρίζουμε το πλήρες όνομα της εκκινούμενης οντότητας συνήθως τα explicit intents περιορίζονται για επικοινωνία μέσα σε μια εφαρμογή.

Από την άλλη πλευρά τα implicit intents είναι πιο γενικά. Σε ένα implicit intent δεν καθορίζεται κάποιο όνομα για την εκκινούμενη οντότητα, αλλά μόνο ο τύπος που επιθυμούμε αυτή να έχει. Τα implicit intents χρησιμοποιούνται για την εκκίνηση οντοτήτων που ανήκουν σε άλλες εφαρμογές.

Ένα παράδειγμα ενός explicit intent, φαίνεται στην παρακάτω εικόνα :

```
private AdapterView.OnItemClickListener categoryListClickListener = new AdapterView.OnItemClickListener()
{
    @Override
    public void onItemClick(AdapterView<?> arg0, View arg1, int position, long arg3)
    {
        // Create an intent to start another activity. Extra parameters
        // for the new activity are specified here
        Intent intent = new Intent(ShowCategory.this, ShowEventCategory.class);
        intent.putExtra("nmCategory", categoryName[position]);
        intent.putExtra("idEventCategory", categoryID[position]);
        startActivity(intent);
    }
};
```

Σχήμα 10 Εκκίνηση ενός activity με χρήση ενός intent

Βλέπουμε τον καθορισμό της κλάσης που θα λάβει το intent (ShowEventCategory.class) καθώς και την προσθήκη κάποιων επιπλέων

δεδομένων με χρήση της μεθόδου ***putExtra()***. Όταν ξεκινήσει το activity που περιγράφει η κλάση ShowEventCategory, μπορεί να αποκτήσει πρόσβαση σε αυτά τα δεδομένα χρησιμοποιώντας την μέθοδο ***getExtras()***.

```
@Override
public void onCreate(Bundle savedInstanceState)
{
    super.onCreate(savedInstanceState);
    setTitle(getIntent().getExtras().getString("nmCategory") + " Events");
    setContentView(R.layout.show_event_category);

    ...
}
```

Σχήμα 11 Ανάκτηση πληροφοριών από intent

Η λογική που ακολουθούν τα implicit intents είναι λίγο διαφορετική. Επειδή σε ένα implicit intent δεν υπάρχουν διαθέσιμες πληροφορίες για το ποια κλάση ακριβώς πρέπει να ενεργοποιηθεί, το Android αναζητά μια κατάλληλη για την εκάστοτε ενέργεια. Για να το κάνει αυτό πρέπει να ξέρει τι είδους ενέργειες μπορεί να χειριστεί κάθε activity που υπάρχει στο σύστημα. Αυτού του είδους την ενημέρωση την κάνουν τα ίδια τα activity μέσα από το AndroidManifest αρχείο με χρήση των intent filters. Στα intent filters που βρίσκονται στο AndroidManifest αρχείο για κάθε activity ορίζονται οι ενέργειες που μπορεί να χειριστεί αυτό το activity, οι κατηγορίες που μπορεί να χειριστεί και ο τύπος των δεδομένων πάνω στον οποίο μπορεί να επιδράσει. Παρατηρούμε ότι αυτά είναι τρία από τα πεδία ενός intent (Ενέργεια, Κατηγορία και Δεδομένα). Έτσι, το Android, αναζητά μια οντότητα της οποίας το intent filter να ταυτίζεται με τα αντίστοιχα πεδία του intent που προσπαθεί να εξυπηρετήσει.

2.3.5 Resources

Για την ανάπτυξη μιας καλής εφαρμογής σπάνια ο κώδικας είναι αρκετός. Οι πόροι είναι όλα τα επιπλέον αρχεία στατικού περιεχομένου, που η εφαρμογή μας αξιοποιεί προκειμένου να προσφέρει μια εμπειρία χρήσης υψηλών προδιαγραφών στους χρήστες της.

Πόροι μιας εφαρμογής μπορεί να είναι οι εικόνες της, τα χρώματά που αυτή χρησιμοποιεί, όλα τα λεκτικά που εμφανίζονται στις οθόνες της, οι διαστάσεις των διαφόρων στοιχείων των διεπαφών της, οι περιγραφή των διατάξεων των διεπαφών της καθώς και πολλά άλλα. Όλοι οι πόροι, αναπαρίστανται με κατάλληλη μορφή και αποθηκεύονται σε κατάλληλο υποφάκελο του φακέλου res στην δομή του project. Οι εικόνες αποθηκεύονται στον υποφάκελο drawable, τα χρώματα, τα λεκτικά και οι διαστάσεις περιγράφονται σε XML και αποθηκεύονται στον υποφάκελο values ενώ οι περιγραφές των διατάξεων των διεπαφών χρήστη περιγράφονται επίσης σε XML και αποθηκεύονται στον υποφάκελο layout.

Η διατήρηση χωριστών αρχείων για τους πόρους είναι μια τακτική που έχει θετικά αποτελέσματα για την ανάπτυξη μιας εφαρμογής. Βασικό πλεονέκτημα είναι ότι επιτρέπεται να γίνεται συντήρηση και ανάπτυξη των πόρων χωριστά από την συντήρηση και ανάπτυξη του κώδικα της εφαρμογής. Συνάμα, έχουμε την δυνατότητα να παρέχουμε επιπλέον πόρους τους οποίους η εφαρμογή μπορεί να χρησιμοποιεί σε διαφορετικές περιπτώσεις χρήσης. Χαρακτηριστικό παράδειγμα είναι η παροχή των λεκτικών της σε διαφορετικές γλώσσες. Η εφαρμογή έχοντας στην διάθεσή της όλα τα λεκτικά σε διαφορετικές γλώσσες μπορεί κατά την εκτέλεση της να επιλέξει ποια γλώσσα θα προβάλει. Έτσι, πετυχαίνουμε με εύκολο τρόπο (και εύκολα συντηρήσιμο και επεκτάσιμο) πολυγλωσσικό περιεχόμενο για τις εφαρμογές μας.

Η δυνατότητα παροχής εναλλακτικών πόρων που είδαμε παραπάνω (παράδειγμα πολυγλωσσικού περιεχομένου) ισχύει για όλους του τύπους πόρων που υποστηρίζει το Android. Γενικά οι πόροι χωρίζονται σε δυο κατηγορίες, στους προκαθορισμένους πόρους και τους εναλλακτικούς.

Οι προκαθορισμένοι πόροι είναι αυτοί τους οποίους η εφαρμογή χρησιμοποιεί ανεξάρτητα από τις ρυθμίσεις και την κατάσταση της συσκευής στην οποία τρέχει ή όταν δεν υπάρχει εναλλακτικός πόρος που να καλύπτει την τρέχουσα κατάσταση της συσκευής. Οι εναλλακτικοί πόροι είναι οι πόροι που θα χρησιμοποιηθούν όταν η συσκευή βρεθεί στην κατάσταση στην οποία αντιστοιχούν αυτοί οι πόροι. Μια πολύ σημαντική περίπτωση όπου η παροχή εναλλακτικών πόρων μπορεί να αποβεί καθοριστικής σημασίας για την εφαρμογή μας είναι αυτή της παροχής εναλλακτικών διατάξεων διεπαφών. Όταν η εφαρμογή μας εκτελείται σε μια συσκευή με μεγαλύτερη οθόνη μπορούμε να εμφανίσουμε μια τελείως διαφορετική διεπαφή η οποία να εκμεταλλεύεται καλύτερα την επιπλέον διαθέσιμη επιφάνεια.

2.3.6 Το αρχείο Android Manifest

Κάθε Android project περιλαμβάνει ένα αρχείο manifest, το AndroidManifest.xml, που αποθηκεύεται στην κορυφή της ιεραρχίας των αρχείων στο project. Το manifest ορίζει τη δομή και τα μεταδεδομένα της εφαρμογής, τα συστατικά της και τις απαιτήσεις της. Περιλαμβάνει κόμβους για κάθε μια από τις Activities, Services, Content Providers και Broadcast Receivers που αποτελούν μια εφαρμογή και χρησιμοποιώντας τα Intent Filters και τα Permissions καθορίζει πως θα αλληλοεπιδρούν μεταξύ τους και με άλλες εφαρμογές. Το manifest μπορεί επίσης να καθορίσει τα μεταδεδομένα της εφαρμογής (όπως τα icons, τον αριθμό της έκδοσης ή το theme) και επιπρόσθετους κόμβους στο top-level που ορίζουν τα απαιτούμενα permissions, τα unit tests ενώ ορίζονται και τις απαιτήσεις ως προς το υλικό, την οθόνη και την πλατφόρμα. Το manifest αποτελείται από το root tag manifest το οποίο περιέχει ένα package attribute που ορίζεται στο πακέτο του project. Περιλαμβάνει επίσης και ένα xmlns:android attribute που παρέχει διάφορα attributes συστήματος που χρησιμοποιούνται μέσα στο αρχείο. Χρησιμοποιούμε το attribute versionCode για να ορίσουμε την τρέχουσα έκδοση της εφαρμογής σαν έναν ακέραιο που αυξάνει με κάθε σημαντική αλλαγή στην εφαρμογή και χρησιμοποιούμε το versionName attribute για να καθορίσουμε το όνομα της έκδοσης που θα είναι ορατή στους χρήστες. Μπορούμε επίσης να ορίσουμε αν θα επιτρέπεται ή αν είναι επιθυμητό να εγκαθίσταται η εφαρμογή σε εξωτερικό

αποθηκευτικό μέσο (συνήθως μια κάρτα SD) αντί μιας εσωτερικής πηγής χρησιμοποιώντας το attribute installLocation, θέτοντας την τιμή preferExternal ή auto, όπου η πρώτη εγκαθιστά την εφαρμογή σε εξωτερικό μέσο όποτε είναι δυνατό και η δεύτερη αφήνει την απόφαση στο σύστημα. Αν δεν ορίσουμε το attribute αυτό, η εφαρμογή θα εγκατασταθεί στην εσωτερική μνήμη και οι χρήστες δεν θα μπορούν να τη μεταφέρουν σε κάποια εξωτερική. Επειδή η εσωτερική μνήμη είναι περιορισμένη, είναι καλό, όποτε αυτό είναι δυνατό, να εγκαθιστούμε την εφαρμογή στην εξωτερική μνήμη.

2.4 Επίλογος

Συνοψίζοντας, σε αυτό το κεφάλαιο παρουσιάζονται αρχικά τα βασικά χαρακτηριστικά με τα οποία μπορεί να χτιστεί μια Android εφαρμογή όπως είναι τα activities, τα services και ο content provider και ο broadcast receiver. Στην συνέχεια γίνεται αναλυτική περιγραφή κάποιων επιπρόσθετων χαρακτηριστικών τα οποία είναι σημαντικά μια την δημιουργία μιας ολοκληρωμένης εφαρμογής αυτά είναι τα fragments, τα views, τα layouts, τα intents, τα resources και η διαχείρηση του αρχείου Android manifest.

ΚΕΦΑΛΑΙΟ 3

3 PHISHING

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί η έννοια του phishing, η εξέλιξή του με το πέρασμα των χρόνων, οι παράγοντες κοινωνικής μηχανικής οι οποίοι ευνοούν την εξάπλωση του phishing, θα παρουσιαστεί το πώς γίνεται η μεταφορά των μηνυμάτων phishing και οι τύποι phishing επιθέσεων και τέλος οι μηχανισμοί αντιμετώπισης που θα πρέπει να λειτουργήσουν ώστε να προστατευθεί ο χρήστης από το phishing.

3.2 Τι είναι το phishing

Το Phishing είναι μια ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή 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.

Αν ήταν εφικτό να αποδώσουμε τον όρο στα Ελληνικά, θα μπορούσαμε κάλλιστα να το αποκαλέσουμε 'Ηλεκτρονικό Ψάρεμα', κι αυτό γιατί αγγλικός όρος δεν απέχει πολύ από αυτό. Ο όρος Phishing, που πρωτοχρησιμοποιήθηκε από τον χάκερ Khan C Smith και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα των χάκερς, προέρχεται από το αγγλικό 'fishing' (ψάρεμα), καθώς η διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες, θυμίζει την διαδικασία του δολώματος στο ψάρεμα.

3.3 Η ιστορία του Phishing

Η λέξη ‘phishing’ αρχικά προέρχεται από την ορολογία την οποία οι εγκληματίες του Internet χρησιμοποιούσαν στέλνοντας e-mail δολώματα για να ‘ψαρέψουν’(phish) κωδικούς και οικονομικά δεδομένα από την ‘θάλασσα’ των χρηστών του Internet. Η χρησιμοποίηση του ‘ph’ ως όρου έχει χαθεί στο πέρασμα των χρόνων, αλλά πιθανότατα συνδέεται με την ονοματολογία την οποία

χρησιμοποιούσαν οι χάκερ όπως ο όρος ‘phreaks’ που χρησιμοποίησαν οι πρώτοι χάκερ που δημιούργησαν το ‘phreaking’ και ήταν το χακάρισμα των τηλεφωνικών συστημάτων. Ο όρος επινοήθηκε το 1996 από χάκερς οι οποίοι έκλεβαν από τους λογαριασμούς της εταιρίας AOL υποκλέπτοντας κωδικούς από ανυποψίαστους χρήστες. Η πρώτη αναφορά του phishing στο Internet έγινε στο alt.2600 ένα γκρουπ των χάκερ τον Ιανουάριο του 1996 παρόλα αυτά ο όρος χρησιμοποιήθηκε νωρίτερα στο δημοφιλές ενημερωτικό δελτίο των χάκερ το ‘2600’.

Από το 1996, οι χακαρισμένοι λογαριασμοί αναφέρονταν ως ‘phish’, και από το 1997 ενεργά τα phish αποτελούσαν ένα αντικείμενο διαπραγμάτευσης ανάμεσα στους χάκερς ως ένας τρόπος ηλεκτρονικού νομίσματος. Υπήρχαν στιγμές που οι phishers συνήθως αντάλλασσαν 10 phish της AOL για ένα κομμάτι χακαρισμένου λογισμικού ή warez (κλεμμένες πιστοποιημένες εφαρμογές ή παιχνίδια). Καμία νωρίτερη αναφορά των μέσων ενημέρωσης στο phishing δεν είχε γίνει μέχρι τον Μάρτιο του 1997.

Πίνακας 2 Η πρώτη αναφορά στον όρο phishing

Η απάτη ονομάζεται «phishing» - όπως και στο ψάρεμα έτσι και με τον κωδικό σας, αλλά γράφεται με διαφορετικό τρόπο - είπε η Τατιάνα Gau, αντιπρόεδρος της διασφάλισης της ακεραιότητας για τις online υπηρεσίες. -Ed Stansel, "Don't get caught by online 'phishers' angling for account information," Florida Times-Union, March 16, 1997

Με την πάροδο του χρόνου, ο ορισμός του τι συνιστά μια επίθεση phishing έχει αλλάξει και έχει επεκταθεί. Ο όρος phishing καλύπτει όχι μόνο την απόκτηση των λεπτομερειών του λογαριασμού χρήστη, αλλά περιλαμβάνει επίσης την πρόσβαση σε προσωπικά και οικονομικά δεδομένα. Αυτό που αρχικά συνεπαγόταν σε εξαπάτηση των χρηστών με μια απάντηση σε e-mail για τους κωδικούς πρόσβασης και τα στοιχεία της πιστωτικής κάρτας, έχει πλέον επεκταθεί σε πλαστές ιστοσελίδες, εγκατάσταση δούρειων ίππων που γίνονται διαχειριστές κλειδιών, λήψη στιγμιότυπων οθόνης και σε man-in-the-middle proxies δεδομένων με όλα αυτά να παραδίδονται μέσω οποιουδήποτε ηλεκτρονικού καναλιού επικοινωνίας.

Λόγω του υψηλού ποσοστού επιτυχίας των phishers, η επέκταση του κλασικού phishing περιλαμβάνει τώρα τη χρήση των πλαστών ιστοσελίδων που

προσφέρουν δουλειά ή πλαστές προσφορές εργασίας. Οι υποψήφιοι δελεάζονται με την ιδέα να βγάλουν πολλά χρήματα με πολύ λίγη εργασία, δημιουργώντας απλά ένα νέο τραπεζικό λογαριασμό, λαμβάνοντας τα κεφάλαια που έχουν μεταφερθεί σε αυτό και αποστέλλοντας τα σε ένα διεθνή λογαριασμό χρημάτων – μια κλασική τεχνική ξεπλύματος χρήματος.

3.4 Η απειλή του phishing

3.4.1 Παράγοντες κοινωνικής μηχανικής

Οι επιθέσεις phishing βασίζονται σε μια μίξη από τεχνικές εξαπάτησης και προσπάθειες κοινωνικής μηχανικής. Στο μεγαλύτερο μέρος των περιπτώσεων, ο επιτιθέμενος πρέπει να πείσει το θύμα να προβεί άθελα του σε ένα σύνολο ενεργειών, που θα αποφέρουν στον επιτιθέμενο πρόσβαση σε εμπιστευτικές πληροφορίες.

Κανάλια επικοινωνίας όπως e-mails, ιστοσελίδες και άμεση ανταλλαγή μηνυμάτων αποτελούν τις πιο γνωστές υπηρεσίες για να επιτευχθεί το phishing. Σε όλες τις περιπτώσεις, ο επιτιθέμενος πρέπει να μιμηθεί κάποια έμπιστη πηγή(όπως το γραφείο βοήθειας μιας τράπεζας, την άμεση υποστήριξη από έναν προμηθευτή τους κτλ) έτσι ώστε το θύμα για να πεισθεί.

Οι πιο επιτυχημένες επιθέσεις phishing συνεχίζουν να γίνονται μέσω e-mails, με τον επιτιθέμενο να μιμείται κάποια έμπιστη πηγή(τέτοια ώστε να πλαστογραφήσει την διεύθυνση αποστολέα και να παραθέσει κάποια κατάλληλα εταιρικά λογότυπα μέσα στο email, με στόχο να γίνει πιο πιστευτός).

Για παράδειγμα, το θύμα λαμβάνει ένα email που υποτίθεται έχει στείλει το τμήμα υποστήριξης της τράπεζας, με την ηλεκτρονική διεύθυνση support@mybank.com(η διεύθυνση έχει πλαστογραφηθεί) και έχει σταλεί στον χρήστη με Θέμα : Ανακοίνωση ασφαλείας, ζητώντας από τον χρήστη να ακολουθήσει ένα συγκεκριμένο υπερσύνδεσμο(link) www.mybank_validate.info (μια διεύθυνση η οποία ανήκει στον επιτιθέμενο και ΟΧΙ στην τράπεζα) και να πληκτρολογήσει τον προσωπικό PIN κωδικό του για λόγους ασφαλείας.

Ωστόσο, ο επιτιθέμενος έχει πολλές άλλες εναλλακτικές μεθόδους για να ασκήσει κοινωνική μηχανική σε θύματα, με σκοπό να αποκομίσουν εμπιστευτικές

πληροφορίες. Ακολουθεί ένα παράδειγμα χρήστης κοινωνικής μηχανικής, όπου ο παραλήπτης είναι πιθανότατα να έχει πιστέψει πως οι τραπεζικές του πληροφορίες έχουν χρησιμοποιηθεί από κάποιον άλλον, ο οποίος επιχείρησε να πάρει εξουσιοδότηση σε κάποιες υπηρεσίες του λογαριασμού του. Το θύμα στην συνέχεια, θα προσπαθήσει να επικοινωνήσει με το email της τράπεζας που αναγράφεται, για να τους ενημερώσει για το πιθανόν πρόβλημα και να ακυρώσει την συναλλαγή. Σύμφωνα με τις λεπτομέρειες της απάτης, ο επιτιθέμενος θα ενημερώσει τον χρήστη(ή θα του παρέχει μια ψεύτικη “ασφαλής” ιστοσελίδα) ότι πρέπει να πληκτρολογήσει εμπιστευτικές πληροφορίες, όπως την διεύθυνση του, τον αριθμό πιστωτικής κάρτας και τον προσωπικό του κωδικό, έτσι ώστε να ακυρώσει την συναλλαγή – με βάση τα οποία πιθανόν να πουλήσει σε άλλους επίδοξους χάκερ ή να πραγματοποιήσει ο ίδιος μια κανονική, πλέον, συναλλαγή.

```
Subject: Web Hosting - Receipt of Payment
QdRvxrOeahwL9xaxdamLRAIe3NM1rL

Dear friend,

Thank you for your purchase!
This message is to inform you that your order has been received
and will be processed shortly.

Your account is being processed for $79.85, for a 3 month term.
You will receive an account setup confirmation within the next
24 hours with instructions on how to access your account.
If you have any questions regarding this invoice, please feel free
to contact us at tekriter.com.
We appreciate your business and look forward to a great
relationship!

Thank You,

The Tekriter.com Team


ORDER SUMMARY
-------------
Web Hosting..... $29.85
Setup..... $30.00

Domain Registration..... $20.00
Sales Date..... 08/04/2004
Domain..... nashshanklin.com

Total Price..... $79.85
Card Type..... Visa
```

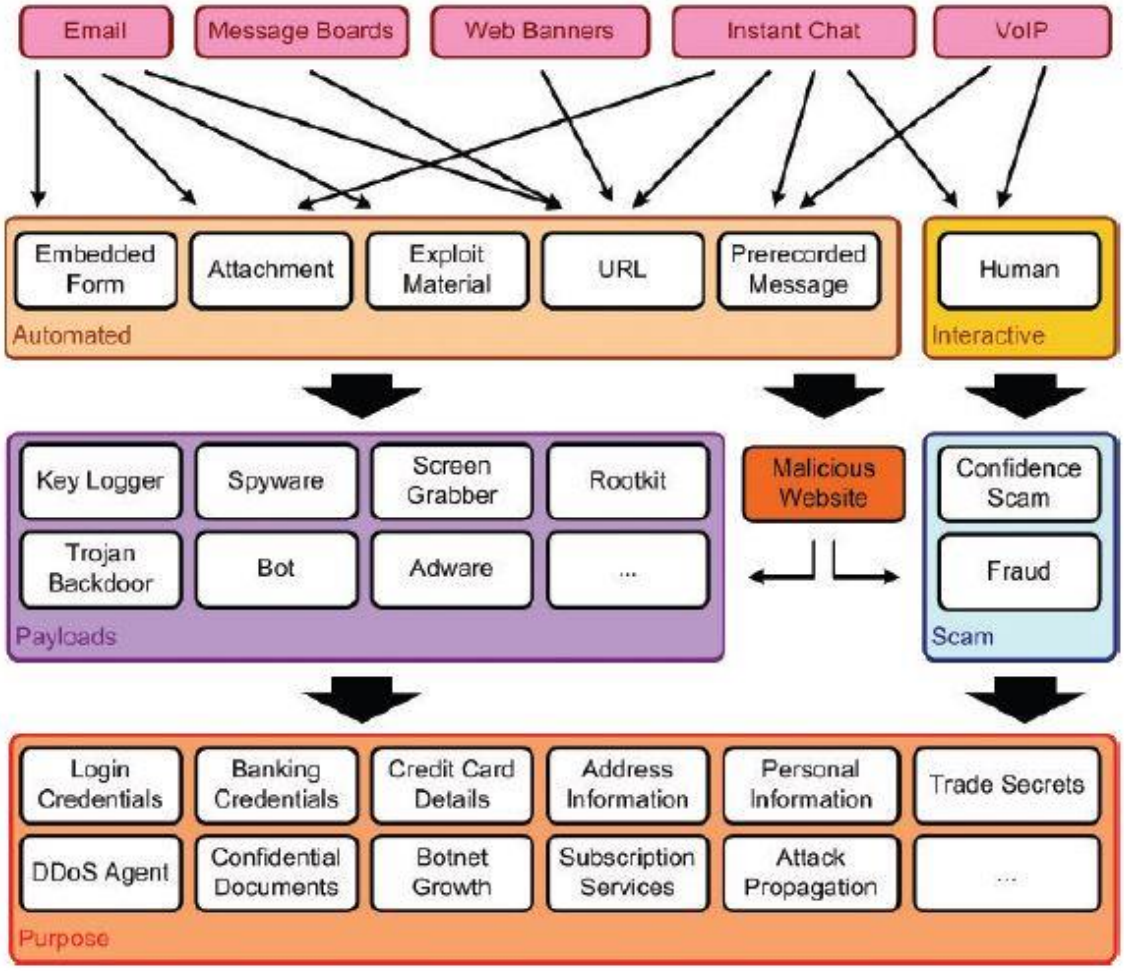
Σχήμα 12 Παράδειγμα phishing e-mail

3.4.1.1 Ο σκοπός του Phishing

Ο όρος στο τι είναι μια επίθεση phishing, έχει αλλάξει τα τελευταία 15 χρόνια. Ο αρχικός σκοπός του phishing ήταν η απόκτηση των στοιχείων εισόδου των καταναλωτών, χρησιμοποιώντας το ίδιο τμήμα με το οποίο ήρθαν σε επαφή οι καταναλωτές για πρώτη φορά μετά την αγορά τους. Για αρκετό καιρό, οι επιτιθέμενοι εστίαζαν στην κλοπή των προσωπικών στοιχείων εισόδου χρησιμοποιώντας emails το ίδιο email για να αποστείλουν ένα ψεύτικο μήνυμα και για να λάβουν πίσω την απάντηση, με τα πιθανός εμπιστευτικά στοιχεία. Για παράδειγμα, ο επιτιθέμενος έστελνε ένα email ζητώντας από τον παραλήπτη να τους απαντήσει με τις απαραίτητες πληροφορίες. Όταν οι παραλήπτες τέτοιων μηνυμάτων, άρχισαν να καταλαβαίνουν τον τρόπο λειτουργίας τους και αυτή η μέθοδος σταμάτησε να είναι το ίδιο αποδοτική, οι επιτιθέμενοι άλλαξαν τον τρόπο αποστολής και λήψης των παραπλανητικών emails, αυξάνοντας την πολυπλοκότητά τους, με σκοπό αυτά να γίνονται δυσκολότερα αντιληπτά.

Στις μέρες μας, οι επιτιθέμενοι συνεχίζουν να χρησιμοποιούν την τεχνική των mails, αλλά επίσης έχουν περάσει και σε άλλους τομείς, συμπεριλαμβάνοντας πίνακες μηνυμάτων σε ιστοσελίδες, banner με διαφημίσεις, άμεση και ζωντανή συνομιλία, ενώ πρόσφατα πέρασαν και στο VOIP(Voice Over IP) για να παραδώσουν τα πειστικά μηνύματα τους και να πείσουν τα θύματα είτε να απαντήσουν με τα στοιχεία εισόδου τους ή να τους οδηγήσουν σε μια πιο ολοκληρωμένη εφαρμογή, η οποία μέσω ενός μηχανισμού θα έκλεβε τα στοιχεία τους.

Ο πιο διάσημος μηχανισμός να αποκτήσουν οι επιτιθέμενοι τις πληροφορίες και τα στοιχεία εισόδου του θύματος σήμερα, είναι να αναπτύξουν και να σχεδιάσουν ιστοσελίδες για να αναπαραστήσουν την πραγματική επιχείριση, από την οποία ήρθε το εκάστοτε μήνυμα. Όμως, τα τελευταία χρόνια υπάρχουν κρούσματα που αναφέρουν ότι οι επίδοξοι 'ληστές', με τις καινούργιες τους τεχνικές, στέλνουν στα θύματά τους συμπιεσμένα αρχεία όπως τα key loggers, spyware, rootkits, bots κτλ τα οποία καταγράφουν τις ενέργειες που έκανε το θύμα και τα στοιχεία που εισήγαγε σε κάποιο σύστημα, και έπειτα τα στέλνουν πίσω στον επιτιθέμενο χρήστη.



Σχήμα 13 Τρόποι που χρησιμοποιούνται για Phishing

Η ραγδαία ανάπτυξη στις τεχνικές αποστολής και η πρόσβαση σε πιο σύνθετα προγράμματα σημαίνει ότι το κίνητρο και οι οικονομικές απολαβές για το phishing έχει αλλάξει και θα συνεχίσει να εξελίσσεται στο μέλλον. Μερικοί βασικοί λόγοι για τους οποίους γίνεται το phishing, περιλαμβάνουν :

- Κλοπή στοιχείων εισόδου-συνήθως στοιχείων για την πρόσβαση σε online υπηρεσίες όπως το eBay, το Hotmail κτλ. Πιο πρόσφατα, η αύξηση των συναλλαγών μέσω διαδικτύου, είχε σαν αποτέλεσμα τα στοιχεία εισόδου των χρηστών να χρησιμοποιούνται αρκετά και πιο εύκολα σε συναλλαγές μέσω διαδικτύου, πράγμα που σήμαινε πως ήταν πιο ευάλωτοι σε τέτοιες επιθέσεις.
- Κλοπή στοιχείων τραπέζης – Συνήθως τα στοιχεία εισόδου της διαδικτυακής υπηρεσίας της τράπεζας είναι πιο γνωστά, για τον

λόγο του ότι οι επιτιθέμενοι είχαν άμεση πρόσβαση σε κεφάλαια και χρήματα, τα οποία ήταν έτοιμα προς μεταφορά

- Πρόσβαση και παρατήρηση στοιχείων της Πιστωτικής κάρτας-πρόσβαση σε έναν μεγάλο αριθμό πληροφοριών της πιστωτικής κάρτας, όπως τον αριθμό της, της ημερομηνία λήξης της, το όνομα του δικαιούχου, τον προσωπικό αριθμό επικύρωσης της. Αυτά τα στοιχεία απέκτησαν άμεσα μεγαλύτερη αξία προς τους εγκληματίες.
- Καταγραφή και ενημέρωση για την διεύθυνση και άλλες προσωπικές πληροφορίες-οποιαδήποτε πληροφορία, ειδικά η διεύθυνση του χρήστη, είναι μεγάλης μεταπολιτικής αξίας και έχει υψηλή ζήτηση σε εταιρίες μάρκετινγκ.
- Κλοπή από μυστικά και απόρρητα έγγραφα – οι εγκληματίες έχουν στο στόχαστρο συγκεκριμένες επιχειρήσεις με σκοπό να υποκλέψουν πληροφορίες και μυστικά, έτσι ώστε να τα πουλήσουν σε αντίπαλες εταιρίες.
- Διανομή αρχείων bot και DdoS στοιχείων – οι εγκληματίες χρησιμοποιούν απάτες phishing για να εγκαταστήσουν ειδικό λογισμικό τύπου bot και DDoS σε ανυποψίαστους υπολογιστές και στην συνέχεια να τους προσθέσουν στο δικό τους δίκτυο. Στην συνέχεια, αυτοί οι μολυσμένοι υπολογιστές μπορούν να νοικιαστούν σε άλλους εγκληματίες, με απώτερο σκοπό μια μεγαλύτερη και συντονισμένη επίθεση.
- Επιθέσεις Διάδοσης – Μέσα από μια μίξη στυγνού phishing και εγκατάστασης bots, οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν έναν μολυσμένο υπολογιστή-σταθμό για να εξαπολύσουν από εκεί μια επίθεση, καλύπτοντας πλήρως τα ίχνη τους.

3.4.1.2 Πλαστογραφώντας τα πιστοποιητικά Γνησιότητας

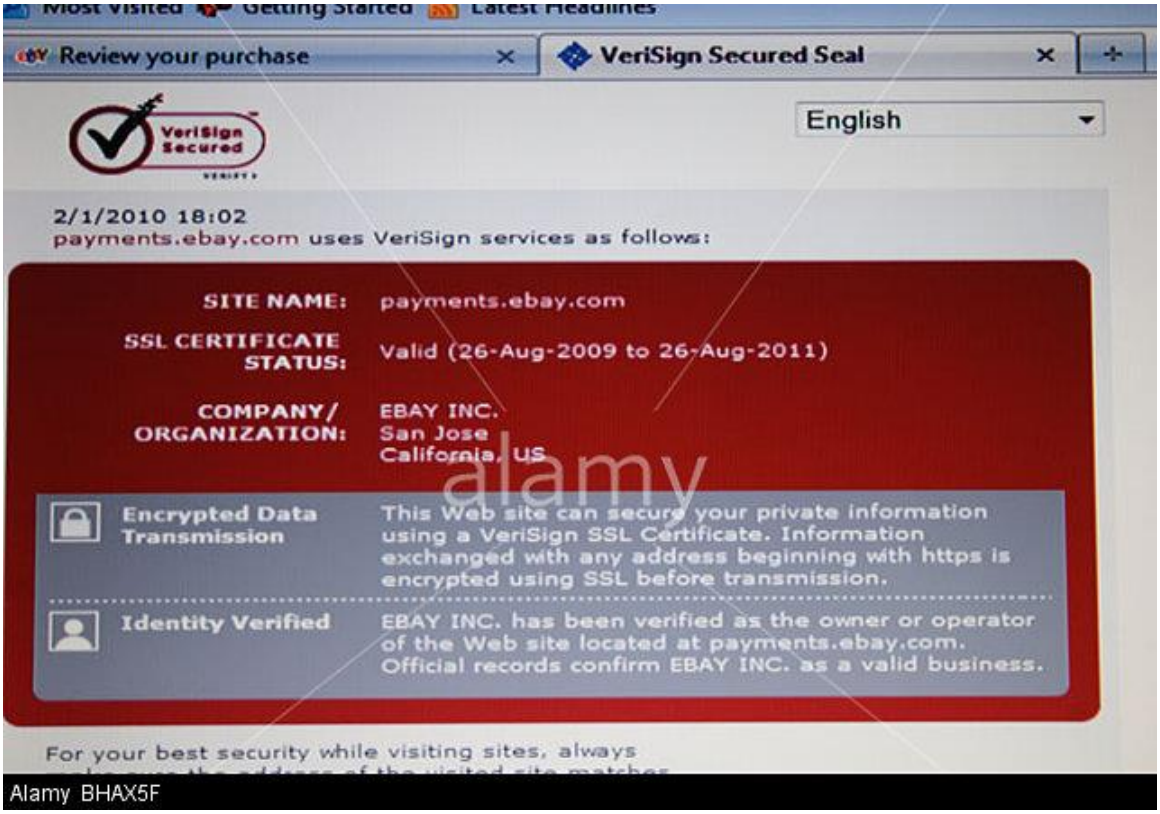
Σε μια προσπάθεια να αντιμετωπίσουν το phishing και άλλες απάτες, οι οποίες στηρίζονται στην δημιουργία ψεύτικων ιστοσελίδων ως βασική τους μέθοδο για να

κλέψουν τα στοιχεία εισόδου των χρηστών, πολλοί οργανισμοί ανέπτυξαν ένα σύστημα επικύρωσης 3rd party. Αυτού του είδους οι υπηρεσίες συνήθως παρουσιάζονται ως ένα γραφικό στοιχείο τοποθετημένο στην ιστοσελίδα, το οποίο είναι ένας ενεργός σύνδεσμος που οδηγεί σε μια έγκυρη πηγή για την επικύρωση ότι αυτή η ιστοσελίδα είναι η αυθεντική και είναι συνήθως συμπληρωματικό του SLL πιστοποιητικού, που παρουσιάζεται στην επίσημη ιστοσελίδα.

Επειδή αυτού του είδους οι γραφικές απεικονίσεις συνήθως χρησιμοποιούν απλά γραφικά και popup μηνύματα, είναι ευπαθής στην πλαστογραφία. Η συγκεκριμένη τακτική έχει λάβει μεγάλη φήμη, λόγο της αυξανόμενης επιτυχίας της, μιας και αρκετοί πελάτες εμπιστεύονται τέτοιου είδους πιστοποιητικά πιο εύκολα. Η παρακάτω εικόνα, είναι ένα παράδειγμα γραφικού που πλαστογραφούνε οι εγκληματίες προκειμένου να πείσουν τον χρήστη πως είναι η επίσημη ιστοσελίδα.

Σχήμα 14 Το λογότυπο της Verisign

Αυτά τα γραφικά tokens, συνήθως υποστηρίζονται από Links για 3rd party επικυρώσεις αυθεντικότητας, που ενημερώνουν τον χρήστη με το μήνυμα ότι “αυτό το site είναι έμπιστο», σε όσους πελάτες κλικάρουν σε αυτό. Τα μηνύματα αυτά είναι εύκολο να πλαστογραφηθούν και για αυτό οι εγκληματίες τα προσθέτουν στον ιστότοπό τους, με σκοπό να αυξήσουν την εμπιστοσύνη του χρήστη πως την ιστοσελίδα.



Σχήμα 15 Η σφραγίδα της Verisign

3.4.2 Μεταφορά phishing μηνυμάτων

3.4.2.1 E-mail και Spam

Οι επιθέσεις phishing με βάση τα e-mails είναι οι πιο συχνές. Χρησιμοποιώντας τεχνικές και εργαλεία που χρησιμοποιούν οι Spammers, οι phishers μπορούν να παραδώσουν ειδικά κατασκευασμένα mails σε εκατομμύρια ενεργές διευθύνσεις μέσα σε μερικές ώρες(ή λεπτά, χρησιμοποιώντας το δίκτυο με τους μολυσμένους με Trojan υπολογιστές). Σε πολλές περιπτώσεις, οι λίστες με τα εκατομμύρια αυτά mails, αγοράζονται από τις ίδιες που αναφέραμε προηγουμένως, από αυτούς δηλαδή που μαζεύουν πληροφορίες για να τις πουλήσουν.

Χρησιμοποιώντας μερικά κενά στο βασικό πρωτόκολλο επικοινωνίας των mail servers, οι εγκληματίες είναι ικανοί να δημιουργήσουν e-mails με πλαστογραφημένα τα στοιχεία αποστολής όπως το “ Μήνυμα Από : “ και να

μιμηθούν οποιονδήποτε οργανισμό αυτοί επιθιμούν. Πολλές φορές επίσης, προσθέτουν και το έξτρα πεδίο “ Απάντηση σε” με μια δικιά τους διεύθυνση, έτσι ώστε αν κάποιος χρήστης προσπαθήσει να απαντήσει σε αυτό το μήνυμα, τότε να πάει κατευθείαν σε αυτούς. Αρκετές μετρήσεις, έχουν δείξει ότι το μεγαλύτερο πλήθος των χρηστών είναι δεν πείθονται εύκολα στο να στείλουν εμπιστευτικές πληροφορίες(όπως αριθμούς και κωδικούς καρτών) μέσω e-mail, παρόλα αυτά όμως αυτή η τεχνική είναι πολύ επιτυχημένη σε αρκετές περιπτώσεις.

Τεχνικές που χρησιμοποιούνται εντός των Phishing E-mails

Με στόχο να μην πέφτουν οι χρήστες θύματα των phishing mails, είναι σημαντικό να καταλάβουν τις τεχνικές που χρησιμοποιούνται κυρίως από τους εγκληματίες για να ξεγελάσουν τα υποψήφια θύματα τους. Παρακάτω παραθέτουμε αυτές τις τεχνικές :

- **Mails τα οποία φαίνονται και μοιάζουν επίσημα -** Χρησιμοποιώντας σωστό συντακτικό και δομή στα μηνύματά τους, οι εγκληματίες έχουν καταφέρει να εισάγουν την κατάλληλη εμπιστοσύνη μέσα στα μηνύματά τους. Στα αρχικά χρόνια της ανάπτυξης του phishing, τα mails ήταν κακώς γραμμένα και αναγνωρίζονταν πολύ συχνά ως ψεύτικα. Στις σήμερον ημέρες, τα mails αυτά είναι σχεδόν απίθανο να καταλάβει κανείς αν είναι από την αληθινή πηγή τους. Σε μερικές περιπτώσεις φυσικά, μερικά από αυτά τα mails είναι ακριβώς αντιγραμμένα από ένα αυθεντικό μήνυμα που έχει σταλεί από την επίσημη εταιρία, με μερικές αλλαγές στα Urls.
- **Mails γραμμένα σε HTML χρησιμοποιούνται για να αποπροσανατολίσουν τις πληροφορίες των URL-** Μιας και η HTML είναι μια ερμηνευτική γλώσσα, είναι εύκολο κανείς να αλλάξει την κατάληξη των URL links με μερικές τεχνικές. Για παράδειγμα :
    - Χρησιμοποιώντας ένα ίδιο χρώμα όπως το παρασκήνιο, έτσι ώστε να αποκρύψουν λεπτομέρειες της Url που θα τους προδώσουν
    - Στην Html το tag <A HREF> σημαίνει το url της διαδρομής, αλλά το συγκεκριμένο στοιχείο μπορεί να αντικατασταθεί από οποιοδήποτε κείμενο String και συνήθως 'κλείνει' με το

tag </A>.Βασική προϋπόθεση, είναι να χρησιμοποιηθεί ένα έγκυρο κείμενο, ενώ το link οδηγεί σε ένα phishing URL

- Η μεταμφίεση των γραφικών έτσι ώστε να φαίνεται σαν ένα κείμενο ή ένα URL
- Το μήνυμα σε HTML Μορφή μπορεί να τροποποιηθεί κατάλληλα, έτσι ώστε να δείχνει ακριβώς όπως ένα απλό και κανονικό κείμενο σε ένα mail

- **Συνημμένα σε E-mails -** Μερικά παραπλανητικά mails, ίσως περιέχουν κάποια συνημμένα αρχεία. Αυτά τα αρχεία είναι πιθανόν να περιλαμβάνουν εκτελέσιμο περιεχόμενο ανάμεσα στο κείμενου του mail. Συνήθως υπάρχουν οδηγίες να ανοίξεις το “Ασφαλές” αυτό συνημμένο, με σκοπό να επικυρώσεις κάποιες λεπτομέρειες της συναλλαγής. Αυτά τα συνημμένα πιθανόν να εγκαταστήσουν ένα αρχείο τύπου 'Trojan keylogger' ή άλλο επικίνδυνο λογισμικό spyware.

- **Anti spam-εντοπισμός και εξαιρέσεις -** Μιας και πολλά phishing e-mails στέλνονται κατά εκατοντάδες σε πιθανά θύματα, βασιζόμενα αποκλειστικά και μόνο σε μια ηλεκτρονική διεύθυνση e-mail ή αποκτημένα από πολλαπλές πηγές, συνήθως αντιμετωπίζονται ως spam mails από το φίλτρο κατά του spamming και καταλήγουν στα Junk Incoming. Για να αποκλείσουν αυτό το ενδεχόμενο, πολλά νέα phishing e-mails προσθέτουν επιπλέον κείμενο, επικεφαλίδες SMTP και αναφορές σχεδιασμένες για να παρακάμπτουν αυτά τα φίλτρα.
- **Χρήση του ψεύτικου “Μήνυμα από : ” διευθύνσεων -** Μια συνηθισμένη πρακτική είναι η χρήση μιας ψεύτικης επικεφαλίδας “Μήνυμα από :” διευθύνσεων, στο ψεύτικο mail για να ξεγελάσουν τον παραλήπτη και να τον κάνουν να θεωρήσει πως το μήνυμα ήρθε από μια έγκυρη πηγή. Το πρωτόκολλο SMPT επιτρέπει στους αποστολείς να προσδιορίσουν οποιαδήποτε ηλεκτρονική διεύθυνση ταχυδρομείου αυτοί επιθυμούν.
- **Χρήση διαφορετικών φόντων και γραμματοσειράς -** Τα Fonts παίζουν έναν πολύ σημαντικό ρόλο στο οπλοστάσιο του εγκληματία phisher, όταν αυτός δημιουργεί ένα e-mail. Ένας από τους πιο

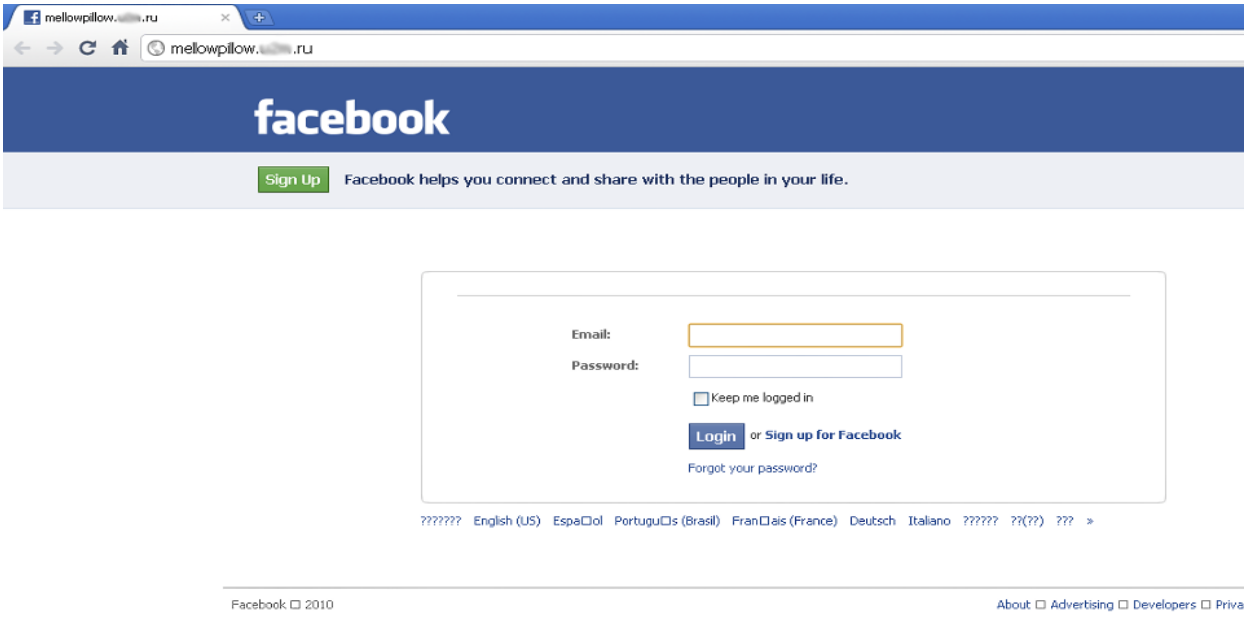
συνηθισμένους τρόπους, είναι να χρησιμοποιήσουν ένα font το οποίο δημιουργεί χαρακτήρες κεφαλαίων ή μικρών γραμμάτων, με σκοπό να εμφανιστούνε ως ένας διαφορετικός χαρακτήρας, πράγμα το οποίο συνηθίζεται για να παρακάμψουν τα φίλτρα λέξεων του anti-spam

- **Χρήση τοπικής γλώσσας -** Τα τελευταία χρόνια, υπάρχει μια μεγάλη έμφαση στη χρήση της γλώσσας, του κοινού στο οποίο απευθύνεται ο κάθε εγκληματίας. Οι phishers οι οποίοι στοχεύουν τους πελάτες μιας συγκεκριμένης οργάνωσης αντιλαμβάνονται ότι τα Αγγλικά(ακόμα και τα Αμερικάνικα των ΗΠΑ),μπορεί να μην είναι αρκετά και πλέον κατασκευάζουν τα e-mails τους χρησιμοποιώντας μια κατάλληλη γλώσσα-για παράδειγμα χρησιμοποιούν Γαλλικά, για να στοχεύσουν τους πελάτες στην Νότια Ελβετία
- **Αριθμοί πιστωτικών καρτών -** Μια διαρκώς αυξανόμενη γνωστή τεχνική, για να πείσουν τα υποψήφια θύματά τους οι εγκληματίες, είναι η χρήση των τεσσάρων πρώτων ψηφίων μιας πιστωτικής κάρτας σε ένα mail. Οι περισσότεροι άνθρωποι είναι συνηθισμένοι να βλέπουν τμήματα από τον αριθμό των πιστωτικών καρτών τους-συνήθως τα τελευταία ψηφία με τα υπόλοιπα σβησμένα. Αρκετά πιθανά θύματα όμως, δεν αντιλαμβάνονται ότι τα τέσσερα πρώτα ψηφία δεν είναι μοναδικά για την κάρτα τους, αλλά συνδέονται με έναν συγκεκριμένο τραπεζικό κωδικό της συγκεκριμένης τράπεζας.

Παράδειγμα phishing Real Time

Μία νέα επίθεση μέσω του Facebook στοχεύει τους ανυποψίαστους χρήστες και αποστέλλει μηνύματα phishing μέσα από παραβιασμένους λογαριασμούς, με σκοπό οι χρήστες να τα ακολουθήσουν και να μεταφερθούν σε μια εικονική σελίδα του Facebook, ώστε να καταχωρίσουν τα στοιχεία του λογαριασμού τους.

Προσέξτε όμως την παρακάτω εικόνα και θα εντοπίσετε ότι στο link που εμφανίζεται επάνω δεν αναφέρεται πουθενά το Facebook.

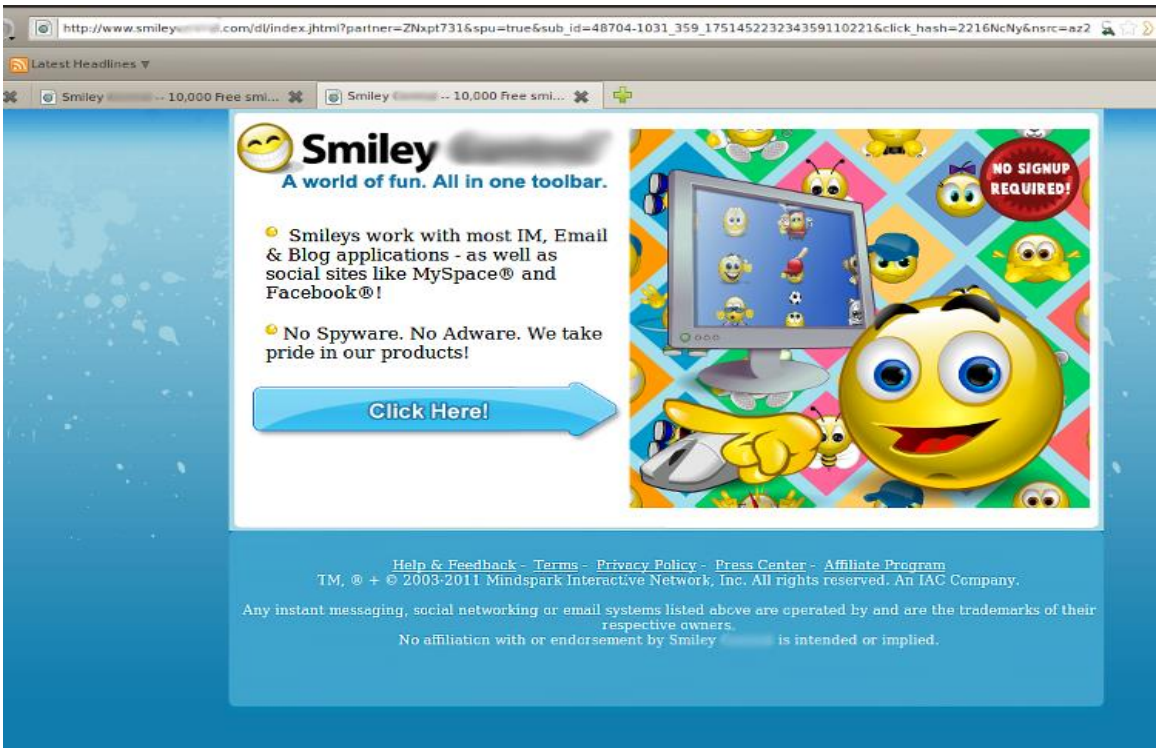


Σχήμα 16 Facebook Phishing (1)

Στη συνέχεια καταχωρίσαμε τα στοιχεία ενός δοκιμαστικού λογαριασμού για να ελεγχθεί η συνέχεια. Το αποτέλεσμα ήταν η παρακάτω εικόνα:

Σχήμα 17 Facebook Phishing (2)

Στη συνέχεια όπως βλέπετε σας προσφέρουν κάποια συσκευή δωρεάν, και ποιος δεν τη θέλει; Εάν λοιπόν κάνετε κλικ επάνω στο 'Claim Now' θα μεταφερθείτε στην παρακάτω ιστοσελίδα:

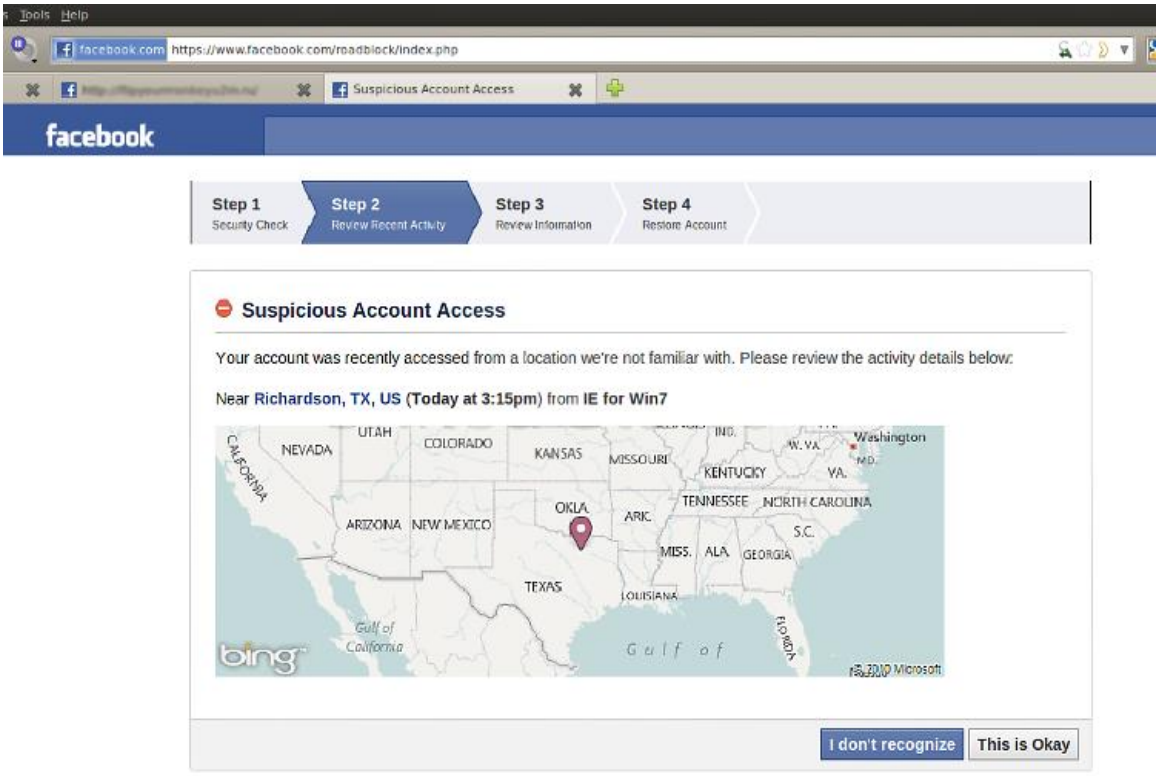


Σχήμα 18 Facebook Phishing (3)

Εάν τώρα κάνετε κλικ στο κουμπί με το βέλος τότε θα εμφανιστεί το παρακάτω μήνυμα όπου θα σας ζητάει να μεταφορτώσετε ένα αρχείο.

Σχήμα 19 Facebook Phishing (4)

Και εάν το μεταφορτώσετε τότε μόλις πληρώσατε με τον λογαριασμό σας ένα κακόβουλο λογισμικό που βρίσκεται τώρα στον υπολογιστή σας. Βέβαια στη συνέχεια το Facebook σας ενημερώνει για ύποπτη κίνηση στον λογαριασμό σας.



Σχήμα 20 Facebook Phishing (5)

Αυτό όμως δεν ισχύει, γιατί πάλι είναι παγίδα καθώς αν κάνετε κλικ στο 'I don't recognize' θα σας ζητηθεί να φτιάξετε νέο account για να επαναφέρετε τον λογαριασμό σας και φυσικά τα στοιχεία καταλήγουν στους επιτιθέμενους.

3.4.2.2 Μεταφορά μέσω Web-Based περιεχομένου

Η πιο διαδεδομένη μέθοδος για να εκτελεστεί μια επίθεση phishing είναι μέσω κακόβουλου περιεχομένου ιστοσελίδας. Το περιεχόμενο αυτό μπορεί να συμπεριλαμβάνεται σε μια ιστοσελίδα που έχει δημιουργηθεί από τον ίδιο τον εγκληματία, ή να είναι μια κανονική σελίδα που χωρίς την έγκρισή του ιδιοκτήτη της περιέχει κακόβουλο περιεχόμενο.

Οι τεχνικές μεταφοράς μέσω Web-Bases περιεχομένου περιλαμβάνουν :

- Η προσθήκη μεταμφιεσμένων HTML links ανάμεσα σε διάσημες ιστοσελίδες, και μέσα κοινωνικής δικτύωσης.
- Χρήση τρίτων ή ψεύτικων λογοτύπων-banner έτσι ώστε να μεταβούν οι πελάτες στην ιστοσελίδα του εγκληματία
- Ενσωμάτωση στην ιστοσελίδα των λεγόμενων web-bugs, τα οποία είναι καλά κρυμμένα στοιχεία μέσα στην ιστοσελίδα που εντοπίζουν πιθανούς χρήστες για 'ψάρεμα'
- Η χρήστη αναδυόμενων παραθύρων έτσι ώστε να 'μεταμφιέσουν' την αληθινή πηγή του μηνύματος του εγκληματία
- Ενσωμάτωση κακόβουλου λογισμικού στην ιστοσελίδα, το οποίο εντοπίζει κενά ασφαλείας στον browser του καταναλωτή και στη συνέχεια εγκαθιστά λογισμικό, της επιλογής του εγκληματία, στον υπολογιστή του θύματος(key-loggers, screen-grabbers, back-doors και άλλα προγράμματα Trojan)
- Αλλαγή των ρυθμίσεων του browser του θύματος, έτσι ώστε να γίνεται επιτρεπτή η εκτέλεση προγραμμάτων από τον χρήστη, δίχως να το γνωρίζει ο ίδιος

Διαφήμιση ψεύτικων banner

Η διαφήμιση μέσω banners είναι μια πολύ απλή μέθοδος που χρησιμοποιούν οι επιτιθέμενοι, με σκοπό να ανακατευθύνουν έναν πελάτη μιας εταιρίας σε ένα ψεύτικο site έτσι ώστε να του κλέψουν απόρρητες πληροφορίες. Χρησιμοποιώντας αντιγραμμένα banners διαφημίσεων και τοποθετώντας τα σε διάσημες ιστοσελίδες, το μόνο που μένει για τους εγκληματίες είναι με διάφορες, εύκολες, τεχνικές να ανακατευθύνουν το θύμα σε κάποιο άλλο site της επιλογής τους.

Σχήμα 21 Πλαστές Διαφημίσεις

Με τόσες πολλές εταιρίες που χρησιμοποιούν banners από τα οποία μπορούνε να διαλέξουν, είναι πολύ εύκολο για τους εγκληματίες να δημιουργήσουν λογαριασμούς και να παρέχουν banners όπως τα παραπάνω τα οποία οδηγούνε σε δικές τους ιστοσελίδες, ενώ ταυτόχρονα μπορούνε να τα ενσωματώσουν και σε πολλές ιστοσελίδες ταυτόχρονα. Χρησιμοποιώντας κλεμμένες ταυτότητες και πιστωτικές κάρτες χρηστών, οι εγκληματίες μπορούνε να προστατευτούνε ταυτόχρονα και από την σύλληψη.

3.4.2.3 Άμεση Συνομιλία (Chat)

Κάτι καινούργιο πλέον για τους εγκληματίες, αποτελεί η Άμεση Συνομιλία, μέσα από forums, μέσα κοινωνικής δικτύωσης και διάσημα sites. Καθώς τα συγκεκριμένα Chats άρχισαν να γίνονται συνεχώς και πιο γνωστά, προσθέτονταν στις ιστοσελίδες μεγαλύτερη πολυπλοκότητα, άρα και περισσότερα τμήματα κώδικα. Έτσι, αποτελούσε εύκολο κομμάτι για τους εγκληματίες η εύρεση οποιουδήποτε κενού ασφαλείας και οι χρήστες έμεναν εκτεθειμένοι.

Παράλληλα, όσο αυξανόταν η πολυπλοκότητα των ιστοσελίδων, οι χρήστες μπορούσαν να μοιραστούν με άλλους μέσω αυτής της συνομιλίας και δυναμικό περιεχόμενο, όπως URLs, γραφικά, πολυμέσα κ.α) μέσω των καναλιών της άμεσης συνομιλίας,πράγμα το οποίο επέτρεπε στους εγκληματίες να μπορούν με μεγαλύτερη ευκολία να βρούνε κενά ασφαλείας,άρα και να κλέψουν απόρρητες πληροφορίες.

Η βασική χρήστη των bots, μιας άλλης μορφής λογισμικού που χρησιμοποιούσαν οι χάκερς, ήταν να παίρνουν μέρος σε μεγάλες συνομιλίες ως χρήστες και να στέλνουν σχετικά links και ψεύτικες πληροφορίες στα υποψήφια θύματά τους.

3.4.2.4 Μολυσμένοι Υπολογιστές(Trojaned Hosts)

Αν και το μέσο μετάδοσης μιας επίθεσης phishing ποικίλει, μεγάλη αύξηση στην μόλυνση δέχονται και οι υπολογιστές των θυμάτων, ως τελικός στόχος. Ως μέρος αυτής της τεχνικής, ένα Trojan horse εγκαθίσταται στον εκάστοτε υπολογιστή του θύματος και επιτρέπει στους phishers(μαζί με τους spammers, warez pirates, DDoS bots κτλ) να χρησιμοποιήσουν τον υπολογιστή ως διαμεσολαβητή για κάποια επίθεση. Αποτέλεσμα αυτής της ενέργειας, είναι πως ο εντοπισμός ενός εγκληματία μέσα από τα ίχνη του αποτελεί πολύ δύσκολη περίπτωση.

Είναι σημαντικό να αναφερθεί, ότι η εγκαταστάσεις των Trojan βρίσκονται πλέον σε έξαρση, παρά τις προσπάθειες των μεγάλων εταιριών Antivirus. Πολλοί κακόβουλοι χρήστες ή ομάδα εγκληματιών έχει αναπτύξει πολύ επιτυχημένες τεχνικές, με σκοπό να πείσει πιο εύκολα τον χρήστη να εγκαταστήσει το λογισμικό ενός Trojan στον υπολογιστή του σπιτιού του. Έτσι, έχουν χτίσει ένα ολόκληρο δίκτυο γεμάτο μολυσμένους υπολογιστές, οι οποίοι αποτελούν πανίσχυρο εργαλείο για να εξαπολύσουν κάποια μεγάλη επίθεση, να στείλουν εκατομμύρια e-mails ή ακόμα και να κρατάνε ψεύτικα, κατάλληλα για phishing sites.

Πληροφορίες σχετικά με μια επίθεση Trojan

Στις αρχές του 2004,ένας phisher δημιούργησε έναν απλό key-logger Trojan. Ενσωματωμένος σε ένα απλό μήνυμα HTML ο κώδικάς του προσπαθούσε να εκτελέσει ένα applet της Java με όνομα “javautil.zip”. Αν και φαινόταν να είναι ένα συμπιεσμένο αρχείο, στην πραγματικότητα ήταν ένα εκτελέσιμο αρχείο το οποίο από την στιγμή που θα εκτελούνταν έμπαινε στους browsers των θυμάτων που είχαν κενά ασφαλείας.

Το Trojan key-logger είχε σχεδιαστεί ειδικά για να κρατάει όλα τα κουμπιά που πατούσαν οι χρήστες, σε παράθυρα του browser τα οποία είχαν τίτλο commbank, Commonwealth, NetBank, Citibank, Bank of America, e-gold, e-bullion, e-Bullion, evocash, EVOCash, EVOcash, intgold, INTGold, paypal, PayPal, bankwest, Bank West, BankWest, National Internet Banking, cibc, CIBC, scotiabank and ScotiaBank.

3.4.2.5 Spear Phishing

Η πιο πρόσφατη εξέλιξη στις τεχνικές phishing είναι η τεχνική spear phishing. Όχι δεν πρόκειται για κάποιο άθλημα, πρόκειται για μία απάτη και εσείς είστε ο στόχος. Η τεχνική spear phishing αποστέλλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο μοιάζει να προέρχεται από κάποιο άτομο ή επιχείρηση που γνωρίζετε. Ωστόσο δεν είναι έτσι. Προέρχεται από τους εγκληματίες χάκερ που θέλουν τους αριθμούς της πιστωτικής σας κάρτας και του τραπεζικού σας λογαριασμού, τους κωδικούς σας και τις οικονομικές πληροφορίες που έχετε στον υπολογιστή σας. Μάθετε πώς μπορείτε να προστατεύσετε τον υπολογιστή σας.

Οι spear phisher τα καταφέρνουν χάρη στην οικειότητα. Γνωρίζει το όνομά σας, τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου και κάποια πράγματα για εσάς. Ο χαιρετισμός του μηνύματος πιθανότατα θα είναι προσωποποιημένος: "Γεια σου Γιώργο" αντί για "Αγαπητέ κύριε." Το ηλεκτρονικό μήνυμα μπορεί να αναφέρεται σε κάποιον "κοινό φίλο". Ή σε κάποια πρόσφατη online αγορά που έχετε κάνει. Επειδή το μήνυμα μοιάζει να προέρχεται από κάποιον που γνωρίζετε, μπορεί να είστε λιγότερο προσεκτικός και να τους παρέχετε τις πληροφορίες που ζητούν. Ενώ όταν πρόκειται για μια επιχείρηση που γνωρίζετε και σας ζητάει την άμεση απάντησή σας, μπορεί να κάνετε το λάθος προτού το σκεφτείτε καλά.

Ένας χρήστης μπορεί να γίνει στόχος ενός spear phisher από τις πληροφορίες που κάνει διαθέσιμες στο διαδίκτυο μέσω του υπολογιστή ή του smartphone του. Για παράδειγμα, οι εγκληματίες μπορεί να σαρώνουν διάφορες σελίδες κοινωνικής δικτύωσης και να εντοπίσουν τη σελίδα του, τη διεύθυνση του ηλεκτρονικού του ταχυδρομείου, τη λίστα των φίλων του και μία πρόσφατη δημοσίευση όπου λέει ο χρήστης στους φίλους σας για την νέα κάμερα που αγόρασε online. Χρησιμοποιώντας αυτές τις πληροφορίες, ένας spear phisher μπορεί να παρουσιαστεί ως φίλος, να του αποστείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου για να ζητήσει τον κωδικό πρόσβασης για τη σελίδα με τις φωτογραφίες του θύματος. Εάν απαντήσει δίνοντας τον κωδικό, εκείνοι θα δοκιμάσουν να χρησιμοποιήσουν αυτό τον κωδικό και διάφορες παραλλαγές του για να αποκτήσουν πρόσβαση στο λογαριασμό του στο ηλεκτρονικό κατάστημα το οποίο αναφέρατε. Εάν καταφέρουν να βρουν το σωστό κωδικό, θα τον χρησιμοποιήσουν για να χρεώσουν το θύμα πιθανόν μεγάλα ποσά. Διαφορετικά ο spear phisher μπορεί να χρησιμοποιήσει τις ίδιες πληροφορίες για να παριστάνει κάποιον εκπρόσωπο του ηλεκτρονικού καταστήματος και να ζητήσει από το θύμα να κάνει επαναφορά του κωδικού ή επαλήθευση του αριθμού της πιστωτικής του κάρτας.

3.4.3 Τύποι επιθέσεων Phishing

Για μια επίθεση phishing για να είναι επιτυχημένη, χρειάζεται να χρησιμοποιηθούν αρκετές τεχνικές για να ξεγελάσουν τον πελάτη-καταναλωτή, στο να κάνει κάτι που αποφέρει το επιθυμητό αποτέλεσμα. Υπάρχει ένας μεγάλος

αριθμός τρόπων, για να γίνει αυτό. Οι πιο κοινές μέθοδοι παραπλάνησης, αναλύονται παρακάτω :

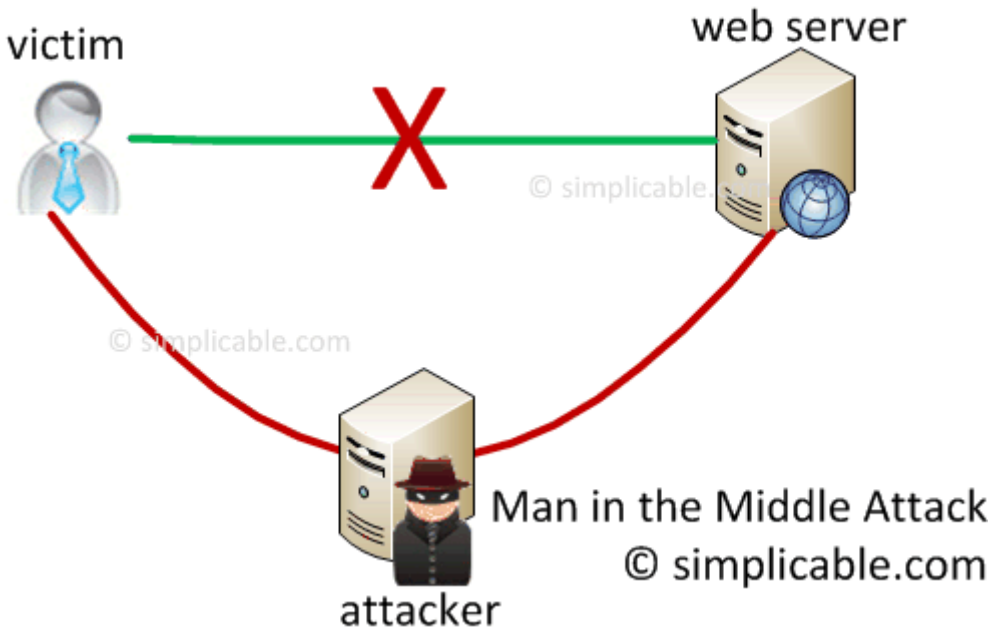
- Man-in-the-middle Attacks
- Cross-site Scripting Attacks
- Preset Session Attacks
- Observing Customer Data
- Client-side Vulnerability Exploitation

3.4.3.1 Επίθεση Man-in-the-middle

Ένας από τους πιο πετυχημένους τρόπους για να λάβει ο εγκληματίας τον έλεγχο από πληροφορίες και στοιχεία ενός θύματος, είναι μέσω της επίθεσης Man-in-the-middle. Σε αυτή την κατηγορία επιθέσεων, οι επιτιθέμενοι τοποθετούνται ανάμεσα στον πελάτη και στην πραγματική εφαρμογή και ουσιαστικά αποτελούν τον ενδιάμεσο, προωθώντας όλη την επικοινωνία ανάμεσα σε αυτούς τους δυο. Από αυτή την πλεονεκτική θέση, οι εγκληματίες μπορούν να παρακολουθούν και να καταγράφουν όλες τις συναλλαγές.

Το συγκεκριμένο είδος επίθεσης, είναι επιτυχημένο και σε HTTP αλλά και σε HTTPS περιπτώσεις. Ο πελάτης, συνδέεται με τον server του εγκληματία σαν να ήταν το πραγματικό site, ενώ ο εγκληματίας από την μεριά του πραγματοποιεί μια σύνδεση ταυτόχρονα στο πραγματικό site. Στη συνέχεια, ο server του επιτιθέμενου διαβιβάζει όλη την επικοινωνία ανάμεσα στον πελάτη και στην πραγματική εφαρμογή της ιστοσελίδας-κανονικά σε πραγματικό χρόνο.

Στην περίπτωση μιας ασφαλής HTTPS επικοινωνίας, μια σύνδεση SSL εγκαθίσταται ανάμεσα στον πελάτη και τον server του εγκληματία(έτσι ώστε να μπορεί να καταγράφει όλες τις συναλλαγές-πληροφορίες σε μη ασφαλή κατάσταση),ενώ ο server του επιτιθέμενου δημιουργεί μια δικιά του SSL σύνδεση μεταξύ του ίδιου και του πραγματικού server.



Σχήμα 22 Επίθεση Man-in-the-middle

Για να είναι επιτυχημένη μια επίθεση Man-in-the-middle,ο εγκληματίας πρέπει να μπορεί να κατευθύνει τον καταναλωτή στον δικό του Server, αντί για τον αληθινό. Μερικές μέθοδοι που του δίνουν αυτή τη δυνατότητα, είναι οι εξής :

- Transparent Proxies
- DNS Cache Poisoning
- URL Obfuscation
- Browser Proxy Configuration

Transparent Proxies

Ο όρος Transparent proxie σημαίνει ότι ο χρήστης δεν βλέπει καμμιά διαφορά είτε η αίτηση γίνεται απευθείας στο διακομιστή, είτε μέσω του εξυπηρετητή. Με αυτή την έννοια, όλοι οι εξυπηρετητές είναι διαφανείς. Με τη χρήση διαφανή εξυπηρετητή(transparent proxie),ο δρομολογητής είναι προγραμματισμένος να κατευθύνει τις αιτήσεις προς τον εξυπηρετητή. Έτσι, το λογισμικό του πελάτη αγνοεί εντελώς την ύπαρξη ενός μεσάζοντα εξυπηρετητή.

DNS Cache Poisoning

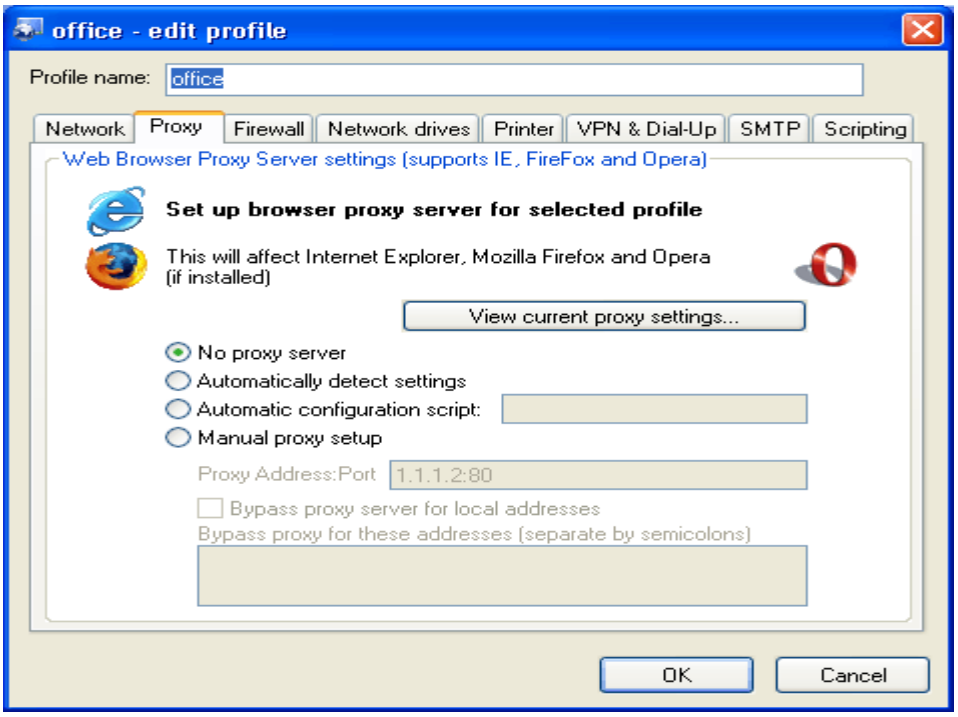
Η τεχνική του DNS Cache Poisoning, μπορεί να χρησιμοποιηθεί για να διακόψει μια κανονική δρομολόγηση, εισχωρώντας μια ψεύτικη διεύθυνση IP για τα domain names. Για παράδειγμα, ο επιτιθέμενος 'δηλητηριάζει' το DNS cache από ένα firewall δικτύου, έτσι ώστε όλη η κίνηση που προορίζεται για την IP της Τράπεζας X να περνάει από τον server του εγκληματία.

URL Obfuscation

Χρησιμοποιώντας την τεχνική URL Obfuscation,ο επιτιθέμενος μπορεί να πείσει το θύμα να ακολουθήσει ένα link το οποίο οδηγεί στο δικό του server, παρά στον κανονικό. Για παράδειγμα, ο πελάτης ίσως ακολουθήσει ένα Link το οποίο οδηγεί στο http://www.mybank.com.ch/ αντί για το http://www.mybank.com/

Browser Proxy Configuration

Παρακάμπτοντας τον browser του πελάτη και αλλάζοντας τις ρυθμίσεις του, ένας εγκληματίας μπορεί να αναγκάσει όλη την κίνηση να περνάει από τον επιλεγμένο, δικό του Server. Η μέθοδος αυτή δεν είναι κρυφή από τον χρήστη, ο οποίος μπορεί ανά πάσα στιγμή να ελέγξει τις ρυθμίσεις του και να διαπιστώσει το πρόβλημα.



Σχήμα 23 Ρύθμιση Browser Proxy Server

3.4.3.2 Cross-site Scripting Attacks

Με τον όρο Cross-site scripting ή XSS (δεν είναι CSS γιατί αλλιώς θα υπήρχε πρόβλημα ονομασίας) αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο. Κάποιος κακόβουλος χρήστης, θα μπορούσε να εισάγει κώδικα σε έναν ιστοχώρο, μέσω ενός κειμένου εισόδου για παράδειγμα, ο οποίος αφού δεν θα φιλτραριζόταν από τον ιστοχώρο σωστά, θα μπορούσε να προκαλέσει προβλήματα στον διαχειριστή ή επισκέπτη του ιστοχώρου. παράδειγμα:

http://www.example.com/index.html?name=<script>alert("xss revealed")</script>

Ο κακόβουλος χρήστης θα μπορούσε να επιτύχει:

- Κλοπή κωδικών/λογαριασμών κλπ προσωπικών δεδομένων
- Αλλαγή ρυθμίσεων του ιστοχώρου
- Κλοπή των cookies
- Ψεύτικη διαφήμιση (μέσω, π.χ., ενός συνδέσμου)

Η ευπάθεια αναφέρεται στην αδυναμία του συστήματος που υποστηρίζει ο ιστοχώρος να φιλτράρει και να απορρίψει τυχόν επιβλαβείς εισόδους.

Κατηγορίες XSS επιθέσεων

Οι περισσότεροι ειδικοί διακρίνουν τις ευπάθειες από XSS επιθέσεις σε δυο βασικές κατηγορίες: μη μόνιμες και μόνιμες. Επίσης δύο άλλες κατηγορίες που μπορούν να χωριστούν είναι σε παραδοσιακές επιθέσεις (που προκαλούνται από την πλευρά του εξηπηρετητή) και σε επιθέσεις βασισμένες σε DOM (που προκαλούνται από την πλευρά του πελάτη).

- Μη μόνιμες:
  Οι ευπάθειες σε μη μόνιμες XSS επιθέσεις είναι και οι πιο δημοφιλείς. Αυτές οι αδυναμίες προκύπτουν όταν τα δεδομένα που δίνονται από έναν web-client χρησιμοποιούνται επιτόπου από κάποιο script, το οποίο λειτουργεί από την πλευρά του εξυπηρετητή ώστε να εμφανιστεί ένα

αποτέλεσμα στον πελάτη, χωρίς όμως πρώτα να έχει προηγηθεί έλεγχος και καθαρισμός του αιτήματος που έστειλε ο πελάτης.

- Μόνιμες:
  Οι ευπάθειες σε μόνιμες XSS επιθέσεις είναι πολύ πιο καταστροφικές. Αυτές προκύπτουν όταν τα δεδομένα τα οποία στέλνονται από κάποιον κακόβουλο χρήστη αποθηκέυονται στον εξυπηρετητή, ώστε μετά να εμφανίζονται μέσα στις ιστοσελίδες του εξυπηρετητή όταν τις επισκέπτονται άλλοι χρήστες. Ένα κλασικό παράδειγμα τέτοιου τύπου επιθέσεων είναι σε online message boards που επιτρέπουν χρήστες να δημοσιεύσουν μηνύματα σε HTML για να τα δουν άλλοι χρήστες.
- Παραδοσιακές & Βασισμένες σε DOM ευπάθειες:
  Οι ευπάθιες απο XSS επιθέσεις οι οποίες είναι βασισμένες σε DOM δημιουργήθηκαν από την ανάπτυξη των web 2.0 εφαρμογών. Ενώ στις παραδοσιακές επιθέσεις είναι συνηθισμένο οι ευπάθειες να οφείλονται στον εξυπηρετητή όταν ετοιμάζει μια HTML απάντηση για κάποιον πελάτη, οι επιθέσεις βασισμένες σε DOM συμβαίνουν στα στάδια επεξεργασίας περιεχομένου που εκτελούνται στον πελάτη. Το όνομα αυτών των επιθέσεων προέρχεται από τον τρόπο που απεικονίζονται τα HTML ή XML αντικείμενα ο οποίος αποκαλείται Document Object Model (DOM).

3.4.3.3 Preset Session Attack

Στην περίπτωση των preset session επιθέσεων, οι Phishers κάνουν χρήση διαμορφωμένων Session Identifiers (SessionIDs) για ν'αποκτήσουν πρόσβαση σε ελεγχόμενο διαδικτυακό περιβάλλον και εξαπολύσουν την επίθεσή τους μέσα από αυτό. Στις περιπτώσεις συστημάτων που επιτρέπουν στις εξαρτημένες —client— συνδέσεις να προσδιορίζουν τα SessionIDs, οι preset session επιθέσεις είναι πιθανότερες και ευκολότερες. Τα SessionIDs συνήθως υλοποιούνται με cookies, hidden fields ή fields που περιέχονται σε URLs.

3.4.3.4 Hidden επιθέσεις

Στις υποκρυπτόμενες—hidden—επιθέσεις,ο Phisher χρησιμοποιεί λογισμικό κώδικα που μπορεί να εκτελεστεί από το λογισμικό πρόγραμμα φυλλομέτρησης ιστοσελίδων των καταναλωτών και να χρησιμοποιηθεί για να υπαγορεύσει τον τρόπο παρουσίασης πληροφοριακού υλικού που ο καταναλωτής αναζητά στο

Διαδίκτυο. Σε αυτό το είδος επιθέσεων ,ο Phisher μετέρχεται διάφορες τεχνικές για να πλαστογραφήσει πληροφοριακό υλικό που περιέχεται σε αξιόπιστους διαδικτυακούς τόπους .Οι πιο γνωστές από αυτές τις τεχνικές περιλαμβάνουν:

1. hidden frames
2. overriding page content
3. graphical substitution

Η τεχνική των hidden frames είναι πιθανώς η ευκολότερη στην εκτέλεσή της κυρίως λόγω της συμβατότητάς της με το σύνολο , σχεδόν , των browsers, αλλά και ης ευκολίας στη σύνταξη του λογισμικού κώδικα για τη δημιουργία των hidden frames. Τα hidden frames μπορούν να χρησιμοποιηθούν για να εξυπηρετήσουν διάφορους εγκληματικούς σκοπούς όπως η απόκρυψη της διαδικτυακής διεύθυνσης του —server—του Phisher, η παροχή ψευδών ενδείξεων ασφαλούς περιβάλλοντος διαδικτυακής επικοινωνίας τύπου HTTPS, η απόκρυψη λογισμικού κώδικα HTML από τον καταναλωτή ή αυτοματοποιημένη μεταβίβαση μολυσμένων εικόνων ή άλλου επιβλαβούς πληροφοριακού υλικού στα υπολογιστικά συστήματα των καταναλωτών και η αποθήκευση αυτού του επιβλαβούς υλικού για μεταγενέστερη χρήση από τον Phisher, η οποία μπορεί να περιλαμβάνει μία ευρεία γκάμα παρεμβατικών δραστηριοτήτων του Phisher επί των υπολογιστικών συστημάτων των καταναλωτών, ακόμη δε και την πλήρη «υποδούλωση» των συστημάτων αυτών και τη χρήση τους ως zombies.

Η τεχνική του overriding page content, συνήθως χρησιμοποιείται σε συνδυασμό με την εκτελέσιμη λειτουργία DIV της D HTML.Η εκτελέσιμη λειτουργία DIV επιτρέπει στον Phisher να τοποθετήσει ζημιογόνο περιεχόμενο σ’έναν εικονικό αποθηκευτικό χώρο που ο ίδιος δημιουργεί κατά τέτοιον τρόπο ώστε αυτός ο αποθηκευτικός χώρος να είναι συνδεόμενος με το υπολογιστικό σύστημα του καταναλωτή.

Η τεχνική του graphical substitution χρησιμοποιείται για να δημιουργήσει τις πλαστές οπτικές ενδείξεις,όπως για παράδειγμα οι ενδείξεις που ενδεικνύουν ασφαλές περιβάλλον διαδικτυακής επικοινωνίας HTTPS με χαρακτηριστικότερη το εικονίδιο της κλειδαριάς που σημαίνει την ύπαρξη μιας κρυπτογραφημένης HTTPS διαδικτυακής επικοινωνίας.Γλώσσες σύνταξης λογισμικού κώδικα που συνήθως χρησιμοποιούνται για να δημιουργηθούν αυτές τις πλαστές οπτικές ενδείξεις

ασφαλείας είναι η JavaScript, VBScript και Java. Είναι,επίσης,σύνηθες σε μια επίθεση αυτού του είδους να συνδυαστεί η πλαστογράφηση οπτικών ενδείξεων με λογισμικό κώδικα που επιτρέπει την αντικατάσταση των πραγματικών στοιχείων των πιστοποιητικών SSL με πλαστά.

3.4.3.5 Observing customer data επιθέσεις

Στις επιθέσεις αυτού του τύπου, ο Phisher παρακολουθεί και υποκλέπτει εμπιστευτικά πληροφοριακά δεδομένα κατά τη διάρκεια που αυτά εισάγονται από το θύμα σε μία διαδικτυακή εφαρμογή. Η παρακολούθηση και υποκλοπή των εμπιστευτικών πληροφοριακών δεδομένων γίνεται τοπικά και συνήθως η πρόσβαση του Phisher στα δεδομένα αυτά γίνεται με χρήση διαφόρων τεχνολογικά υποβοηθούμενων μεθόδων που εξασφαλίζουν συγχρονισμένη ροή (real time)των δεδομένων, δηλαδή τα εμπιστευτικά πληροφοριακά δεδομένα αποστέλλονται στον Phisher κατά τη διάρκεια της εισαγωγής τους σε κάποια διαδικτυακή εφαρμογή είτε από το υποκείμενο των δεδομένων είτε από τρίτον ,μέσω τοπικής σύνδεσης του Phisher στο δίκτυο κυκλοφορίας των εμπιστευτικών πληροφοριακών δεδομένων μέσα από την οποία τοπική σύνδεση τα εμπιστευτικά πληροφοριακά δεδομένα διαρρέουν στον server του Phisher με χρήση πρωτοκόλλων διαδικτυακής επικοινωνίας τύπου FTP 40 , HTTP και SMTP 41. Επίσης, ένας Phisher μπορεί να χρησιμοποιεί διάφορα τεχνολογικά εργαλεία για την παρακολούθηση και υποκλοπή πληροφοριακών δεδομένων, όπως key-loggers και screen-grabbers.

Key Logging

Ο σκοπός των key loggers,είναι να παρατηρούν και να καταγράφουν όλα τα κουμπιά που πατήθηκαν από τον πελάτη-πιο συγκεκριμένα,όταν αυτοί πρέπει να πληκτρολογήσουν πληροφορίες και στοιχεία εισόδου τους σε κάποια υπηρεσία. Με αυτά τα στοιχεία,ο phisher μπορεί να χρησιμοποιήσει τον λογαριασμό τους για δική του χρήση,σε κάποια άλλη χρονική στιγμή.

Τα key-loggers μπορεί να είναι αντικείμενα τα οποία παρατηρούν όλα τα πλήκτρα που θα πατηθούν από το θύμα,ανεξάρτητα με το περιεχόμενο ή την εφαρμογή τους(για παράδειγμα,μπορεί να καταγράφουν όσα πλήκτρα πατάει το θύμα στο Word)- ή μπορεί να έχουν προγραμματιστεί κατάλληλα στην μεριά του χρήστη,ώστε να καταγράφουν όλα τα πλήκτρα που πατιούνται μέσα σε ένα

περιεχόμενο ενός browser. Λόγο των επιτρεπτών ρυθμίσεων στην μεριά του χρήστη,για χρήστη script προγράμματα,είναι συνήθως ευκολότερο να πετύχει μια επίθεση phishing.

Screen Grabbing

Κάποιες ενδιαφέρουσες επιθέσεις Phishing,χρησιμοποιούν κώδικα ο οποίος έχει σχεδιαστεί για να παίρνει screen shots(στιγμιότυπο οθόνης,για μια συγκεκριμένη χρονική στιγμή) από δεδομένα τα οποία έχουν εισαχθεί σε μια ηλεκτρονική υπηρεσία. Αυτού του είδους οι επιθέσεις, χρησιμοποιούνται για να παρακάμψουν πιο ασφαλείς ηλεκτρονικές εφαρμογές,οι ποίες έχουν ειδικά χαρακτηριστικά που τις κάνει μη ευάλωτες σε επιθέσεις key-logging.

Σε πολλές περιπτώσεις, χρειάζεται μόνο η σχετική περιοχή προς παρακολούθηση(μόνο ένα μικρό κομμάτι,παράδειγμα αυτό του log in και όχι ολόκληρης της ιστοσελίδας) και το πρόγραμμα των εγκληματιών θα καταγράψει μόνο αυτό το κομμάτι από πληροφορίες – έτσι, κρατάει μικρό το μέγεθος της εικόνας που καταγράφεται, με αποτέλεσμα να είναι ευκολότερο και γρηγορότερο να ανέβει σε κάποιον server.

3.4.3.6 Ευπάθειες στην Πλευρά του Χρήστη

Οι browsers που χρησομοποιούν οι πελάτες για να σερφάρουν στο διαδίκτυο,όπως όλα τα άλλα λογισμικά, έχουν συχνά αρκετές ευπάθειες οι οποίες χρησιμοποιούνται για επιθέσεις.Όσο περισσότερο πολύπλοκος και με περισσότερες δυνατότητες είναι ο browser, τόσο πιο πιθανόν είναι να υπάρχουν ευπάθειες σε αυτόν που μπορούν να βρεθούν από έναν επιτιθέμενο, έτσι ώστε να πάρει πρόσβαση ή αλλίως να παρακολουθεί εμπιστευτικές πληροφορίες και στοιχεία εισόδου του πελάτη.

Αν και οι εταιρίες που δημιουργούνε τους browsers κάνουν μεγάλη προσπάθεια έτσι ώστε να βγάζουν συνεχώς updates και patches για τους browsers,οι μέσοι χρήστες δεν έχουν την γνώση να τα εγκαταστήσουν.Αυτό,σε συνδυασμό με ότι εγκαθιστούν υποπρογράμματα όπως Flash,real player και άλλα add ons,σημαίνει ότι μένουν εκτεθιμένοι σε μια πιθανή επίθεση.

Όπως και με τους ιούς και τα worms, αυτές οι ευπάθειες μπορούν να εντοπιστούν με αρκετούς τρόπους. Ωστόσο, αντίθετα με τους ιούς και τα worms,

πολλές από τις επιθέσεις δεν μπορούν να τις σταματήσουν τα λογισμικά antivirus,γιατί είναι πολύ δυσκολότερο να εντοπίσουν και να προλάβουν μια τέτοια επίθεση(συνήθως τα λογισμικά αυτά,ενεργοποιούνται αφού το σύστημα έχει μολυνθεί και ο επιτιθέμενος προσπαθήσει να εγκαταστήσει ένα πολύ γνωστό Backdoor Trojar ή ένα key-logger.

3.5 Μηχανισμοί αντιμετώπισης

3.5.1 Η αντιμετώπιση της απειλής

Όπως αναφέραμε προηγουμένως, οι phishers έχουν ένα μεγάλο αριθμό μεθόδων στη διάθεσή τους ,κατά συνέπεια δεν υπάρχει ενιαία λύση που μπορεί να καταπολεμήσει όλους αυτούς τους διαφορετικούς τρόπους επιθέσεων. Ωστόσο, είναι δυνατόν να εμποδίστουν οι τρέχουσες και μελλοντικές επιθέσεις phishing με τη χρήση ενός μίγματος των τεχνολογιών της πληροφορίας και των τεχνικών ασφάλειας. Για καλύτερη προστασία, αυτές οι τεχνολογίες και οι τεχνικές ασφάλειας πρέπει να αναπτυχθούν σε τρεις λογικές κατηγορίες:

- Η Client-side που περιλαμβάνει το PC του χρήστη.
- Η Server-side που περιλαμβάνει τα ορατά συστήματα και τις εξειδικευμένες εφαρμογές του Internet.
- Η προστασία σε επίπεδο επιχείρησης - τεχνολογίες κατανεμημένων συστημάτων και 3rd party υπηρεσίες διαχείρισης.

Αυτή η ενότητα περιγράφει λεπτομερώς τους διαφορετικούς μηχανισμούς άμυνας διαθέσιμους σε κάθε κατηγορία.

3.5.2 Client-side

Η πλευρά του χρήστη πρέπει να θεωρηθεί ότι αντιπροσωπεύει την πρώτη γραμμή του anti-phishing. Δεδομένης της διαδομένης χρήσης του υπολογιστών στο σπίτι και τα ευρέως διαφορετικά επίπεδα δεξιοτήτων και την ευαισθητοποίηση των χρηστών, η ασφάλεια σε επίπεδο client-side είναι γενικά πολύ φτωχότερη από ότι ένα διαχειριζόμενο σταθμό εργασίας για εταιρική χρήση. Ωστόσο, υπάρχουν πολλές λύσεις για πρόληψη στο προσωπικό υπολογιστή αλλά και σε εταιρικά περιβάλλοντα.

Στην πλευρά του χρήστη, την προστασία από phishing μπορεί να παρέχεται από:

- Τεχνολογίες Desktop προστασίας
- Αξιοποίηση των κατάλληλων ρυθμίσεων επικοινωνίας
- Λύσεις παρακολούθησης χρήστη σε επίπεδο εφαρμογής
- Δυνατότητες Locking-down του προγράμματος περιήγησης
- Ψηφιακή υπογραφή και την επικύρωση του e-mail
- Γενική ευαισθητοποίηση των χρηστών σε θέματα ασφάλειας

3.5.2.1 Desktop Προγράμματα Προστασίας

Οι περισσότεροι χρήστες των desktop συστημάτων είναι εξοικειωμένοι με τοπικά εγκατεστημένα προστασία λογισμικού, τυπικά υπό τη μορφή μιας ολοκληρωμένης λύσης anti-virus. Ιδανικά, τα desktop συστήματα θα πρέπει να ρυθμιστούν ώστε να χρησιμοποιεί πολλαπλά προγράμματα προστασίας (έστω και αν αυτή η λειτουργία αναπαράγει οποιαδήποτε υπηρεσία προστασίας), και να είναι σε θέση να επιτελεί τις ακόλουθες υπηρεσίες:

- Τοπική προστασία Anti-Virus
- Προσωπικό Firewall
- Προσωπικά IDS
- Προσωπικά Anti-Spam
- Ανίχνευση Spyware

Πολλοί προμηθευτές λογισμικού προστασίας επιφάνειας εργασίας (όπως η Symantec, η McAfee, η Microsoft, κλπ) παρέχουν πλέον λύσεις που είναι σε θέση να εκπληρώσουν μια ή περισσότερες από αυτές τις λειτουργίες. Ειδικά για phishing επιθέσεις, οι λύσεις (ή ο συνδυασμός αυτών) θα πρέπει να παρέχουν τις ακόλουθες λειτουργίες:

- Την ικανότητα να εντοπίζει και να μπλοκάρει προσπάθειες εγκατάστασης κακόβουλου λογισμικού (όπως δούρειους ίππους, key-logger, screengrabbers και τη δημιουργία backdoors) μέσω των συνημμένων ενός e-mail, ενός αρχείου λήψης, η μέσω ενός δυναμικού HTML και scripted περιεχομένου.
- Τη δυνατότητα να προσδιορίσει τις κοινές τεχνικές παράδοσης spam και να βάλει σε καραντίνα μηνύματα προσβολής.

- Η ικανότητα να εγκαταστήσει τις τελευταίες anti-virus και anti-spam υπογραφές και την εφαρμογή τους στο λογισμικό προστασίας. Λαμβάνοντας υπόψη την ποικιλία των τεχνικών spamming, αυτή η διαδικασία θα πρέπει να προγραμματιστεί ως μια καθημερινή δραστηριότητα.
- Η ικανότητα να ανιχνεύει και να εμποδίζει τη μη εξουσιοδοτημένες εξερχόμενες συνδέσεις από το εγκατεστημένο λογισμικό ή από ενεργές διεργασίες. Για παράδειγμα, εάν προηγουμένως έχει εντοπίσει κίνδυνο, η λύση προστασίας πρέπει να είναι σε θέση να διερευνήσει την αυθεντικότητα της σύνδεσης και να την επαληθεύσει ο χρήστης.
- Η ικανότητα να ανιχνεύει ανωμαλίες στα προφίλ κίνησης του δικτύου (εισερχόμενα και εξερχόμενα) και να λάβει τα κατάλληλα μέτρα. Για παράδειγμα, να ανιχνεύσει ότι μια εισερχόμενη HTTP σύνδεση έχει σημαντική εξερχόμενη κίνηση SSL η οποία ξεκινά από μια μη τυπική θύρα.
- Τη δυνατότητα να μπλοκάρει τις εισερχόμενες συνδέσεις σε μη συνδεδεμένες ή περιορισμένες θύρες δικτύου και των υπηρεσιών τους.
- Η ικανότητα να εντοπίζουν κοινές εγκαταστάσεις Spyware και η ικανότητα να αποτρέψει την εγκατάσταση του λογισμικού και ο αποκλεισμός εξερχόμενων επικοινωνιών με τα γνωστές Spyware ιστοσελίδες.
- Να μπλοκάρει αυτόματα εξερχόμενη παράδοση ευαίσθητων πληροφοριών σε ύποπτα σημεία. Οι ευαίσθητες πληροφορίες περιλαμβάνουν εμπιστευτικά οικονομικά στοιχεία και πληροφορίες της επαφής. Ακόμη και αν ο χρήστης δεν μπορεί να προσδιορίσει οπτικά την πραγματική ιστοσελίδα που θα λάβει τις ευαίσθητες πληροφορίες, κάποιες λύσεις λογισμικού μπορούν.

Πίνακας 3 Πλεονεκτήματα – Μειονεκτήματα Desktop προγραμμάτων προστασίας

Πλεονεκτήματα	Μειονεκτήματα
Ευαισθητοποίηση Τοπικής Άμυνας Η τοπική εγκατάσταση των μέσων προστασίας είναι ένα εύκολο έργο, και οι περισσότεροι χρήστες ήδη εκτιμούν την αξία του λογισμικού anti-virus. **Αλληλοεπικάλυψη προστασίας** Χρησιμοποιώντας μια ποικιλία προγραμμάτων προστασίας από διάφορους κατασκευαστές λογισμικού μπορεί να προκληθεί επικάλυψη στο γενικό επίπεδο προστασίας. Αυτό σημαίνει ότι μια αποτυχία ή ένα κενό ασφαλείας σε ένα προϊόν μπορεί να είναι ανιχνεύθει και να καλυφθεί από ένα άλλο. **Άμυνα σε βάθος** Η ανεξάρτητη λειτουργία των προγραμμάτων προστασίας σημαίνει ότι δεν επηρεάζουν (ή δεν επηρεάζονται) από τη λειτουργικότητα της ασφάλειας των άλλων εξωτερικών υπηρεσιών συμβάλλοντας έτσι στην συνολική άμυνα σε βάθος ενός οργανισμού.	**Τιμή Αγοράς** Η τιμή αγοράς των προγραμμάτων προστασίας δεν είναι μια άνευ σημασίας επένδυση για πολλούς χρήστες. Αν χρειάζονται πολλά προγράμματα για την πλήρη κάλυψη των επιθέσεων μπορεί να υπάρξει ένας πολλαπλασιασμός του κόστους για πολύ λίγη επιπλέον ασφάλεια. **Ανανεώσεις Συνδρομής** Πολλά από τα προγράμματα προστασίας βασίζονται σε μηνιαίες ή ετήσιες πληρωμές συνδρομής για να κρατήσει το τρέχουσα εγκατάσταση των χρηστών. Αν οι ανανεώσεις δεν πραγματοποιηθούν και τα προγράμματα προστασίας θα είναι ξεπερασμένα. **Πολυπλοκότητα & Διαχειρισιμότητα** Για εταιρικά περιβάλλοντα, τα προγράμματα προστασίας μπορεί να έχουν πολύπλοκη υποστήριξη και διαχείριση – ιδιαίτερα στο επίπεδο μιας επιχείρησης. Δεδομένου ότι αυτές οι λύσεις απαιτούν συνεχή υποστήριξη του προϊόντος (μερικές φορές σε ένα καθημερινή βάση), μπορεί να υπάρχει απαίτηση μιας επιπλέον θέσης στο ανθρώπινο δυναμικό.

3.5.2.2 Πολυπλοκότητα του E-mail

Πολλές εταιρικές e-mail εφαρμογές και άλλες απλές εφαρμογές χρησιμοποιούνται για να την πρόσβαση σε πόρους του Internet που παρέχει ένα ολοένα αυξανόμενο επίπεδο λειτουργικότητας και πολυπλοκότητας. Ενώ μερικές λειτουργίες μπορεί να απαιτούνται για εξελιγμένες εταιρικές εφαρμογές και συστήματα, η χρήση των τεχνολογιών αυτών κατά κανόνα ισχύει μόνο σε συστήματα των εταιρειών. Η περισσότερη από αυτή τη λειτουργικότητα δεν απαιτείται για την καθημερινή χρήση και ιδιαίτερα για τις υπηρεσίες επικοινωνίας μέσω Internet.

Αυτή η περιττή ενσωμάτωση λειτουργικότητας αξιοποιείται από τις επιθέσεις phishing (μαζί με την αύξηση της πιθανότητας άλλου είδους επιθέσεων). Σε γενικές γραμμές, οι περισσότερες δημοφιλείς εφαρμογές επιτρέπουν στους χρήστες να απενεργοποιούν την πιο επικίνδυνη λειτουργικότητα.

HTML-based e-mail

Πολλές από τις επιθέσεις που περιγράφονται σε προηγούμενα κεφάλαια είναι επιτυχής λόγω της HTML-based λειτουργικότητας e-mail, ιδίως, η δυνατότητα να απόκρυψης του αληθινού προορισμού των συνδέσεων, η δυνατότητα να ενσωμάτωσης στοιχείων scripting και η αυτόματη εκτέλεση των ενσωματωμένων (ή συνδεδεμένων) στοιχείων πολυμέσων. Η λειτουργικότητα της HTML πρέπει να απενεργοποιηθεί σε όλες τις εφαρμογές e-mail που είναι ικανές να αποδεχτούν ή να αποστείλουν e-mails. Αντ 'αυτού, e-mail μόνο με απλό κείμενο θα πρέπει να χρησιμοποιείται, και ιδανικά η επιλεγμένη γραμματοσειρά θα πρέπει να είναι μια από της βασικές όπως η Courier.

Τα e-mails θα πρέπει να συσταθούν σε μορφή απλού κειμένου, εμποδίζοντας την πιο κοινού τύπου επίθεση. Ωστόσο, οι χρήστες θα πρέπει να είναι έτοιμοι να λάβουν κάποια e-mail τα οποία θα είναι μπερδεμένα λόγω θεμάτων στη μορφοποίησης κειμένου ή πιθανώς γιατί περιλαμβάνουν κώδικα HTML. Μερικά δημοφιλή e-mail client θα αφαιρέσουν αυτόματα τον κώδικα HTML. Ενώ η εμφάνιση των e-mails μπορεί να αλλάξει, η ασφάλεια θα έχει βελτιωθεί σημαντικά.

Οι χρήστες δεν πρέπει να χρησιμοποιούν άλλες επιλογές σύνταξης e-mail(όπως εμπλουτισμένο κείμενο ή εργαλεία σύνταξης όπως το Microsoft Word) καθώς είναι

γνωστό ότι υπάρχουν κενά ασφαλείας με αυτές τις μορφές οι οποίες θα μπορούσαν επίσης να αξιοποιηθούν από τους phishers.

Μπλοκάρισμα συνημμένων

Οι εφαρμογές διαχείρισης e-mail που είναι ικανές να μπλοκάρουν ‘επικίνδυνα’ συνημμένα αρχεία και να εμποδίσουν τους χρήστες από τη γρήγορη εκτέλεση ή προβολή περιεχομένου που επισυνάπτεται θα πρέπει να χρησιμοποιούνται όποτε είναι δυνατό.

Μερικές δημοφιλείς εφαρμογές ηλεκτρονικού ταχυδρομείου (όπως το Microsoft Outlook) διατηρεί κατάλογο των ‘επικίνδυνων’ μορφών συνημμένων, και αποτρέπει τους χρήστες από το να τα ανοίξουν. Ενώ άλλες εφαρμογές αναγκάζουν τον χρήστη να αποθηκεύσει το αρχείο κάπου αλλού πριν να μπορέσει να έχει πρόσβαση.

Στην ιδανική περίπτωση, οι χρήστες δεν θα πρέπει να είναι σε θέση να έχουν άμεση πρόσβαση σε συνημμένα αρχεία από e-mail μέσα από την εφαρμογή. Αυτό ισχύει για όλους τους τύπους συνημμένων (συμπεριλαμβανομένων των εγγράφων του Microsoft Word, αρχεία πολυμέσων και binary αρχεία) καθώς πολλές από αυτές τις μορφές αρχείων μπορούν να περιέχουν κακόβουλο κώδικα ικανό εκμεταλλεύεται την εκτέλεση της εφαρμογής. Επιπλέον, με την αποθήκευση του αρχείου τοπικά, τα προγράμματα anti-virus που είναι εγκατεστημένα τοπικά είναι σε καλύτερη θέση για να επιθεωρήσου το αρχείο για ιούς ή άλλο κακόβουλο περιεχόμενο.

Πίνακας 4 Πλεονεκτήματα – Μειονεκτήματα πολυπλοκότητας του e-mail

Πλεονεκτήματα	Μειονεκτήματα
Προσπερνά τις τεχνικές επίθεσης μέσω της HTML Αναγκάζοντας όλα τα εισερχόμενα e-mail να είναι σε μορφή μόνο απλού κειμένου είναι αποτελεσματικό απέναντι στις τεχνικές επίθεσης μέσω της HTML . **Προσπερνά συνημμένα που περιέχουν Ιούς** Αποκλείοντας τα συνημμένα, ή αναγκάζοντας το περιεχόμενο να αποθηκευτεί αλλού, καθιστά πιο δύσκολο για τις αυτοματοποιημένες επιθέσεις που πρόκειται να διεξαχθούν και να παρέχει επιπλέον στοιχεία στα τυποποιημένα προϊόντα anti-virus για να εντοπίσουν κακόβουλο περιεχόμενο.	**Αναγνωσιμότητα** Η μετατροπή των HTML-based e-mails συχνά σημαίνει ότι αφαιρώντας τα στοιχεία κώδικα HTML το μήνυμα μπορεί να είναι δύσκολο διαβαστεί και να κατανοηθεί. **Περιορισμοί μηνύματος** Συχνά οι χρήστες δυσκολεύονται να συμπεριλάβουν συνημμένα (όπως γραφικά) σε e-mail απλού κειμένου έχοντας συνηθίσει να χρησιμοποιούν drag and drop ενσωμάτωση των εικόνων σε HTML ή σε Microsoft Word συντάκτες e-mail. **Ισχυρό μπλοκάρισμα** Η προεπιλογή μπλοκαρίσματος των "επικίνδυνων" συνημμένα συχνά έχει ως αποτέλεσμα σε τεχνητούς χρήστες που προσπαθούν να παρακάμψουν αυτούς τους περιορισμούς σε εμπορικά περιβάλλοντα που χρησιμοποιούνται για την επισύναψη ή τη λήψη εκτελέσιμου περιεχομένου.

3.5.2.3 Δυνατότητες προγράμματος περιήγησης

Τα κοινά προγράμματα περιήγησης στο Web μπορούν να χρησιμοποιηθούν ως μέσο άμυνας ενάντια στις phishing επιθέσεις ,με τη προϋπόθεση ότι έχει ρυθμιστεί σωστά. Όπως και με τα προβλήματα με τις εφαρμογές διαχείρισης e-mail, έτσι και τα προγράμματα περιήγησης προσφέρουν επίσης εκτεταμένη λειτουργικότητα που μπορεί να είναι χρησιμοποιηθεί κακόβουλα (συχνά σε μεγαλύτερο βαθμό από ότι

στις εφαρμογές διαχείρισης e-mail). Για τους περισσότερους χρήστες, οι web browser είναι ίσως το πιο τεχνολογικά εξελιγμένα εφαρμογή που χρησιμοποιούν.

Τα πιο δημοφιλή προγράμματα περιήγησης προσφέρουν μια τόσο μεγάλη σειρά από λειτουργίες, ικανοποιώντας όλους τους χρήστες σε όλα τα περιβάλλοντα, που ακούσια παρέχουν κενά ασφαλείας που εκθέτουν την ακεραιότητα του συστήματος του υπολογιστή για να δεχθεί επίθεση(Είναι σχεδόν εβδομαδιαίο περιστατικό ένα νέο κενό ασφαλείας να ανακαλύπτεται σε ένα από τα δημοφιλή προγράμματα περιήγησης).

Οι απλοί χρήστες και οι επιχειρήσεις πρέπει να επιλέξουν να χρησιμοποιήσουν ένα πρόγραμμα περιήγησης που θα είναι ο κατάλληλος για την εργασία την οποία θέλουν να πραγματοποιήσουν. Ειδικότερα, εάν ο σκοπός του προγράμματος περιήγησης είναι να περιηγηθεί μόνο στις υπηρεσίες του Διαδικτύου, ένα πολύπλοκο πρόγραμμα περιήγησης δεν είναι απαραίτητο.

Για να βοηθήσουν οι χρήστες στην πρόληψη πολλών τύπων phishing επιθέσεων, θα πρέπει να:

- απενεργοποιήσουν όλη την pop-up window λειτουργικότητα
- απενεργοποιήσουν την java runtime υποστήριξη
- απενεργοποιήσουν την ActiveX υποστήριξη
- απενεργοποιήσουν όλα τα πολυμέσα και τις επεκτάσεις που τρέχουν ή εκτελούνται αυτόματα
- αποτρέπουν την αποθήκευση των μη ασφαλών cookies
- διασφαλίζουν ότι οι λήψεις δε θα μπορούν να εκτελεστούν αυτόματα από το πρόγραμμα περιήγησης, και αντίθετα, θα πρέπει να τις κατεβάζουν σε έναν κατάλογο για antivirus επιθεώρηση

Η απομάκρυνση από τον Microsoft Internet Explorer

Το πρόγραμμα περιήγησης της Microsoft, Internet Explorer, είναι το πιο εξελιγμένο από τα διαθέσιμα. Κατά συνέπεια, έχει μια πολύ μακρά προϊστορία στην ανακάλυψη ευπαθειών και στην απομακρυσμένη εκμετάλλευση. Για το τυπικό web browsing, χρησιμοποιείται λιγότερο από το 5% της ενσωματωμένης λειτουργικότητας. Στην πραγματικότητα, πολλά από τα "χαρακτηριστικά" που είναι διαθέσιμα προστέθηκαν για την προστασία από τα προηγούμενες επιθέσεις.

Δυστυχώς, κάθε νέο χαρακτηριστικό φέρνει μαζί του μια σειρά προβλημάτων ασφάλειας και πρόσθετη πολυπλοκότητα.

Ενώ ορισμένες από τις πιο επικίνδυνες λειτουργίες μπορούν να απενεργοποιηθούν χρησιμοποιώντας διάφορες επιλογές διαμόρφωσης, οι απλοί και οι εταιρικοί χρήστες παροτρύνονται να χρησιμοποιήσουν ένα πρόγραμμα περιήγησης που είναι πιο πολύπλοκο απ' όσο θα έπρεπε για την εργασία που θέλει να εκτελέσει.

Υπάρχει ένας αριθμός από κατασκευαστές που προσφέρουν προγράμματα περιήγησης που είναι περισσότερο ασφαλή κατά ένα ευρύτερο φάσμα επιθέσεων, συμπεριλαμβανομένου και του phishing. Ένα δημοφιλές πλήρως παραμετροποιήσιμο, πρόγραμμα περιήγησης είναι το Firefox (http://www.mozilla.org). Με μια προεπιλεγμένη εγκατάσταση αυτό το πρόγραμμα περιήγησης είναι ένα από τα πιο ασφαλή , αλλά μπορεί να καταφέρει να διαχειριστεί σε ένα εταιρικό περιβάλλον και είναι επεκτάσιμο μέσω επιλεκτικών add-on modules.

Anti-Phishing Plug-ins

Υπάρχει ένας αυξανόμενος αριθμός εξειδικευμένων anti-phishing παραγωγών λογισμικού που παρέχουν browser plug-ins. Τις περισσότερες φορές, τα plug-ins προστίθενται στη γραμμή εργαλείων του προγράμματος περιήγησης και παρέχει ενεργή παρακολούθηση. Αυτές οι γραμμές εργαλείων πιστοποιούν για κάθε διεύθυνση URL ότι δεν είναι στη λίστα με τις γνωστές διευθύνσεις απάτης phishing.

Πίνακας 5 Πλεονεκτήματα – Μειονεκτήματα χρησιμοποίησης δυνατοτήτων Browser

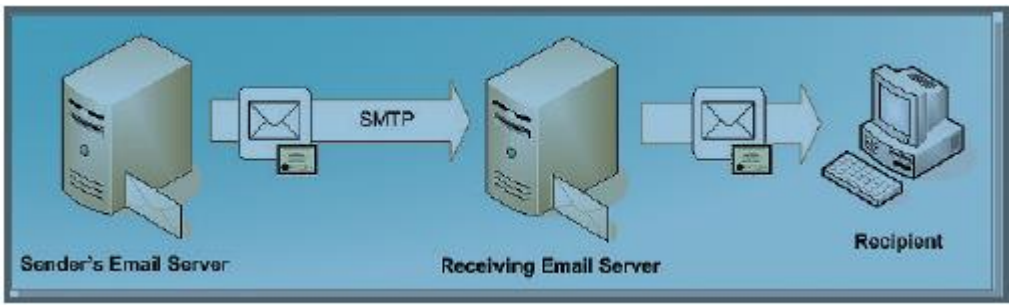
Πλεονεκτήματα	Μειονεκτήματα
Άμεσες Βελτιώσεις Ασφαλείας Η απομάκρυνση από ένα σύνθετο πρόγραμμα περιήγησης με μειωμένη λειτουργικότητα θα μετριάσει τα κενά ασφαλείας και τρωτά σημεία του Internet Explorer. **Ταχύτητα** Λιγότερο εξελιγμένα προγράμματα περιήγησης συνήθως έχει πρόσβαση και εμφανίζει το υλικό πιο γρήγορα.	**Απώλεια εκτεταμένης λειτουργικότητας** Για εταιρικά περιβάλλοντα, η απώλεια μερικής εκτεταμένης λειτουργικότητας μπορεί να απαιτεί αφιερωμένες εφαρμογές αντί για επεκτάσεις πάνω στο πρόγραμμα περιήγησης. **Απόδοση σύνθετων web εφαρμογών** Η απομάκρυνση ορισμένων πολύπλοκων λειτουργιών (ιδίως μερικών client-side scripting γλωσσών) μπορεί να προκαλέσει στις web εφαρμογές να μην αποδώσουν περιεχόμενο της σελίδας σωστά. **Ανταπόκριση των plug-ins** Τα τρέχοντα anti-phishing plug-ins είναι τόσο καλά όσο και η διατήρηση του καταλόγου των γνωστών phishing διευθύνσεων από τον πάροχο τους. Τα plug-ins είναι συνήθως καλά μόνο για ευρέως γνωστές phishing επιθέσεις.

3.5.2.4 Ψηφιακά υπογεγραμμένο E-mail

Είναι δυνατή η χρήση δημόσιου κλειδιού κρυπτογράφησης για την ψηφιακή υπογραφή ενός e-mail. Αυτή η υπογραφή μπορεί να χρησιμοποιηθεί για να επαληθεύσει την ακεραιότητα του περιεχομένου των μηνυμάτων, πιστοποιώντας έτσι αν το περιεχόμενο του μηνύματος τροποποιήθηκε κατά τη μεταφορά. Ένα υπογεγραμμένο μήνυμα μπορεί να αποδοθεί μόνο σε ένα συγκεκριμένο δημόσιο κλειδί.

Σχεδόν όλες οι γνωστές εφαρμογές διαχείρισης e-mail υποστηρίζουν την υπογραφή και την επαλήθευση των υπογεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Συνιστάται στους χρήστες:

- Να δημιουργήσουν ένα προσωπικό ζεύγος δημόσιου / ιδιωτικού κλειδιού
- Να ανεβάσουν το δημόσιο κλειδί τους σε έμπιστους διαχειριστές κλειδιών servers έτσι ώστε οι άλλοι άνθρωποι οι οποίοι θα λαμβάνουν τα e-mail να μπορούν να επαληθεύσουν την ακεραιότητα τους
- Να ενεργοποιήσουν, από προεπιλογή, την αυτόματη υπογραφή e-mail
- Να ελέγχουν όλες τις υπογραφές για τα εισερχόμενα e-mail και να είναι προσεκτικοί με τα ανυπόγραφα ή τα άκυρα υπογεγραμμένα μηνύματα



Σχήμα 24 Ψηφιακή υπογραφή email

Μια υπογραφή μηνύματος είναι ουσιαστικά μια εξελιγμένη μοναδική hash value η οποία χρησιμοποιεί πτυχές του ιδιωτικού κλειδιού του αποστολέα, του μήκος του μηνύματος, της ημερομηνία και της ώρα. Το email του παραλήπτη χρησιμοποιεί το δημόσιο κλειδί που σχετίζεται με την e-mail διεύθυνση του αποστολέα για να ελέγξει αυτή την hash value. Τα περιεχόμενα του μηνύματος δεν θα πρέπει να έχουν επηρεαστεί από τους ενδιάμεσους διακομιστές διαμεσολάβησης ταχυδρομείου.

Είναι σημαντικό να σημειωθεί ότι, σε γενικές γραμμές, δεν υπάρχουν περιορισμοί σχετικά με τη δημιουργία ενός ζεύγους ιδιωτικού / δημόσιου κλειδιού

για κάθε διεύθυνση e-mail που ένα άτομο μπορεί να επιλέξει και στην συνέχεια, να ανεβάσει το δημόσιο κλειδί σε έναν εξυπηρετητή διαχειριστή κλειδιών στο διαδίκτυο. Ως εκ τούτου, είναι ακόμα δυνατό για ένα phisher να στείλει ένα e-mail με κάποια πλαστή διεύθυνση και να το υπογράψει ψηφιακά με ένα κλειδί που κατέχει.

S / MIME και PGP

Υπάρχουν επί του παρόντος δύο δημοφιλείς μέθοδοι για την παροχή ψηφιακών υπογραφών. Αυτές είναι οι S / MIME και PGP (συμπεριλαμβανομένου του PGP / MIME και το νεότερο OpenPGP πρότυπο). Οι περισσότεροι μεγάλοι κατασκευαστές εφαρμογών ηλεκτρονικού ταχυδρομείου φτιάχνουν προϊόντα που είναι σε θέση να χρησιμοποιούν τις μεθόδους S / MIME, PGP / MIME, και OpenPGP.

Πίνακας 6 Πλεονεκτήματα – Μειονεκτήματα ψηφιακής υπογραφής email

Πλεονεκτήματα	Μειονεκτήματα
Επιχειρησιακό Πρότυπο Το S / MIME είναι ήδη ένα επιχειρησιακό πρότυπο, και είναι ήδη ενσωματωμένο στις περισσότερες εφαρμογές διαχείρισης e-mail. Ως εκ τούτου, μπορεί να λειτουργήσει χωρίς πρόσθετες απαιτήσεις λογισμικού. **Διαδρομή ελέγχου ταυτότητας** Οι phishers που υπογράφουν ψηφιακά τα e-mail τους πρέπει να καταχωρήσουν τα δημόσια κλειδιά τους σε μια κεντρική αρχή διαχείρισης κλειδιών. Αυτή η διαδικασία εγγραφής μπορεί να παράσχει μια ισχυρότερη διαδρομή ελέγχου κατά τη δίωξη του phisher.	**Web-based e-mail υποστήριξη** Δεν υποστηρίζουν όλες οι web-based εφαρμογές ηλεκτρονικού ταχυδρομείου το πρότυπο S / MIME (όπως Hotmail, AOL, Yahoo! Mail, το Outlook Web Access for Exchange 5.5). **Παραπλανητικά Domains** Οι χρήστες πρέπει να επιθεωρούν στενά την διεύθυνση παραλαβής για παραπλανητικά domains (όπως support@mybánk.com αντί για support@mybank.com). **Έλεγχος ανάκλησης** Οι δικαιούχοι δεν μπορούν να ελέγξουν την κατάσταση ανάκλησης πιστοποιητικών.

Σχέση εμπιστοσύνης Τα νόμιμα επιχειρηματικά e-mail μπορούν να προσδιοριστούν καλύτερα από τους χρήστες, ως εκ τούτου, δημιουργούν μεγαλύτερη σχέση εμπιστοσύνης με τους πελάτες τους.	

3.5.2.5 Γενική επαγρύπνηση χρηστών

Οι χρήστες μπορούν να λάβουν μια σειρά από μέτρα για να αποφύγουν να πέσουν θύματα μιας επίθεσης phishing που περιλαμβάνουν τον έλεγχο του περιεχομένου που παρουσιάζεται σ 'αυτούς και την αμφισβήτηση της αυθεντικότητας του.

Γενικά η επαγρύπνηση περιλαμβάνει:

- Εάν λάβετε ένα e-mail που σας προειδοποιεί, ότι λογαριασμός σου θα κλείσει αν δεν επιβεβαιώσετε τις πληροφορίες του τραπεζικού λογαριασμού σας μην απαντήσετε ή κάνετε κλικ στο σύνδεσμο του e-mail. Αντ 'αυτού, επικοινωνήστε με την εταιρεία που παρατίθενται στο e-mail, χρησιμοποιώντας έναν αριθμό τηλεφώνου ή μια ηλεκτρονική διεύθυνση που ξέρετε ότι είναι γνήσια.
- Ποτέ μην απαντάτε σε μηνύματα ηλεκτρονικού ταχυδρομείου HTML με ενσωματωμένα έντυπα υποβολής. Κάθε πληροφορία που υποβάλλεται μέσω του ηλεκτρονικού ταχυδρομείου (ακόμη και αν αυτό είναι θεμιτό) θα πρέπει να αποστέλλεται σε σαφές κείμενο.
- Αποφύγετε να περιλαμβάνετε σε e-mail προσωπικές και οικονομικές πληροφορίες. Πριν υποβάλετε χρηματοοικονομικές πληροφορίες μέσω ενός web site, αναζητήστε ένα εικονίδιο με μια κλειδαριά στη γραμμή κατάστασης του προγράμματος

περιήγησης. Σηματοδοτεί ότι οι πληροφορίες σας είναι ασφαλείς κατά τη διάρκεια της μετάδοσης.

- Για τις τοποθεσίες που δείχνουν ότι είναι ασφαλής, επανεξετάστε το πιστοποιητικό SSL το οποίο έχει ληφθεί και να διασφαλιστεί ότι έχει εκδοθεί από μια αξιόπιστη αρχή έκδοσης πιστοποιητικών. Οι πληροφορίες για το πιστοποιητικό SSL μπορούν να ληφθούν κάνοντας διπλό κλικ στο εικονίδιο με την κλειδαριά στο κάτω μέρος του browser, ή με δεξί κλικ σε μια σελίδα και επιλέγοντας τις ιδιότητες.
- Επιθεωρείστε τους λογαριασμούς του τραπεζικού σας λογαριασμού και της πιστωτικής κάρτας μόλις τους λάβετε για να διαπιστωθεί αν υπάρχουν μη εξουσιοδοτημένες χρεώσεις. Εάν ο λογαριασμός σας καθυστερεί πάνω από μια-δυο μέρες, καλέστε την εταιρεία της πιστωτικής κάρτας ή της τράπεζάς σας για να επιβεβαιώσετε τη διεύθυνση χρέωσης και τα υπόλοιπα των λογαριασμών.

Απάτες για ξέπλυμα βρώμικου χρήματος με προσφορά εργασίας

Λαμβάνοντας υπόψη τις επιτυχίες με τις απάτες του phishing στη λήψη προσωπικών οικονομικών πληροφορίων από τα θύματά τους, οι phishers έχουν αναπτύξει απάτες για να μεταφέρουν με ασφάλεια τα κλεμμένα χρήματα. Μια ολοένα και πιο δημοφιλής μέθοδος για να το πετύχουν αυτό είναι μέσω της προσφοράς δουλειάς που δεν υπάρχει.

Έτσι λειτουργούν αυτές οι απάτες για προσφορά εργασίας:

- Οι phishers εκμεταλλεύονται μια σειρά τραπεζικών λογαριασμών μέσω τυπικών επιθέσεων phishing.
- Στη συνέχεια, έχουν πρόβλημα στο να πάρουν τα χρήματα αυτά από τους λογαριασμούς καθώς οι περισσότερες διαδικτυακές τραπεζικές υπηρεσίες δεν επιτρέπουν άμεσες μεταβιβάσεις σε υπεράκτιους λογαριασμούς.
- Ένας συνήθης τρόπος για την αποφυγή αυτών των περιορισμών είναι μέσω απάτες προσφοράς εργασίας. Οι Phishers προσφέρουν αυτές τις «θέσεις εργασίας» μέσω spam e-mails,

ψεύτικες αγγελίες θέσεων εργασίας σε πραγματικές ιστοσελίδες προσφοράς δουλειάς ή spam μέσω άμεσης συνομιλίας.

- Από τη στιγμή που έχει προσληφθεί ένα ‘θύμα’ , του δίνουν την εντολή να δημιουργήσει ένα νέο τραπεζικό λογαριασμό στην τράπεζα στην οποία οι phishers έχουν αξιοποιήσει λογαριασμούς στο παρελθόν. Οι phishers στη συνέχεια, αφαιρούν χρήματα από τους λογαριασμούς που έχουν υποκλέψει και τα βάζουν στο λογαριασμό του θύματος.
- Στο ‘θύμα’ λένε ότι αυτή είναι μια πληρωμή που πρέπει να μεταφερθεί και του ζητούν να αποσύρει τα χρήματα κρατώντας τη αμοιβή του και τα στέλνουν μέσω υπηρεσιών, όπως η Western Union σε μια άλλη χώρα.
- Οι phishers έχουν πλέον την πλειοψηφία των χρημάτων από τους αρχικούς λογαριασμούς και όταν τα χρήματα εντοπιστούν από τις τράπεζες ή την αστυνομία, το ‘θύμα’ έχει απομείνει υπόλογο.

Πίνακας 7 Πλεονεκτήματα – Μειονεκτήματα Επαγρύπνησης χρηστών

Πλεονεκτήματα	Μειονεκτήματα
Κόστος Με το να παραμείνουν ενημερωμένοι για τις κοινές επιθέσεις phishing και να κατανοήσουν πώς πρέπει να ανταποκριθούν σε αυτές, οι χρήστες μπορούν να λάβουν οικονομικά αποδοτικές δράσεις για να προστατεύσουν τον εαυτό τους.	**Υπερφόρτωση με πληροφορίες** Με τόσους πολλούς τύπους επιθέσεων και τα αντίστοιχα βήματα που πρέπει να ληφθούν για τον εντοπισμό της απειλής, οι χρήστες είναι συχνά μπερδεμένοι με τις απαραίτητες διαδικασίες ανίχνευσης. Αυτό μπορεί να οδηγήσει τους χρήστες να μην εμπιστεύονται τη χρήση οποιασδήποτε ηλεκτρονικής μεθόδου επικοινωνίας. **Αλλαγή Πεδίου Δράσης** Οι Phishers συνεχώς αναπτύσσουν νέες παραπλανητικές τεχνικές για να μπερδεύουν τους χρήστες και να κρύψουν την αληθινή φύση του

	μηνύματος. Είναι όλο και πιο δύσκολο να εντοπιστούν οι επιθέσεις.

3.5.3 Server-side

Η υλοποίηση ευφυών anti-phishing τεχνικών στην ασφάλεια των διαδικτυακών εφαρμογών των οργανισμών, η ανάπτυξη εσωτερικών διαδικασιών για την καταπολέμηση των phishing επιθέσεων και η εκπαίδευση των χρηστών, είναι δυνατόν να παίζουν σημαντικό ρόλο στην προστασία των χρηστών από μελλοντικές επιθέσεις. Με την εκτέλεση αυτού του έργου από την server-side πλευρά, οι οργανισμοί μπορούν να κάνουν μεγάλα βήματα στην προσπάθεια να προστατευθούν από μια περίπλοκη και επίβουλη απειλή.

Στην πλευρά του server, η προστασία από το phishing μπορεί να παρέχεται από:

- Τη βελτίωση της ευαισθητοποίησης των πελατών
- Τη παροχή πληροφοριών επικύρωσης για τις επίσημες επικοινωνίες
- Τη διασφάλιση ότι η διαδικτυακή εφαρμογή είναι αναπτυγμένη με ασφάλεια και δεν περιλαμβάνει εύκολα εκμεταλλεύσιμα κενά ασφαλείας
- Τη χρησιμοποίηση ισχυρών token-based συστημάτων ελέγχου ταυτότητας
- Την τήρηση ονοματολογίας των συστημάτων ώστε να είναι απλή και κατανοητή

3.5.3.1 Ευαισθητοποίηση Χρηστών

Είναι σημαντικό οι οργανώσεις να ενημερώνουν συνεχώς τους χρήστες τους άλλα και τους χρήστες άλλων εφαρμογών για τους κίνδυνους από επιθέσεις phishing και για τα προληπτικά μέτρα τα οποία είναι διαθέσιμα. Ειδικότερα, οι πληροφορίες πρέπει να είναι ορατές για το πώς ο οργανισμός επικοινωνεί με ασφάλεια με τους χρήστες του. Για παράδειγμα, ένα απόσπασμα παρόμοιο με το ακόλουθο θα βοηθήσει τους χρήστες να αναγνωρίσουν τα phishing e-mails τα οποία αποστέλλονται με το όνομα του οργανισμού.

Πίνακας 8 Παράδειγμα email για αναγνώριση από τους χρήστες των αυθεντικών email των οργανισμών

Η MyBank δεν πρόκειται ποτέ να σας ζητήσει για ευαίσθητες πληροφορίες μέσω e-mail (δηλαδή, τον αριθμό κοινωνικής ασφάλισης, τον αριθμό προσωπικής ταυτότητας, τον κωδικό πρόσβασης, το PIN ή τον αριθμό λογαριασμού). Εάν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που ζητά αυτού του είδους τις ευαίσθητες πληροφορίες, θα πρέπει να είστε καχύποπτοι με αυτό. Εμείς προτείνουμε να μην μοιράζεστε τον αριθμό προσωπικής ταυτότητας, τον κωδικό πρόσβασης, το PIN ή τον αριθμό λογαριασμού με κανέναν, κάτω από οποιεσδήποτε συνθήκες. Αν υποψιάζεστε ότι έχετε λάβει ένα παραπλανητικό e-mail, ή αν θέλετε να επικυρώσετε επίσημα ένα e-mail από την MyBank, παρακαλώ επισκεφθείτε την antiphishing μας σελίδα http://mybank.com/antiphishing.aspx "

Βασικά βήματα στην προσπάθεια να εξασφαλιστεί η ευαισθητοποίηση των χρηστών και τη συνεχή τους επαγρύπνηση είναι:

- Οι υπενθυμίσεις στους πελάτες επανειλημμένα. Αυτό μπορεί να επιτευχθεί με μικρές ειδοποιήσεις σχετικά με τις κρίσιμες σελίδες στις οποίες οι χρήστες εισάγουν πληροφορίες, για το πώς η οργάνωση επικοινωνεί με τους χρήστες της. Στους χρήστες που μπαίνουν σε μια σελίδα θα πρέπει να ζητηθεί να σκεφτούν αν το e-mail που τους οδήγησε στην σελίδα είναι γνήσιο.
- Να δοθεί μια εύκολη μέθοδος για τους χρήστες να αναφέρουν τις απάτες phishing, ή άλλα πιθανώς πλαστά e-mail που αποστέλλονται με το όνομα του οργανισμού. Αυτή η μέθοδος μπορεί να επιτευχθεί με την παροχή σαφών links με επιβεβαίωση κλειδιού και με βοηθητικές ιστοσελίδες που θα δίνουν την δυνατότητα στους χρήστες να αναφέρουν μια πιθανή απόπειρα phishing όπως επίσης και με την παροχή συμβουλών σχετικά με την αναγνώριση μιας απάτης. Ο οργανισμός θα πρέπει να επενδύσει σε επαρκείς πόρους για να επανεξετάσει τις εισηγήσεις αυτές, θα πρέπει να είναι σε θέση να συνεργάζεται με τις

υπηρεσίες επιβολής του νόμου και τους ISPs για να σταματήσει μια επίθεση σε εξέλιξη.

- Η παροχή συμβουλών για το πώς ο χρήστης να ελέγξει την ακεραιότητα μιας ιστοσελίδας που χρησιμοποιεί. Αυτό περιλαμβάνει το πώς να:
  - Ελέγξει τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησής του
  - Βεβαιωθεί ότι η σύνδεση με την ιστοσελίδα είναι ασφαλής μέσω SSL
  - Επανεξετάσει την υπογραφή του πιστοποιητικού της σελίδας
  - Αποκρυπτογραφήσει τη γραμμή URL του προγράμματος περιήγησης
- Η καθιέρωση πολιτικών στην εταιρική επικοινωνία και η επιβολή τους. Η δημιουργία πολιτικών μέσα στην εταιρία για το περιεχόμενο των e-mail θα πρέπει να είναι τέτοια έτσι ώστε τα νόμιμα e-mail να μην συγχέονται με τις επιθέσεις phishing. Να βεβαιώνουν οι υπηρεσίες που ενδέχεται να επικοινωνούν με τους χρήστες ότι θα κατανοήσουν με σαφήνεια την πολιτική της και να λάβουν μέτρα για την εφαρμογή τους.

Για να είναι αποτελεσματικοί, οι οργανισμοί πρέπει να διασφαλίζουν ότι στέλνουν ένα σαφές, συνοπτικό και συνεκτικό μήνυμα στους χρήστες τους. Για παράδειγμα, να μην κοινοποιούν εκ των υστέρων ανακοινώσεις που ισχυρίζονται ότι ‘ποτέ δεν πρέπει οι χρήστες να συμπληρώσουν φόρμες σε ένα e-mail’ την μία ημέρα και την επόμενη μέρα να στέλνουν ένα e-mail για online πληρωμή λογαριασμών, το οποίο περιλαμβάνει μια φόρμα σύνδεσης στο e-mail του χρήση.

- Η ανταπόκριση στις απάτες phishing που έχουν εντοπιστεί θα πρέπει να είναι γρήγορη και με σαφήνεια. Είναι σημαντικό ότι οι χρήστες να κατανοούν ότι η απειλή είναι πραγματική και, το σημαντικότερο, πώς η οργάνωση εργάζεται για την προστασία τους ενάντια στην επίθεση. Ωστόσο, οι οργανισμοί πρέπει να προσέξουμε να μην ‘βομβαρδίζουν’ τους χρήστες με πληροφορίες.

Πίνακας 9 Πλεονεκτήματα – Μειονεκτήματα ευαισθητοποίησης χρηστών

Πλεονεκτήματα	Μειονεκτήματα
Χαμηλό κόστος Από όλες τις anti-phishing τεχνικές, οι οποίες εξασφαλίζουν ότι οι πελάτες έχουν επίγνωση των απειλών και μπορούν να λαμβάνουν προληπτικά μέτρα για τους εαυτούς τους, αποδεικνύεται ότι είναι αυτή που αξίζει περισσότερο την επένδυση. **Ελάχιστη Χρήση Τεχνολογίας** Παρέχοντας μια λύση χωρίς πολλές απαιτήσεις τεχνολογίας σε μια σύνθετη απειλή, οι πελάτες εμπιστεύονται περισσότερο τη σχέση τους με την οργάνωση.	**Συνέπεια** Πρέπει να ληφθεί μέριμνα για να διασφαλιστεί ότι οι επικοινωνίες διεξάγονται με συνέπεια. Μια κακή απόφαση μπορεί να υπονομεύσει μεγάλο μέρος της εργασίας. **Υπερφόρτωση με πληροφορίες** Πρέπει να ληφθεί μέριμνα για να μην επιβαρύνει τους χρήστες με πάρα πολλές πληροφορίες και να μην τους κάνει να φοβούνται να χρησιμοποιήσουν τις διαδικτυακές υπηρεσίες του οργανισμού.

3.5.3.2 Επικύρωση επίσημων επικοινωνιών

Υπάρχουν βήματα που μπορούν να ληφθούν από έναν οργανισμό για να βοηθήσουν στην επίσημη επικύρωση των επικοινωνιών με τους χρήστες και να παρέχουν ένα μέσο για τον εντοπισμό πιθανών επιθέσεων. Υπάρχουν μια σειρά από τεχνικές που ένας οργανισμός μπορεί να χρησιμοποιήσει στις επίσημες επικοινωνίες με τους χρήστες, οι οποίες είναι στενά συνδεμένα με την ευαισθητοποίησης των πελατών, ωστόσο πρέπει να ληφθεί μέριμνα ώστε να χρησιμοποιούν μόνο οι τεχνικές που είναι κατάλληλες ανάλογα με την τεχνική ικανότητα του κοινού και την αξία των συναλλαγών.

Εξατομίκευση E-mail

Τα e-mails που αποστέλλονται σε χρήστες πρέπει να είναι σε εξατομικευμένη μορφή για το συγκεκριμένο παραλήπτη. Αυτή η εξατομίκευση μπορεί να διαφέρει από τη χρήση του ονόματος του πελάτη, ή των αναφορών, ανάλογα με το κομμάτι των πληροφοριών που μοιράζονται μεταξύ του χρήστη και της οργάνωσης.

Τα παραδείγματα περιλαμβάνουν:

- ‘Αγαπητέ κύριε Παπαδόπουλε’ αντί για ‘Αγαπητέ κύριε,’
- Ο κάτοχος Λογαριασμού Πιστωτική κάρτα ‘**** **** ** 32 6722’ (διασφαλιστεί ότι μόνο τμήματα των εμπιστευτικών πληροφοριών θα χρησιμοποιηθούν)

Οι οργανισμοί πρέπει να μεριμνούν ώστε να μην διαρρεύσουν άλλες εμπιστευτικές πληροφορίες σχετικά με τον χρήστη (όπως τα πλήρη στοιχεία διεύθυνσης, κωδικοί πρόσβασης, ατομικά στοιχεία λογαριασμού, κλπ) στο πλαίσιο της επικοινωνίας τους.

Παραπομπή στο προηγούμενο μήνυμα

Είναι πιθανόν να αναφερθεί ένα e-mail το οποίο είχε σταλεί προηγουμένως στον χρήστη, για να χτιστεί η εμπιστοσύνη στις επικοινωνίες. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Οι πιο κοινές μέθοδοι είναι:

• Σαφής αναφορά του θέματος και της ημερομηνίας του προηγούμενου e-mail.

• Παροχή ενός αύξοντα αριθμού στο e-mail.

Ενώ αυτές οι μέθοδοι παραπομπής e-mail είναι πολύτιμες, είναι επίσης πολύπλοκο για τον χρήστη να τις επικυρώσει. Δεν υπάρχουν εγγυήσεις ότι ο πελάτης εξακολουθεί να διατηρεί την πρόσβαση σε ένα προηγούμενο e-mail για να εξακριβώσει την ακολουθία ιδιαίτερα όταν ο οργανισμός στέλνει στον πελάτη ένα μεγάλο όγκο από e-mails, ή συχνά διαφημιστικά μηνύματα.

Ψηφιακές Υπογραφές

Η χρήση των ψηφιακών πιστοποιητικών για την υπογραφή μηνυμάτων συνιστάται. Ωστόσο, πρέπει να ληφθεί μέριμνα ώστε να εκπαιδευτούν οι χρήστες σχετικά με τη χρήση τους και να κατανοήσουν πώς λειτουργεί η επικύρωση των υπογραφών.

Portal Επικύρωσης

Μια επιτυχημένη μέθοδος που θα παρέχει διαβεβαιώσεις προς τους χρήστες σχετικά με την αυθεντικότητα της επικοινωνίας, και επίσης θα παρέχει τη δυνατότητα να προσδιορίσει μια νέα phishing επίθεση, είναι η ύπαρξη ενός portal στην ιστοσελίδα του οργανισμού. Το διαδικτυακό portal υπάρχει ώστε ο χρήστης

να κάνει αντιγραφή / επικόλληση το περιεχόμενο του μηνύματος που έλαβε σε μια διαδραστική φόρμα, και η εφαρμογή να εμφανιστεί αν το μήνυμα είναι αυθεντικό.

Αν το μήνυμα αποτύχει στους ελέγχους γνησιότητας, το μήνυμα θα πρέπει να χειροκίνητα να επαληθευθεί από τον οργανισμό για να αξιολογηθεί κατά πόσο το μήνυμα περιέχει μια κακόβουλες επιθέσεις phishing.

Ομοίως, θα πρέπει να παρέχεται μια διεπαφή στην οποία ο χρήστης θα μπορεί να κάνει αντιγραφή / επικόλληση ύποπτες διευθύνσεις URL που έχει λάβει. Η εφαρμογή στη συνέχεια θα επικυρώνει αυτή είναι μια νόμιμη διεύθυνση URL που σχετίζεται με την οργάνωση.

Οπτική ή ακουστική εξατομίκευση των e-mail

Είναι δυνατό να ενσωματωθούν προσωπικά οπτικά ή ακουστικά στοιχεία μέσα σε ένα e-mail. Το υλικό αυτό θα έχουν παρασχεθεί από τον πελάτη στο παρελθόν. Ωστόσο, η μέθοδος αυτή δεν συνιστάται καθώς μπορεί να καταστεί αναποτελεσματική λόγω της αποφυγής εμφάνισης των μη-HTML ή των συνημμένων σε e-mail στην πλευρά του πελάτη.

Πίνακας 10 Πλεονεκτήματα – Μειονεκτήματα επικύρωσης επίσημων επικοινωνιών

Πλεονεκτήματα	Μειονεκτήματα
Αποτελεσματικότητα Η απλή διαδικασία εξατομίκευσης επικοινωνιών καθιστά πολύ πιο εύκολο για τους χρήστες να ξεχωρίσουν τις επίσημες επικοινωνίες από τα spam. Κάνοντας τη διαδικασία της επικύρωσης της πηγής του μηνύματος ταχύτερη και πιο αποτελεσματική.	**Πρόσθετοι πόροι** Οι οργανισμοί πρέπει να επεκτείνουν τις online υπηρεσίες τους επικύρωσης οι οποίες θα απαιτήσουν πρόσθετους πόρους, τόσο στην ανάπτυξη όσο και στην καθημερινή διαχείριση. **Ευαισθητοποίηση Χρηστών** Οι πελάτες μπορεί να μη χρησιμοποιήσουν ή να μην έχουν επίγνωση της σημασίας της αυτών των προσωπικών ενέργειων προστασίας.

3.5.3.3 Προσαρμογή ασφάλειας Web εφαρμογών

Οι οργανισμοί υποτιμούν συνεχώς την anti-phishing ικανότητα των προσαρμοσμένων εφαρμογών διαδικτύου τους. Με την εφαρμογή ισχυρού περιεχομένου, έλεγχο των λειτουργιών και την υλοποίηση μερικών εξατομικευμένων προσθηκών ασφαλείας, πολλοί δημοφιλές τύποι phishing επιθέσεων μπορούν να αποφευχθούν.

Η ενίσχυση της ασφάλειας των web-based εφαρμογών είναι η καλύτερη μέθοδος για την προστασία των πελατών από επιθέσεις phishing.

Μια βασική ανησυχία για την ασφάλεια περιστρέφεται γύρω από τα ολοένα και πιο μεγάλα κενά από cross-site scripting . Αυτές οι ευπάθειες cross-site scripting συχνά ξεφύγουν από άλλες στρατηγικές για την προστασία του υπολογιστή του χρήστη λόγω της εμπιστοσύνης που υπάρχει στις σχέσεις μεταξύ του χρήστη και του ιδιοκτήτη της ιστοσελίδας, με αποτέλεσμα να γίνονται άκρως επιτυχημένες (και μη ανιχνεύσιμες) επιθέσεις.

Επικύρωση Περιεχομένου

Ένα από τα πιο κοινά κενά ασφαλείας σε προσαρμοσμένες web-based εφαρμογές σχετίζεται με κακή λειτουργία επικύρωσης των διαδικασιών εισόδου.

Οι βασικές αρχές για την επιτυχή εφαρμογή των διαδικασιών επικύρωσης του περιεχόμενου περιλαμβάνει:

- Ποτέ να μην είναι έμπιστα τα δεδομένα που υποβάλλονται από ένα χρήστη ή μια άλλη εφαρμογή.
- Ποτέ να μην παρουσιάζονται δεδομένα απευθείας σε ένα χρήστη της εφαρμογής χωρίς να ελεγχθούν πρώτα.
- Πάντα να ελέγχονται τα δεδομένα πριν την επεξεργασία ή την αποθήκευσή τους.
- Επιβεβαίωση ότι όλοι οι επικίνδυνοι χαρακτήρες (δηλ χαρακτήρες που μπορεί να διερμηνεύονται από το πρόγραμμα περιήγησης ή από διαδικασίες που εκτελούνται στο παρασκήνιο) οι οποίοι αποτελούν στοιχεία μιας εκτελέσιμης γλώσσας να αντικαθίστανται με τις κατάλληλο HTML ασφαλείς αντιστοιχίσεις τους.

- Βεβαίωση ότι όλα τα δεδομένα εξετάζονται με τα κοινά συστήματα κωδικοποίησης (όπως% 2E,% C0% AE, u002E%, %% 35% 63) σύμφωνα με τους βασικούς χαρακτήρες. Και πάλι, αν ο χαρακτήρας δεν είναι ασφαλής, θα πρέπει να μετατρέπεται στην αντίστοιχη μορφή HTML. Πρέπει να τονιστεί ότι η διαδικασία της αποκωδικοποίησης μπορεί να πρέπει να διεξαχθεί πολλές φορές, μέχρι όλες οι κωδικοποιημένες αλληλουχίες να αφαιρεθούν.

Χειρισμός Session

Η φύση της επικοινωνίας μέσω HTTP και HTTPS απαιτεί την ορθή εφαρμογή των διαδικασιών χειρισμού session. Πολλές προσαρμοσμένες εφαρμογές εφαρμόσουν ρουτίνες χειρισμού session για τα προκαθορισμένα session που είναι δυνητικά ευάλωτα σε επιθέσεις.

Για να ξεπεραστεί μια προκαθορισμένη επίθεση σε session, οι προγραμματιστές θα πρέπει να εξασφαλίσουν τις ακόλουθες λειτουργίες της εφαρμογής:

- Ποτέ να μην αποδέχονται τις πληροφορίες του session μέσα σε μια διεύθυνση URL.
- Να βεβαιώνουν ότι τα sessionId έχουν προθεσμία λήξης και ότι ελέγχονται πριν από τη χρήση για κάθε αίτημα του χρήστη.
- Η εφαρμογή θα πρέπει να είναι σε θέση να ανακαλέσει ένα ενεργό sessionId και να μην ανακυκλώνει το ίδιο sessionid για παρατεταμένο χρονικό διάστημα.
- Οποιεσδήποτε προσπάθειες να υποβληθεί ένα μη έγκυρο sessionId (δηλαδή αυτό που έχει λήξει, που έχει ανακληθεί, που έχει ξεπεράσει το χρόνο ζωής του, ή που δεν εκδόθηκε ποτέ), θα πρέπει να οδηγήσει σε ένα μια ανακατεύθυνση στη σελίδα σύνδεσης και να εκδοθεί ένα νέο sessionId.
- Ποτέ να μην διατηρείτε ένα sessionId που αρχικά παρέχεται μέσω HTTP μετά την ασφαλή σύνδεση του χρήστη(δηλαδή με HTTPS). Μετά τον έλεγχο ταυτότητας, ο χρήστης θα πρέπει πάντα να παίρνει ένα νέο sessionId.

Αξιολόγηση URL

Για web-based εφαρμογές που θεωρούν ότι είναι απαραίτητο να χρησιμοποιείται ανακατεύθυνση σε άλλες θέσεις της σελίδας, πρέπει να δοθεί ιδιαίτερη προσοχή στην αξιολόγηση του υπερσυνδέσμου. Οι προγραμματιστές εφαρμογών θα πρέπει να γνωρίζουν τις τεχνικές που αναλύθηκαν στο προηγούμενο κεφάλαιο.

Βέλτιστες πρακτικές για την αξιολόγηση ενός URL είναι:

- Η μη αναφορά διευθύνσεων URL ανακατεύθυνσης ή εναλλακτικών διαδρομών των αρχείων απευθείας στο πρόγραμμα περιήγησης (όπως http://mybank.com/redirect.aspx?URL=secure.mybank.com).
- Πάντα να διατηρείτε μια έγκυρη λίστα των διευθύνσεων URL ανακατεύθυνσης. Για παράδειγμα, η διαχείριση μιας server-side λίστας των διευθύνσεων URL που συνδέεται με ένα δείκτη παραμέτρου. Όταν ένας χρήστης ακολουθεί έναν υπερσύνδεσμο, η υποβολή του θα αναφέρεται σε αυτόν τον δείκτη, και η σελίδα ανακατεύθυνσης που θα του επιστραφεί θα περιλαμβάνει το πλήρες URL.
- Ποτέ να μην επιτρέπεται στους χρήστες να παρέχουν τις δικές τους διευθύνσεις.
- Ποτέ να μην επιτρέπεται οι διευθύνσεις IP να χρησιμοποιούνται στις πληροφορίες του URL. Πάντα να χρησιμοποιείτε το πλήρως αναγνωρισμένο domain όνομα, ή στην έσχατη περίπτωση να διεξάγεται μια αντίστροφη αναζήτηση του ονόματος στη διεύθυνση IP και να βεβαιώνεται ότι βρίσκεται σε ένα domain το είναι αξιόπιστο από την εφαρμογή.

Διαδικασίες αυθεντικοποίησης

Για πολλές απάτες phishing, ένας βασικός στόχος της επίθεσης είναι να υποκλέψει από τον χρήστη τα διαπιστευτήρια ελέγχου ταυτότητας. Για να γίνει αυτό, ο εισβολέας θα πρέπει να είναι σε θέση να παρακολουθεί όλες τις πληροφορίες που υποβάλλονται κατά τη φάση σύνδεσης στην εφαρμογή. Οι

οργανισμοί μπορούν να χρησιμοποιήσουν πολλές μεθόδους για να κάνουν αυτή τη διαδικασία πιο δύσκολη για τον phisher.

Οι προγραμματιστές εφαρμογών θα πρέπει να επανεξετάσουν τον ολοκληρωμένο κώδικα HTML της εφαρμογής κυρίως στα σημεία που γίνεται αυθεντικοποίηση για να αποτρέψουν τις περισσότερες μορφές των πιθανών επιθέσεων. Ωστόσο, ειδικά για τις phishing επιθέσεις οι προγραμματιστές θα πρέπει:

- Να βεβαιωθούν ότι χρησιμοποιείται το ελάχιστο μια διαδικασία σύνδεσης δύο φάσεων. Στο χρήστη αρχικά θα πρέπει να παρουσιάζεται με μια σελίδα σύνδεσης στην οποία θα πρέπει να εισάγει τα στοιχεία του λογαριασμού που είναι τυπικά λιγότερο ασφαλείς (δηλαδή υπάρχει μια μεγάλη πιθανότητα ότι ο πελάτης να χρησιμοποιεί τα στοιχεία αυτά και σε άλλες ιστοσελίδες ,όπως το όνομα χρήστη και τον αριθμό πιστωτικής κάρτας). Μετά την επιτυχή εισαγωγή των στοιχείων σε αυτήν τη σελίδα, να πρέπει να παρουσιάζεται μια δεύτερη σελίδα που θα απαιτεί δύο ή περισσότερα μοναδικά κομμάτια πληροφοριών ταυτότητας για να μπορέσει να προχωρήσουν στην εφαρμογή.
- Η χρήση των διαδικασιών anti key-logging, όπως η επιλογή συγκεκριμένων τμημάτων ενός κωδικού πρόσβασης ή ενός συνθηματικού από μια drop-down λίστα συνιστάται ιδιαίτερα.
- Πρέπει να προσπαθήσουν να χρησιμοποιήσουν εξατομικευμένο περιεχόμενο (σε συνδυασμό με την ευαισθητοποίηση των πελατών) για τον εντοπισμό πλαστών ιστοσελίδων. Για παράδειγμα, όταν ένας χρήστης δημιουργεί τον online λογαριασμό του θα πρέπει να είναι σε θέση να επιλέξει ή να ανεβάσει μια προσωπική εικόνα. Αυτή η εικόνα θα είναι πάντα να παρουσιάζεται κατά το δεύτερο στάδιο ελέγχου ταυτότητας και σε κάθε έλεγχο ταυτότητας στη σελίδα. Αυτή η εικόνα μπορεί να χρησιμοποιηθεί ως υδατογράφημα γνησιότητας για την καταπολέμηση του ψευδούς περιεχομένου.

- Να μην καταστεί η διαδικασία πιστοποίησης πολύ πολύπλοκη. Θα πρέπει να γνωρίζουν ότι χρήστες με ειδικές ανάγκες μπορεί να έχουν δυσκολία με κάποια λειτουργία, όπως τα drop-down κουτιά.

Καθορισμός εικόνας

Επειδή πολλές phishing επιθέσεις βασίζονται σε ένα αντίγραφο της ιστοσελίδας που είναι στόχος το οποίο είναι σε ένα σύστημα υπό τον έλεγχο του phisher, υπάρχουν πιθανές κατευθύνσεις για τους οργανισμούς ώστε να εντοπίσει αυτόματα μια ψεύτικη ιστοσελίδα.

Ανάλογα με το αν η phisher έχει αντιγράψει το σύνολο της ιστοσελίδας (συμπεριλαμβανομένων των σελίδων και των γραφικών τους) ή απλά φιλοξενεί μια τροποποιημένη HTML σελίδα (η οποία έχει αναφορές για τα γραφικά που βρίσκονται στους πραγματικούς διακομιστές των οργανώσεων), είναι δυνατόν να διακοπεί ή να προσδιοριστεί με μοναδικό τρόπο η πηγή της επίθεσης.

Δύο μέθοδοι είναι διαθέσιμες για τους προγραμματιστές εφαρμογών:

- Ανακύκλωση Εικόνων
  Κάθε νόμιμη σελίδα μιας εφαρμογής αναφορές για τις εικόνες που περιλαμβάνει με ένα μοναδικό όνομα. Κάθε ώρα, τα ονόματα των εικόνων πρέπει να αλλάζουν και οποιαδήποτε σελίδα που έχει αναφορές σε αυτά θα πρέπει να τις αλλάζει. Ως εκ τούτου, οποιοδήποτε αντίγραφο της σελίδας θα πρέπει να αλλάζει γρήγορα της αναφορές στις εικόνες για να είναι ενημερωμένη. Έτσι εάν ζητηθεί μια εικόνα της οποία η αναφορά έχει λήξει δεν θα εμφανίζεται. Γι αυτό συνίσταται να ενημερώνεται ο χρήστης ότι ο χρόνος της εικόνας έληξε και να προσπαθήσει να μπει ξανά στην ιστοσελίδα.

  • Session-bound Εικόνες
  Η επέκταση περαιτέρω της αρχής της ανακύκλωσης των εικόνα, είναι στις αναφορές των εικόνων να περιλαμβάνεται και το τρέχων sessionId του χρήστη. Ως εκ τούτου, αν ανακαλυφθεί μία φορά μια

πλαστή ιστοσελίδα, ο οργανισμός μπορεί να ελέγξει τα στοιχεία που έχει διαθέσιμα ώστε να προσπαθήσει να ανακαλύψει την πηγή της πλαστής ιστοσελίδας. Αυτό είναι ιδιαίτερα χρήσιμο για πλαστές ιστοσελίδες που χρησιμοποιούν επίσης περιεχόμενο που απαιτεί έλεγχο ταυτότητας και η πρόσβαση μπορεί να αποκτηθεί μόνο από ένα phisher που χρησιμοποιεί έναν πραγματικό λογαριασμό. Επιπλέον, ο οργανισμός μπορεί να χρησιμοποιήσει τεχνολογίες υδατογράφησης και να ενσωματώσει πληροφορίες του session στην ίδια την εικόνα. Ωστόσο, η διαδικασία αυτή θα επέφερε υψηλά έξοδα στη server-side πλευρά.

Πίνακας 11 Πλεονεκτήματα – Μειονεκτήματα προσαρμογής ασφάλειας στις Web εφαρμογές

Πλεονεκτήματα	Μειονεκτήματα
Ευρωστία Με την προσθήκη κατάλληλης ασφάλειας για αναπτυγμένες εφαρμογές web, οι οργανώσεις διαπιστώνουν ότι οι εφαρμογές τους δεν είναι μόνο σε καλύτερη θέση να αντιστέκονται σε επιθέσεις phishing, αλλά ότι οι συνολική ανθεκτικότητα έναντι άλλων πιο προηγμένων επιθέσεων έχει αυξηθεί. **Σχέση κόστους - αποτελεσματικότητας** Με την αντιμετώπιση θεμάτων ασφάλειας μέσα στην εφαρμογή, ο αριθμός των τύπων επιθέσεων που είναι διαθέσιμος σε ένα phisher μειώνεται σημαντικά. Η εξασφάλιση της ασφάλειας της βασικής εφαρμογής αποδεικνύεται ότι είναι οικονομικά	**Απαιτεί ικανούς προγραμματιστές** Η εφαρμογή αυτών των προσθηκών ασφάλειας απαιτεί εξειδικευμένους προγραμματιστές με κάποια εμπειρία στην εφαρμογή της ασφάλειας. Οι πόροι αυτοί είναι συνήθως δύσκολο να βρεθούν. **Πρέπει να δοκιμαστεί** Οι οργανισμοί πρέπει να εξασφαλίζουν ότι όλα τα νέα χαρακτηριστικά ασφαλείας (μαζί με τυχόν τροποποιήσεις) πρέπει να δοκιμαστούν διεξοδικά από πλευράς ασφάλειας πριν χρησιμοποιηθούν. **Περισσότεροι πόροι συστήματος** Επιπλέον πόροι επεξεργασίας απαιτούνται για να εφαρμοστούν αυτοί οι μηχανισμοί ασφαλείας. Επομένως η απόδοση των εφαρμογών μπορεί να επηρεαστεί αρνητικά.

αποδοτική έναντι των τρεχουσών και μελλοντικών απειλών. **Ανεξαρτησία Χρηστών** Οι βελτιώσεις στην ασφάλεια από την πλευρά του διακομιστή γενικά δεν περιλαμβάνουν αλλαγές στην εμπειρία του χρήστη. Ως εκ τούτου, οι αλλαγές μπορεί να γίνονται ανεξάρτητα από την πλευρά του χρήστη.	

3.5.3.4 Ισχυρή Token-based Αυθεντικοποίηση

Υπάρχει ένας αριθμός από μεθόδους ελέγχου ταυτότητας που κάνουν χρήση εξωτερικών συστημάτων για την παραγωγή μιας χρήσης κωδικούς πρόσβασης ή κωδικούς πρόσβασης με χρονικό όριο. Τα συστήματα αυτά, συχνά αναφέρονται ως token-based συστήματα αυθεντικοποίησης, μπορεί να βασίζονται σε φυσικές συσκευές ή λογισμικό. Ο σκοπός τους είναι η δημιουργία ισχυρών (μιάς χρήσης) κωδικών πρόσβασης που δεν θα μπορούν να χρησιμοποιηθούν επανειλημμένα για την είσοδο σε μια εφαρμογή. Οι χρήστες μιας web-based εφαρμογής θα χρησιμοποιήσει μια φυσική συσκευή όπως μια έξυπνη κάρτα για να παράσχει έναν κωδικό πρόσβασης μιας χρήσης ή με χρονικό όριο λήξης.

Λόγω του υψηλού κόστους εγκατάστασης και συντήρησης, αυτή η λύση είναι η καταλληλότερη για web εφαρμογές συναλλαγών με πολύ υψηλή αξία που είναι απίθανο να απαιτήσει ένα μεγάλο αριθμό χρηστών.

Όπως και με κάθε διαδικασία ελέγχου ταυτότητας, οι οργανώσεις πρέπει να επιτύχουν μια ισορροπία μεταξύ του να είναι τα προσωπικά ή εμπιστευτικά στοιχεία τα ελάχιστα απαιτούμενα για τη μοναδική ταυτοποίηση ενός χρήστη, και ποιες από αυτές τις πληροφορίες μπορούν να γίνουν γνωστές δημόσια και ποιες ενδέχεται να χρησιμοποιηθούν από τον χρήστη για να αποκτήσει πρόσβαση σε μια web-based εφαρμογή ενός άλλου οργανισμού. Με τη μείωση της πιθανότητας τα στοιχεία ταυτότητας να είναι ίδια μεταξύ πολλών οργανώσεων, υπάρχουν λιγότερες ευκαιρίες για έναν εισβολέα να επιτύχει την κλοπή τους.

Πίνακας 12 Πλεονεκτήματα – Μειονεκτήματα ισχυρής token-based αυθεντικοποίησης

Πλεονεκτήματα	Μειονεκτήματα
Εξάρτηση από τον χρόνο Ο κωδικός πρόσβασης εξαρτάται από το χρόνο. Επομένως, ο phisher για να ανακτήσει και να χρησιμοποιήσει αυτές τις πληροφορίες έχει προκαθορισμένα χρονικά όρια, γιατί ο κωδικός θα έχει λήξει και θα είναι άχρηστος με τον πάροδο του χρόνου. **Φυσική συσκευή πρόσβασης** Ο phisher πρέπει να αποκτήσει φυσική πρόσβαση στη συσκευή για να μιμηθεί το χρήστη και να πραγματοποιήσει την κλοπή. **Αίσθηση εμπιστοσύνης** Οι χρήστες είναι περισσότερο διατεθειμένοι να εμπιστεύονται token-based συστήματα ελέγχου ταυτότητας για τις χρηματικές τους συναλλαγές. **Καταπολέμησης της Απάτης** Η αντιγραφή της φυσικής συσκευής απαιτεί πολύ περισσότερη δεξιότητα, ακόμα και αν το θύμα τους παρέχει τον προσωπικό αριθμό PIN που σχετίζεται με τη συσκευή.	**Εκπαίδευση Χρηστών** Στους χρήστες θα πρέπει να παρέχονται οδηγίες για το πώς να χρησιμοποιήσει τη συσκευή μέσα σε ένα πλαίσιο συγκεκριμένο χρονικό πλαίσιο. **Οι συσκευές κοστίζουν** Οι φυσικές συσκευές είναι συνήθως δαπανηρές για να κατασκευαστούν και να διανεμηθούν στους χρήστες. **Η ρύθμιση χρειάζεται χρόνο** Η δημιουργία λογαριασμού και η διανομή απαιτεί μερικές ημέρες μέχρι να μπορέσει ο χρήστης να έχει πρόσβαση στην εφαρμογή web. **Υψηλό κόστος διαχείρισης** Η διαχείριση ενός συστήματος που βασίζεται σε αυτή τη λογική απαιτεί περισσότερη προσπάθεια και μεγαλύτερη πρόσβαση σε εσωτερικούς πόρους. **Υπερφόρτωση του χρήστη** Ένας πελάτης μπορεί να χρειάζεται να μεταφέρει πολλές συσκευές, μια για κάθε υπηρεσία στην οποία έχουν εγγραφεί.

3.5.4 Προστασία σε επίπεδο επιχειρήσεων

Οι επιχειρήσεις και οι ISP μπορούν να λάβουν μέτρα σε επίπεδο επιχειρήσεων για να προστατευτούν από το phishing, προστατεύοντας έτσι τόσο τους χρήστες των εφαρμογών τους όσο και τους υπαλλήλους τους. Αυτές οι επιχειρηματικές

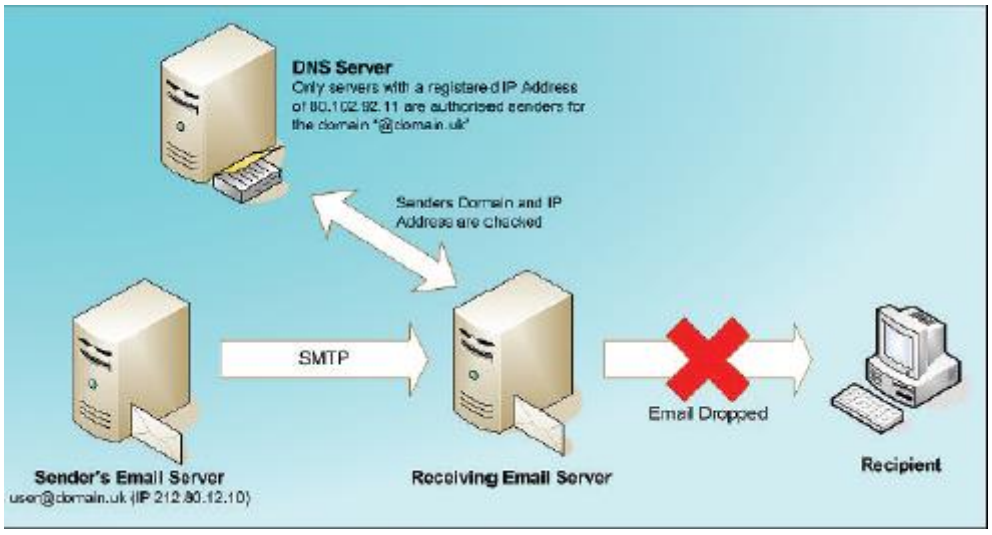
λύσεις ασφάλειας που λειτουργούν σε συνδυασμό με τους client-side και τους server-side μηχανισμούς ασφάλειας, προσφέρουν σημαντική προστασία σε βάθος κατά του phishing και ένα πλήθος άλλων σύγχρονων απειλών.

Βασικά βήματα για την ασφάλεια ενάντια στο phishing σε επίπεδο επιχείρησης είναι:

- Η αυτόματη επικύρωση αποστολής των e-mail διευθύνσεων διακομιστή
- Η Ψηφιακή υπογραφή των e-mail υπηρεσιών
- Η παρακολούθηση των εταιρικών domain και την κοινοποίηση των "παρόμοιων" εγγραφών
- Προγράμματα προστασίας gateway

3.5.4.1 Αυθεντικοποίηση Mail server

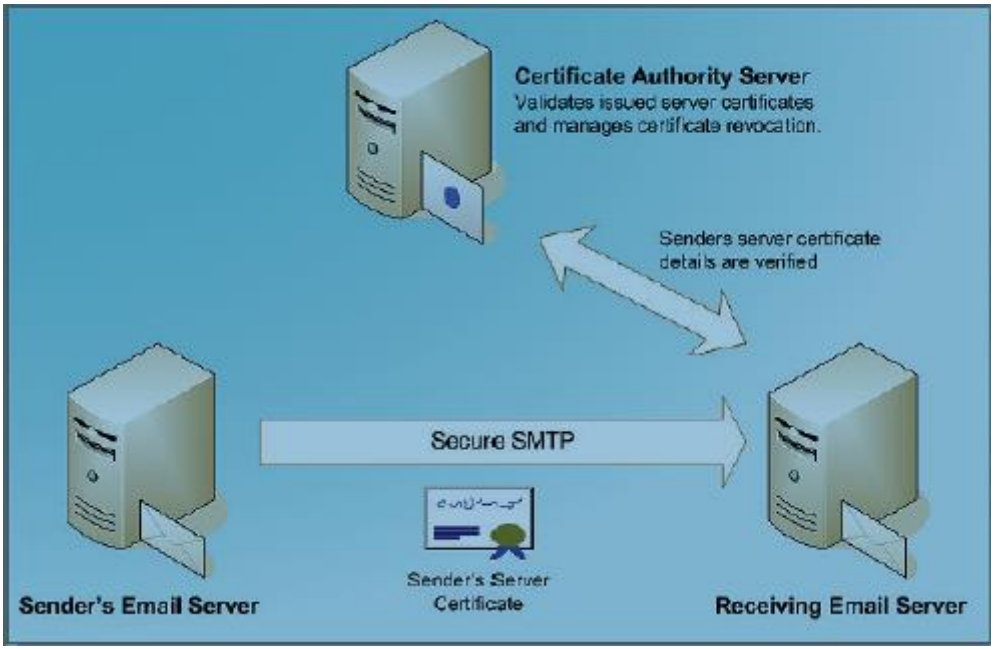
Πολλαπλές μέθοδοι έχουν προταθεί για τον έλεγχο ταυτότητας εισερχόμενων των Mail server. Στην ουσία, ο mail server του αποστολέα έχει επικυρωθεί (όπως η αντίστροφη ανάλυση των πληροφοριών domain σε μια συγκεκριμένη διεύθυνση IP ή σε ένα εύρος διευθύνσεων) από τον e-mail server από τον οποίο λαμβάνει. Εάν η διεύθυνση IP του αποστολέα δεν είναι εξουσιοδοτημένη για το domain του e-mail, το e-mail απορρίπτεται από τον mail server ο οποίος το λαμβάνει.



Σχήμα 25 Αυθεντικοποίηση mail server

Εναλλακτικά, μέσω της χρήσης του Secure SMTP, η μεταφορά των e-mail θα μπορούσε να διεξαχθεί μέσω μιας κρυπτογραφημένης SSL/TLS σύνδεσης. Όταν

ο διακομιστής αλληλογραφίας του αποστολέα συνδέεται με τον διακομιστή αλληλογραφίας του παραλήπτη, τα πιστοποιητικά ανταλλάσσονται πριν από η κρυπτογραφημένη σύνδεση εγκατασταθεί. Η επικύρωση του πιστοποιητικού μπορεί να χρησιμοποιηθεί για να προσδιοριστεί επακριβώς ένας έμπιστος αποστολέας. Αν τα πιστοποιητικά δεν υπάρχουν, είναι άκυρα ή έχουν ανακληθεί δεν θα εγκατασταθεί μια ασφαλής σύνδεση και δεν θα επιτρέπεται η παράδοση των e-mails.



Σχήμα 26 Αυθεντικοποίηση mail server με Secure SMTP

Εάν είναι επιθυμητό, ένας πρόσθετος έλεγχος με το διακομιστή DNS μπορεί να χρησιμοποιηθεί για να εξασφαλιστεί ότι μόνο εξουσιοδοτημένοι διακομιστές ηλεκτρονικού ταχυδρομείου μπορούν να στείλουν e-mail μέσω της ασφαλούς SMTP σύνδεσης.

Ο σκοπός της επικύρωσης της διεύθυνσης του διακομιστή αποστολής είναι να βοηθήσει να περικοπεί ο όγκος των μηνυμάτων spam, και να επιταχυνθεί η λήψη των e-mails που είναι γνωστό ότι προέρχονται από μια ‘καλή’ πηγή. Ωστόσο, και τα δύο συστήματα μπορούν να ξεπεραστούν αν γίνει κακή διαμόρφωση του διακομιστή - ιδιαίτερα αν ο server αποστολέας μπορεί να λειτουργήσει ως ένας agent ανοικτής αναμετάδοσης. Είναι σημαντικό να σημειωθεί ότι Secure SMTP δεν χρησιμοποιείται συνήθως. Ωστόσο, η επικύρωση του διακομιστή e-mail είναι χρήσιμη σε ενδο-εταιρικές επικοινωνίες όταν συνδυάζεται με τους κανόνες του

διακομιστή αλληλογραφίας που μπλοκάρει ή απαγορεύει τα εισερχόμενα e-mail τα οποία χρησιμοποιούν ‘Από:’ διευθύνσεις που θα μπορούσαν να προέλθουν μόνο από εσωτερικούς χρήστες.

Πίνακας 13 Πλεονεκτήματα – Μειονεκτήματα αυθεντικοποίησης mail server

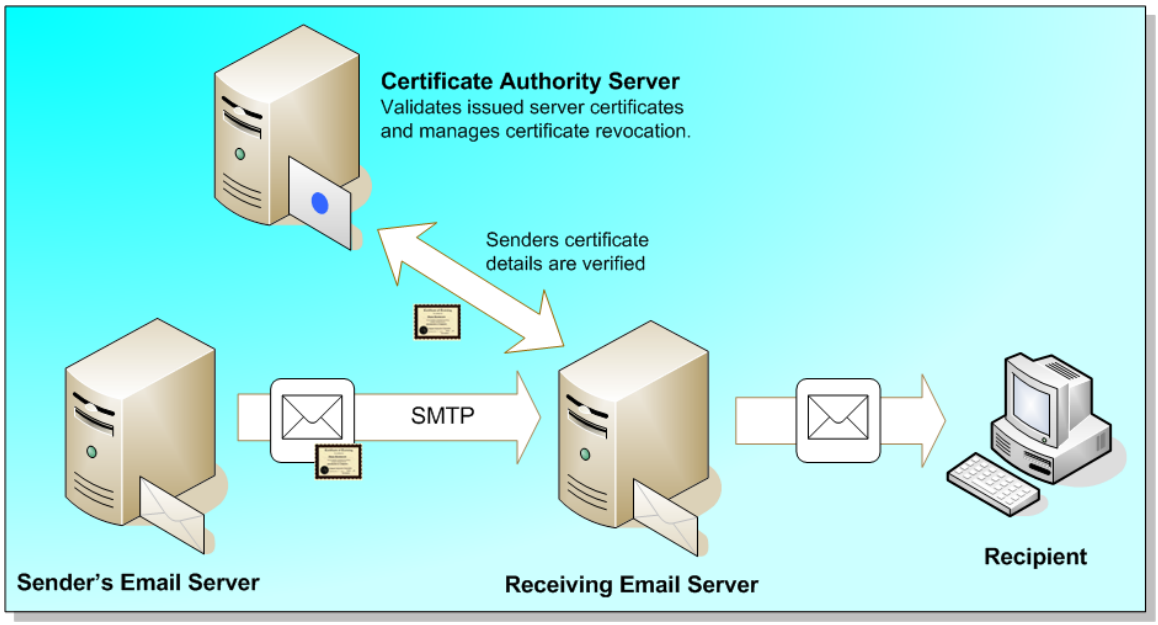
Πλεονεκτήματα	Μειονεκτήματα
Εύκολη ρύθμιση Η ενημέρωση του διακομιστή DNS με τις σχετικές MX εγγραφές για κάθε διακομιστή αλληλογραφίας είναι απαραίτητη για την αντίστροφη ανάλυση των έγκυρων εξυπηρετητών ταχυδρομείου μέσα σε ένα domain. **Πρόληψη ανωνυμίας** Οι διακομιστές αποστολής επικυρώνονται πριν τα e-mail γίνουν αποδεκτά από το διακομιστή παραλαβής. Συνεπώς, ο διακομιστής αποστολής των phishers δεν μπορεί να είναι ανώνυμος. **Αναγνώριση Business E-mail** Η επικύρωση του διακομιστή αποστολής μπορεί να χρησιμοποιηθεί για να εντοπιστούν τα νόμιμα επιχειρηματικά e-mail, έτσι ώστε να μειωθούν τα spam e-mail.	**Spoofing διεύθυνσης ‘Από:’** Δεδομένου ότι η διεύθυνση του αποστολέα SMTP συνήθως δεν είναι εμφανής στους παραλήπτες e-mail, είναι ακόμα δυνατό γίνει spoof η ‘Από:’ διεύθυνση. **Προώθηση E-mail** Καμία μέθοδος δεν επιτρέπει τις e-mail διαδικασίες προώθησης. Η επικύρωση του διακομιστή αποστολής εξαρτάται από την άμεση σύνδεση αποστολέα και παραλήπτη. **E-mail Υπηρεσίες από τρίτους** Οι 3rd-party υπηρεσίες e-mail λειτουργούν με το να προωθούν τα e-mail. **Διανομή Secure SMTP** Η χρησιμοποίηση SMTP μέσω SSL/TLS πρωτόκολλα δεν είναι κοινή.

3.5.4.2 Ψηφιακά υπογεγραμμένα e-mails

Επεκτείνοντας τις ενέργειες για τα ψηφιακά υπογεγραμμένα e-mails,οι εταιρίες μπορούν να ρυθμίσουν τους server εισερχόμενης αλληλογραφίας τους, να επικυρώνουν αυτόματα οποιαδήποτε εισερχόμενα emails έρχονται, τα οποία είναι ψηφιακά υπογεγραμμένα, πριν αυτά φτάσουν στον παραλήπτη τους. Αυτή η διαδικασία φαίνεται να είναι αρκετά αποδοτική για τις εταιρίες, ενώ μπορούν να

προστεθούν κάποια αυτόματα βήματα, που θα ενημερώνουν τους παραλήπτες για άκυρα ή μη υπογεγραμμένα mails.

Παράλληλα, ο servers της εταιρίας για τα εξερχόμενα e-mails μπορεί να ρυθμιστεί κατάλληλα έτσι ώστε να υπογράφει ψηφιακά τα εξερχόμενα e-mails. Λειτουργώντας κατά αυτόν τον τρόπο, ένα γνήσιο, υπογεγραμμένο πιστοποιητικό της εταιρίας θα χρησιμοποιείται μαζί με τα εξερχόμενα e-mails,και οι παραλήπτες θα μπορούν να είναι σίγουροι ότι το mail που έλαβαν είναι αξιόπιστο και γνήσιο.



Σχήμα 27 Αυθεντικοποίηση server με ψηφιακά υπογεγραμμένα μηνύματα

3.5.4.3 Παρακολούθηση Domain

Είναι σημαντικό οι εταιρίες να ελέγχουν προσεκτικά τις εγγραφές των ηλεκτρονικών Domains, τα οποία σχετίζονται με την επιχείρησή τους. Οι εταιρίες πρέπει να ελέγχουν συχνά τον χώρο των Domains, για ονόματα τα οποία είναι ίδια ή παρόμοια με το δικό τους, τα οποία θα μπορούσαν να χρησιμοποιηθούν για να ξεγελάσουν κάποιους καταναλωτές. Υπάρχουν δύο περιοχές ανησυχίας :

1. Η λήξη και η ανανέωση του ήδη υπάρχοντος domain ενός οργανισμού
2. Η εγγραφή-καταχώρηση παρόμοιων domain ονομάτων

Λήξη και ανανέωση Domain Name

Υπάρχουν αρκετές εταιρίες hosting-domain naming οι οποίες επιτρέπουν την καταχώρηση domains που προηγουμένως έχουν χρησιμοποιηθεί από κάποιον οργανισμό ή εταιρία και δεν έχουν ανανεωθεί. Μιας και πλέον, αρκετοί οργανισμοί έχουν πολλαπλά domains, χρειάζεται μεγάλη προσοχή και διαχείριση όσον αφορά τις πληρωμές ανανεώσεων, αν θέλει μια εταιρία να διατηρήσει το domain της. Η αποτυχία επανακαταχώρησης ενός domain, αποτελεί χρονοβόρα διαδικασία η οποία θα έχει ως συνέπεια τη μη διαθεσιμότητα της σελίδας για ένα μεγάλο χρονικό διάστημα ή στην ακόμα χειρότερη περίπτωση, το domain έχει αγοραστεί-καταχωρηθεί από κάποιον τρίτο.

Εγγραφή παρόμοιων domain name

Είναι μια απλή διαδικασία για οποιονδήποτε να καταχωρήσει ένα domain name μέσω της υπηρεσίας καταχωρήσεων, σε οποιοδήποτε μέρος παγκοσμιως. Συνεπώς, είναι συνηθισμένο και αποτελεί ευκαιρία για αρκετούς 'τρίτους' με κατοχυρώσουν ένα domain name το οποίο θα αποτελέσει το μελλοντικό όνομα-σήμα κατατεθέν μιας εταιρίας για να το μεταπωλήσουν σε αυτούς ή για να ξεγελάσουν τους πελάτες στο να πιστέψουν ότι έχουν εισέλθει σε έναν έγκυρο ιστότοπο.

Πλεον, υπάρχουν εμπορικές υπηρεσίες διαθέσιμες οι οποίες βοηθάν τους οργανισμούς να ελέγχουν και να ενημερώνονται για τις πιθανές αλλαγές και για την δημιουργία νέων domains, τα οποία έχουν σχέση με την εταιρία τους. Παρόμοιες, ενημερωτικές υπηρεσίες υπάρχουν επίσης και είναι αυτές που παρατηρούν μεγάλα hacking chat rooms και διάσημα forum συζητήσεων για επιθέσεις phishing και άλλες μεγάλες απάτες.

3.5.4.4 Υπηρεσίες Gateway

Η περίμετρος του δικτύου των επιχειρήσεων είναι ένα ιδανικό μέρος για την προσθήκη υπηρεσιών προστασίας στην gateway που θα μπορούν να παρακολουθούν και να ελέγχουν τόσο τις εισερχόμενες και τις εξερχόμενες επικοινωνίες. Οι υπηρεσίες αυτές μπορούν να χρησιμοποιηθούν για τον εντοπισμό κακόβουλου phishing περιεχομένου που βρίσκεται μέσα σε e-mail άλλα και σε

άλλες ψηφιακές ροές. Οι τυπικές υπηρεσίες gateway σε επίπεδο επιχείρησης περιλαμβάνουν:

- Gateway Anti-Virus Scanning - χρησιμοποιείται για την ανίχνευση των ιών, κακόβουλου scripting κώδικα και binary συνημμένα που περιέχουν Trojan λογισμικό.
- Gateway Anti-Spam Filtering – επίβλεψη που βασίζεται σε κανόνες ελέγχου του περιεχομένου των e-mail για λέξεις κλειδιά, που χρησιμοποιούνται συνήθως για να τον εντοπισμό των κοινών ανεπιθύμητων μηνυμάτων, αλλά είναι ικανή να σταματήσει και πολλές μορφές phishing επιθέσεων που έχουν σχεδιαστεί για να μοιάζουν με απλά spam μηνύματα.
- Gateway Content Filtering - επιθεώρηση των πολλών τύπων των μεθόδων επικοινωνίας (όπως e-mail, IM, AOL, HTTP, FTP) για ‘κακό’ περιεχόμενο ή αιτήματα. Απλή προστασία από τους χρήστες που επισκέπτονται γνωστές επικίνδυνες ιστοσελίδες.
- Υπηρεσίες Proxy - διαχείριση της συνένωσης των πρωτοκόλλων του Διαδικτύου και έλεγχος των επικοινωνιών εξόδου. Προστασία κατά των εισερχόμενων επιθέσεων με τη χρήση της μετάφρασης διευθύνσεων δικτύου. Καλή προστασία ενάντια στη κοινή διαρροή πληροφοριών διαμόρφωσης του εσωτερικού δικτύου.

Πίνακας 14 Πλεονεκτήματα – Μειονεκτήματα εφαρμογής υπηρεσιών gateway

Πλεονεκτήματα	Μειονεκτήματα
Αποδοτικότητα Ενημέρωσης Είναι πολύ πιο εύκολο και πιο γρήγορο, για ένα μεγάλο ίδρυμα να ενημερώνει σχετικά μικρό αριθμό gateway ελέγχων απ’ ότι είναι να εξασφαλίζει ότι όλοι οι desktop έλεγχοι είναι ενημερωμένα. **Ανεξαρτησία ISP** Το φιλτράρισμα του gateway περιεχομένου είναι πολύ	**Περιορισμοί κυκλοφορίας** Ορισμένες μορφές της κίνησης του δικτύου δεν μπορεί να ελεγχθούν. **Αλλαγές Τείχους προστασίας** Ορισμένες gateway εφαρμογές ενδέχεται να απαιτούν χειροκίνητη διαμόρφωση των firewalls και άλλες gateway συσκευές για την εφαρμογή των κανόνων μπλοκαρίσματος.

αποτελεσματικό στο να εμποδίζει την πρόσβαση σε γνωστές ιστοσελίδες phishing ή σε περιεχόμενο phishing, χωρίς να περιμένει από έναν ISP να αφαιρέσει την phishing ιστοσελίδα. **Προληπτική Προστασία** Κακόβουλος κώδικας μπορεί να αποκλειστεί πριν εισέλθει στο δίκτυο.	**Προστασία χρήστη κατά την περιαγωγή** Οι χρήστες περιαγωγής, όπως οι πωλητές που μετακινούνται δεν προστατεύονται από τις υπηρεσίες gateway.

3.6 Επίλογος

Συνοψίζοντας λοιπόν σε αυτό το κεφάλαιο έγινε μια παρουσίαση του κυρίως θέματος της πτυχιακής εργασίας που είναι το Phishing. Αρχικά δόθηκε ένας ορισμός για το phishing και μια ιστορική αναδρομή στην εξέλιξη του. Στη συνέχεια παρουσιάστηκε η απειλή του phishing, οι τρόποι με τους οποίους μεταφέρονται τα μυνήματα phishing και οι τύποι των επιθέσεων phishing. Τέλος αναφέρθηκαν οι μηχανισμοί αντιμετώπισης της απειλής του phishing χωρισμένοι σε τρία επίπεδα στο επίπεδο προστασίας client-side, στο επίπεδο προστασίας server-side και στο επίπεδο προστασίας από τις επιχειρήσεις.

ΚΕΦΑΛΑΙΟ 4

4 Αναλυτική λειτουργία και χρήση της εφαρμογής

4.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο, παρουσιάζονται οι κύριες λειτουργίες της εφαρμογής. Θα αναλυθούν οι τρόποι και οι μέθοδοι που χρησιμοποιήθηκαν για την δημιουργία της, ενώ παράλληλα θα δοθούν κατάλληλα κομμάτια κώδικα έτσι ώστε να γίνει πιο σαφής και κατανοητή.

4.2 Λειτουργίες Εφαρμογής

Η εφαρμογή αποτελεί ένα portal, το οποίο παρέχει πληροφορίες για την κλοπή διαδικτυακής ταυτότητας ή αλλιώς Phishing. Στην εφαρμογή μπορούν να βρεθούν

γενικές πληροφορίες και ιστορικά στοιχεία, σχετικά με το Phishing, τρόποι διάδοσης του και τα είδη των επιθέσεων που χρησιμοποιούν οι εγκληματίες. Στην συνέχεια, αναλύονται οι τρόποι που μπορεί να προστατευτεί ένας μέσος χρήστης, μια εταιρία ή ένας οργανισμός από το Phishing, ενώ παράλληλα, έχουν τοποθετηθεί Videos για την καλύτερη κατανόηση της έννοιας του Phishing και των λειτουργιών του.

4.3 Διαδικασία Ανάπτυξης της Εφαρμογής

4.3.1 Σχεδιασμός και δημιουργία της βάσης δεδομένων της εφαρμογής

Τα δεδομένα της εφαρμογής που χρησιμοποιήθηκαν είναι αποθηκευμένα σε μια SQLite βάση δεδομένων. Για να δημιουργήσουμε την βάση χρησιμοποιήσαμε την Singleton κλάση DatabaseAdapter,μέσα από την οποία δημιουργούνται οι εντολές για την δημιουργία των πινάκων που χρειαζόμαστε, σε μορφή String και τα queries τα οποία μας επιστρέφουν τα αποτελέσματα με την μορφή αντικειμένων. Παράλληλα, σε αυτή την κλάση περιέχεται και η κλάση DatabaseHelper, η οποία αποτελεί επέκταση της SQLiteOpenHelper. Η SQLiteOpenHelper είναι μια κλάση του Android λειτουργικού συστήματος η οποία βοηθά στην δημιουργία μιας SQLite βάσης δεδομένων.

Σε αυτό το κομμάτι του κώδικα, παρουσιάζεται η δημιουργία της βάσης, ενώ παρέχονται και τα SQL insert Statements για την εισαγωγή των δεδομένων.

Δημιουργία της βάσης:

```
protected static final String TAG = "DatabaseAdapter";
    // Table Names
    public static final String TABLE_1 = "TABLE_1";
    public static final String TABLE_2 = "TABLE_2";
    public static final String TABLE_3 = "TABLE_3";
    public static final String TABLE_4 = "TABLE_4";
    public static final String TABLE_5 = "TABLE_5";
    protected static final String mID = "_id";
    protected static final String mTitle = "Title";
    protected static final String mContent = "Content";
    protected static final String mImage = "Image_Path";
    protected static final String mVideoUrl = "URL";
    // Database Version
    private static final int DATABASE_VERSION = 1;
    // Database Name
    private static final String DATABASE_NAME = "PhishingManager";
    private static final String CREATE_TABLE_1 = "CREATE TABLE "
            + TABLE_1 + " (" + mID + " INTEGER PRIMARY KEY NOT NULL,"
            + mTitle + " TEXT NOT NULL, "
            + mContent + " TEXT NOT NULL, "
            + mImage + " TEXT NOT NULL "
            + ")";

      protected static DatabaseHelper mDatabaseHelper;
    protected static DatabaseAdapter instance;
    protected static Context mContext;
    protected SQLiteDatabase db;
```

Sql insert Statements για την εισαγωγή των δεδομένων:

```
private static String[] populateTable1(String mTableName) {
        String[] tableArray = new String[5];

        for (int i = 0; i < tableArray.length; i++) {
            tableArray[i] = " INSERT INTO "
                    + mTableName + " (" + mTitle + ", " + mContent +
", " + mImage + ") " +
                    " VALUES ('" +
mContext.getResources().getStringArray(R.array.table_1_title)[i] +
"'," +
                    " '" +
(mContext.getResources().getStringArray(R.array.table_1_content)[i])
+
                    "', '" +
mContext.getResources().getStringArray(R.array.table_1_images)[i] +
"')";

        }

        return tableArray;

    }


      public static synchronized DatabaseAdapter getInstance(Context
mContext) {
        if (instance == null) {
            instance = new
DatabaseAdapter(mContext.getApplicationContext());

        }

        return instance;
    }
```

Παίρνουμε τα data της βάσης και επιστρέφουμε σε ένα ArrayList αντικειμένων τύπου Fishing:

```
public List<Fishing> getAllTableData(String tableName) {
        ArrayList<Fishing> mFishingList = new ArrayList<Fishing>();
        String selectQuery = "SELECT * FROM " + tableName;
        db = mDatabaseHelper.getReadableDatabase();
        Cursor c = db.rawQuery(selectQuery, null);
        // looping through all rows and adding to list
        if (c.moveToFirst()) {
            do {
                Fishing mFishing = new Fishing();
                mFishing.mTitle =
(c.getString(c.getColumnIndex(mTitle)));
                mFishing.mContent =
(c.getString((c.getColumnIndex(mContent))));
                mFishing.mImage =
((c.getString(c.getColumnIndex(mImage))));


                // adding to todo list
                mFishingList.add(mFishing);
            } while (c.moveToNext());
        }
        c.close();
        return mFishingList;
    }


       public DatabaseAdapter open() throws SQLException {

        mDatabaseHelper =
DatabaseHelper.getInstance(mContext.getApplicationContext());

        db = mDatabaseHelper.getWritableDatabase();

        return this;
    }
```

Η database helper class στην οποία δημιουργούνται οι πίνακες της βάσης:

```
public static class DatabaseHelper extends SQLiteOpenHelper {

        DatabaseHelper(Context context) {
            super(context, DATABASE_NAME, null, DATABASE_VERSION);
        }

        public static DatabaseHelper getInstance(Context mContext) {

            if (mDatabaseHelper == null) {
                mDatabaseHelper = new
DatabaseHelper(mContext.getApplicationContext());
            }
            return mDatabaseHelper;
        }


        @Override
        public void onCreate(SQLiteDatabase db) {
            db.execSQL(CREATE_TABLE_1);
            db.execSQL(CREATE_TABLE_2);
            db.execSQL(CREATE_TABLE_3);
            db.execSQL(CREATE_TABLE_4);
            db.execSQL(CREATE_TABLE_5);
            populateAllTables(db);

        }

        @Override
        public void onUpgrade(SQLiteDatabase db, int oldVersion, int
newVersion) {
            Log.w(TAG, "Upgrading database from version " +
oldVersion + " to "
                    + newVersion + ", which will destroy all old
data");
            db.execSQL("DROP TABLE IF EXISTS " + CREATE_TABLE_1);
            db.execSQL("DROP TABLE IF EXISTS " + CREATE_TABLE_2);
            db.execSQL("DROP TABLE IF EXISTS " + CREATE_TABLE_3);
            db.execSQL("DROP TABLE IF EXISTS " + CREATE_TABLE_4);
            db.execSQL("DROP TABLE IF EXISTS " + CREATE_TABLE_5);
            onCreate(db);
        }


        @TargetApi(Build.VERSION_CODES.JELLY_BEAN)
        @Override
        public void onConfigure(SQLiteDatabase db) {
            super.onConfigure(db);
            db.setForeignKeyConstraintsEnabled(true);

        }

        @Override
        public void onOpen(SQLiteDatabase db) {
            super.onOpen(db);
            if (Build.VERSION.SDK_INT <
Build.VERSION_CODES.JELLY_BEAN) {
                if (!db.isReadOnly()) {
                    db.execSQL("PRAGMA foreign_keys = ON;");
                }
            }
        }
```

4.3.2 Activities που χρησιμοποιήθηκαν

Τα activities που χρησιμοποιήθηκαν είναι τα εξής :

α)SplashScreenActivity

β)FishingActivity

γ)FishingDetailsActivity

4.3.2.1 SplashScreenActivity

Το SplashScreenActivity είναι το εναρκτήριο Activity.Είναι αυτό που εκτελείται όταν ξεκινάει η εφαρμογή. Όταν εκτελείται, εμφανίζει την κύρια εικόνα της εφαρμογής και μετά από ένα χρονικό διάστημα που έχει προδηλωθεί, ξεκινάει το FishingActivity.

```
public class SplashScreenActivity extends Activity {
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_splash_creen);
        Intent mIntent = new Intent(this, FishingActivity.class);
        delay(mIntent);
    }
```

Εκκίνηση του FishingActivity μετά από 3000 millisecond

```
    private void delay(final Intent mIntent) {
        new Handler().postDelayed(new Runnable() {
            @Override
            public void run() {
                startArticleActivity(mIntent);

            }
        }, 3000);
    }
```

Εκκίνηση του νέου Activity

```
private void startArticleActivity(Intent mIntent) {
        this.startActivity(mIntent);
        this.finish();
    }
```

Σχήμα 28 Splash Screen

4.3.2.2 FishingActivity

Το FishingActivity περιέχει ένα NavigationDrawer, το οποίο έχει την λίστα με τις κατηγορίες της εφαρμογής και μια λίστα των data από κάθε κατηγορία.

```
public class FishingActivity extends AppCompatActivity {
    ...
     @Override
 protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_fishing);
    mDrawerLayout = (DrawerLayout) findViewById(R.id.drawer_layout);

        // αρχικοποίηση του NavigationDrawer
        navigationView = (NavigationView)
findViewById(R.id.nav_view);
        if (navigationView != null) {
            setupDrawerContent(navigationView);
            if (savedInstanceState == null)

navigationView.getMenu().performIdentifierAction(R.id.nav_generic,
Menu.FIRST);

        }
```

Παρακάτω παρουσιάζεται το Onclick Event για το άνοιγμα του navigation drawer

```
@Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case android.R.id.home:
                mDrawerLayout.openDrawer(GravityCompat.START);
                return true;
        }
        return super.onOptionsItemSelected(item);
    }
```

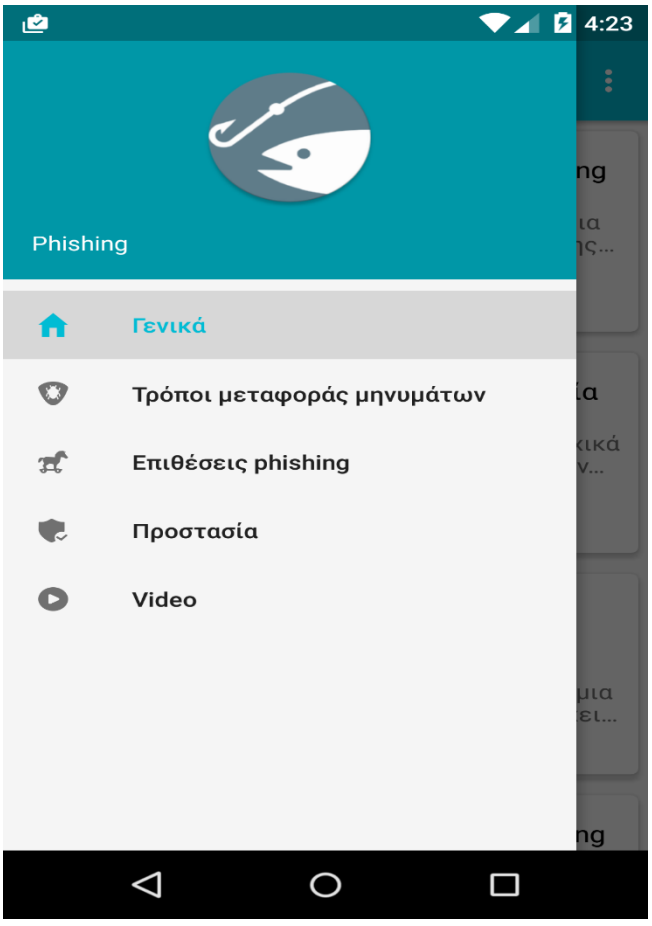
Ενώ εδώ, είναι το OnClick event για την εμφάνιση του Fishing Fragment που

περιέχει τη λίστα με τα data κάθε κατηγορίας:

```
private void setupDrawerContent(NavigationView navigationView) {
        navigationView.setNavigationItemSelectedListener(
                new NavigationView.OnNavigationItemSelectedListener()
{
                    @Override
                    public boolean onNavigationItemSelected(final
MenuItem menuItem) {
                        menuItem.setChecked(true);

                        new Handler().postDelayed(new Runnable() {
                            @Override
                            public void run() {
                                mDrawerLayout.closeDrawers();
                            }
                        }, 100);
                        if
(getSupportFragmentManager().getBackStackEntryCount() > 0) {
                            Log.d("FishingActivity", "Fragment
backstack count is  :" +
getSupportFragmentManager().getBackStackEntryCount());

getSupportFragmentManager().popBackStackImmediate("FishingFragment",
FragmentManager.POP_BACK_STACK_INCLUSIVE);
                        }

getSupportFragmentManager().beginTransaction().replace(R.id.container
, FishingFragment.newInstance(menuItem.getItemId()))
                                .addToBackStack("FishingFragment")
                                .commit();

                        return true;
                    }
                });


    }
```

Το layout του fishing activity που περιέχει το navigation View, δηλαδή το navigation drawer:

```
<?xml version="1.0" encoding="utf-8"?>
<android.support.v4.widget.DrawerLayout
xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:draggable_panel="http://schemas.android.com/tools"
    android:id="@+id/drawer_layout"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:fitsSystemWindows="true">
    <SurfaceView
        android:layout_width="0px"
        android:layout_height="0px"
        android:visibility="gone"/>

    <include layout="@layout/include_list_container" />

    <android.support.design.widget.NavigationView
        android:id="@+id/nav_view"
        android:layout_width="320dp"
        android:layout_height="match_parent"
        android:layout_gravity="start"
        app:headerLayout="@layout/nav_header"
        app:menu="@menu/drawer_view" />
</android.support.v4.widget.DrawerLayout>
```



Σχήμα 29 Navigation Drawer

4.3.2.2.1 FishingFragment

Είναι το Fragment το οποίο περιέχει την λίστα με τα data κάθε κατηγορίας του NavigationDrawer.

```
public class FishingFragment extends Fragment {

    private List<Fishing> mFishingList;
    private RecyclerView mRecyclerView;
    private RecyclerView.LayoutManager mLayoutManager;
    private FishingAdapter mFishingAdapter;
    private int mContentID;

    // Η δημιουργία του fishing fragment όπου περνιέται η επιλογή του
navigation drawer σαν παράμετρος
    public static FishingFragment newInstance(int contentID) {
        FishingFragment mFragment = new FishingFragment();
        Bundle args = new Bundle();
        args.putInt(Utils.CONTENT_ID, contentID);
        mFragment.setArguments(args);
        return mFragment;
    }
```

Σχήμα 30 Fishing Fragment

Η μέθοδος αρχικοποίησης των views του fragment και του adapter της λίστας :

```
@Override
    public void onViewCreated(View view, @Nullable Bundle
savedInstanceState) {
        super.onViewCreated(view, savedInstanceState);

        mFishingList = new ArrayList<>();
        mRecyclerView = (RecyclerView)
getView().findViewById(R.id.fishing_recycler_view);
        mLayoutManager = new LinearLayoutManager(getActivity());
        mRecyclerView.setLayoutManager(mLayoutManager);
        //adapter
        mFishingAdapter = new FishingAdapter(getActivity(),
mFishingList);
        mRecyclerView.setAdapter(mFishingAdapter);
    }

    @Override
    public void onActivityCreated(@Nullable Bundle
savedInstanceState) {
        super.onActivityCreated(savedInstanceState);
        getContent();

    }
```

Η μέθοδος που επιστρέφει τα δεδομένα από τη βάση και ανάλογα με την επιλογή της κατηγορίας από το navigation drawer:

```
private void getContent() {
        DatabaseAdapter mDatabaseAdapter =
DatabaseAdapter.getInstance(getActivity().getApplicationContext());
        mDatabaseAdapter.open();
        switch (mContentID) {
            case R.id.nav_generic:
                mFishingList =
mDatabaseAdapter.getAllTableData(DatabaseAdapter.TABLE_1);
                break;
            case R.id.nav_contamination:
                mFishingList =
mDatabaseAdapter.getAllTableData(DatabaseAdapter.TABLE_2);
                break;
            case R.id.nav_attacks:
                mFishingList =
mDatabaseAdapter.getAllTableData(DatabaseAdapter.TABLE_3);
                break;
            case R.id.nav_security:
                mFishingList =
mDatabaseAdapter.getAllTableData(DatabaseAdapter.TABLE_4);
                break;
            case R.id.nav_video:
                mFishingList = mDatabaseAdapter.getVideoTable();
                break;
        }
        mFishingAdapter.setmFishingList(mFishingList);
        mFishingAdapter.notifyDataSetChanged();

    }
```

FishingAdapter

Είναι ο Adapter που είναι υπεύθυνος για την εμφάνιση των δεδομένων της κάθε σειράς της λίστας. Ο Adapter αυτός παίρνει σαν παράμετρο ένα List με τα αντικείμενα της Fishing, τα οποία περιέχουν τα δεδομένα για την συγκεκριμένη κατηγορία και είναι υπεύθυνος για την εμφάνισή τους.

Για την εμφάνιση των thumbnails των youtube video της εφαρμογής, χρησιμοποιείται μια εξωτερική βιβλιοθήκη, την Picasso. Η συγκεκριμένη βιβλιοθήκη, είναι κατάλληλη για φόρτωση εικόνων μέσω διαδικτύου. Επίσης υπάρχει ένα event onClick, το οποίο ξεκινάει το activity FishingDetailsActivity που εμφανίζει το κάθε άρθρο διαφορετικά, ανάλογα με την θέση του.

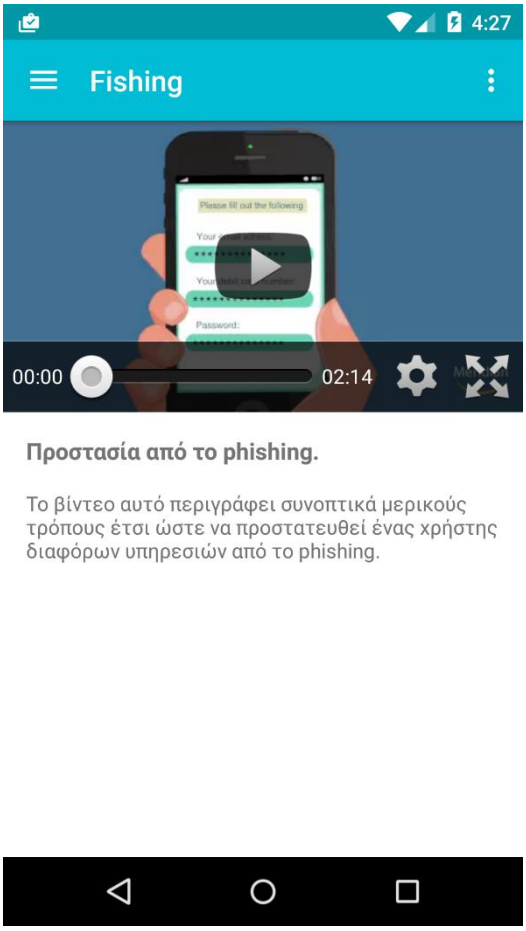
Η μέθοδος που φαίνεται στην παρακάτω φωτογραφία εμφανίζει τα δεδομένα της κάθε σειράς της λίστας:

```
  public void onBindViewHolder(final ViewHolder holder, int position)
{
        holder.mRowContainer.animate().setStartDelay(100 + position *
30).scaleX(1).scaleY(1);
        final Fishing fishing = getValueAt(position);
        final boolean isVideo = fishing.isVideo();

        String thumbnail;

        final int mImageID = Utils.getDrawableId(fishing.mImage,
mActivity);

        holder.mTextView.setText(fishing.mTitle);
        holder.mContentShortTextView.setText(fishing.mContent);

        if (isVideo) {
            if (position == 1) {
                thumbnail = fishing.mImage;
            } else {
                thumbnail = "http://img.youtube.com/vi/" +
fishing.mImage + "/maxresdefault.jpg";
            }
            Picasso.with(mActivity)
                    .load(thumbnail)
                    .into(holder.mImageView);
        } else
            holder.mImageView.setImageResource(mImageID);

        holder.mPlayImageView.setVisibility(isVideo ? View.VISIBLE :
View.GONE);

        holder.mRowContainer.setOnClickListener(new
View.OnClickListener() {
            @Override
            public void onClick(View v) {
                if (!isVideo)
                    ((FishingActivity)
mActivity).animateActivity(holder.mImageView, fishing);
                else
                    ((FishingActivity)
mActivity).showVideoFragment(fishing);
            }
        });


    }
```

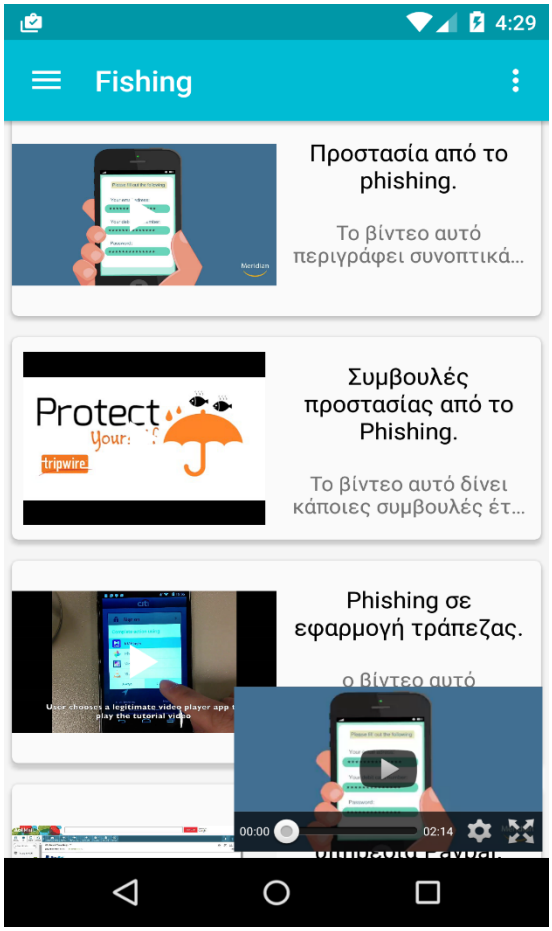
4.3.2.2.2 Video Fragment

Εφόσον ο χρήστης επιλέξει στο NavigationDrawer την κατηγορία Video, το OnClick event μέσα στο Adapter δημιουργεί ένα καινούργιο Fragment, το VideoFragment, που περιέχει ένα Youtube Video με μικρή περιγραφή του συγκεκριμένου video.

Το Video Fragment παρέχει την δυνατότητα στο χρήστη, να κάνει με ένα DragEvent να κάνει minimize το συγκεκριμένο fragment του video που βλέπει, όπου από τη κατάσταση του minimize με κλίκ επανέρχεται στην αρχική του μορφή (maximize), αλλιώς με swipe δεξιά η αριστερά το fragment αφαιρείται. Η συγκεκριμένη λειτουργεία ενσωματώνεται μέσω μιας βιβλιοθήκης, το DraggablePanel.



Σχήμα 32 Video Maximize



Σχήμα 31 Video Minimize

Youtube Api key:

```
private static final String YOUTUBE_API_KEY =
"AIzaSyA9JTeWhQGRzen6cEJ6UyeBZchaf_VMIzA";
```

Αυτή η μέθοδος αρχικοποιεί το youtube player και τα υπόλοιπα views:

```
public void onViewCreated(View view, @Nullable Bundle
savedInstanceState) {
        super.onViewCreated(view, savedInstanceState);

        mYoutubeFragment = (YouTubePlayerSupportFragment)
getChildFragmentManager().findFragmentById(R.id.player_fragment);
        mDraggableView = (DraggableView)
getView().findViewById(R.id.draggable_view);
        mVideoContentTextView = (TextView)
getView().findViewById(R.id.fishing_content_text_view);
        mVideoTitleTextView = (TextView)
getView().findViewById(R.id.fishing_title_text_view);
        mYoutubeContainer = (FrameLayout)
getView().findViewById(R.id.youtube_container);
        initializeDraggableView();
    }
```

Οι παρακάτω μέθοδοι αρχικοποιούν το youtube player με το συγκεκριμένο video που έχει επιλεχθεί από το χρήστη:

```
public void onActivityCreated(@Nullable Bundle savedInstanceState) {
        super.onActivityCreated(savedInstanceState);
        initializeYoutube();
        mVideoContentTextView.setText(mFishing.mContent);
        mVideoTitleTextView.setText(mFishing.mTitle);

    }

    private void initializeYoutube() {
        mYoutubeFragment.initialize(YOUTUBE_API_KEY, this);
    }
```

Εφόσον η αρχικοποίηση είναι επιτυχής καλείται η παρακάτω μέθοδος με την οποία το video αρχίζει την αναπαραγωγή του:

```
public void onInitializationSuccess(YouTubePlayer.Provider provider,
YouTubePlayer youTubePlayer, boolean wasRestored) {
        this.mYoutubePlayer = youTubePlayer;
        mDraggableView.setVisibility(View.VISIBLE);
        mDraggableView.maximize();
        mYoutubeContainer.setVisibility(View.VISIBLE);
        hookDraggablePanelListeners();


mYoutubePlayer.setFullscreenControlFlags(YouTubePlayer.FULLSCREEN_FLA
G_CONTROL_SYSTEM_UI);
        mYoutubePlayer.setFullscreen(false);
        mYoutubePlayer.setOnFullscreenListener(this);
        if (mYoutubePlayer != null && !wasRestored) {
            mYoutubePlayer.cueVideo(mFishing.mVideoUrl);
        }


    }
```

4.3.3 FishingDetailsActivity

Το FishingDetailsActivity είναι το Activity που περιέχει τις λεπτομέρειες (content) του άρθρου της επιλογής του χρήστη.

Δημιουργία του FishingDetailsActivity:

```
public class FishingDetailsActivity extends AppCompatActivity {

     @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_fishing_detail);
```

Το content αυτό παρουσιάζεται μέσω ενός fragment, το FishingDetailFragment που φαίνεται πως δημιουργείται μέσα στο FishingDetailsActivity παρακάτω:

```
if (savedInstanceState == null) {
            getSupportFragmentManager().beginTransaction()
                    .replace(R.id.container,
FishingDetailFragment.newInstance(mFishing),
"FishingDetailsFragment")
                    .addToBackStack("FishingDetailsFragment")
                    .commit();
        }
```

4.3.3.1 *FishingDetailFragment*

Το συγκεκριμένο fragment περιέχει ένα απλό textView και παρουσιάζει τα δεδομένα με το Content της επιλογής του χρήστη.

Σχήμα 33 Fishing details Content

4.4 Επίλογος

Στο τελευταίο αυτό κεφάλαιο παρουσιάστηκαν οι λειτουργίες της εφαρμογής και σημαντικά κομμάτια του κώδικα. Επίσης χρησιμοποιήθηκαν αρκετά παραδείγματα και επίσης παρουσιάστηκαν στιγμιότυπα της εφαρμογής για να γίνει πιο κατανοητή η χρήση της εφαρμογής.

5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα πτυχιακή εργασία, αναπτύχθηκε μια εφαρμογή για κινητά τηλέφωνα και συσκευές που έχουν ως λειτουργικό τους σύστημα το Android. Αναλύσαμε το Λ.Σ του Android στα πρώτα δύο κεφάλαια και αναφέραμε την ιστορία τους, τις ιδιότητές τους και τα χαρακτηριστικά τους, ενώ το μεγαλύτερο κομμάτι της αγοράς των ηλεκτρονικών συσκευών που χρησιμοποιούν κάποιο λειτουργικό σύστημα, χρησιμοποιεί Android.

Η εφαρμογή που αναπτύξαμε, αποτελεί ένα ηλεκτρονικό Portal όπου οι χρήστες θα μπορούν να ενημερώνονται για την εγκληματική απάτη της κλοπής ηλεκτρονικών προσωπικών στοιχείων, το Phishing.Γίνεται επίσης εκτενής αναφορά σε όλες τις τεχνικές των επιθέσεων που χρησιμοποιούν οι εγκληματίες, ενώ ταυτόχρονα οι χρήστες ενημερώνονται πως μπορούν να προστατευτούν από αυτές λαμβάνοντας δραστικά μέτρα, είτε είναι ένας μέσος χρήστης από το σπίτι του, είτε είναι μια μεγάλη εταιρία ή ένας οργανισμός. Βάση δίνεται επίσης, στον τρόπο με τον οποίο επεκτείνεται η τεχνική του Phishing και το πως μπορεί κανείς να πέσει θύμα τέτοιας απάτης. Τέλος, επισυνάπτουμε αρκετά βίντεο, τα οποία με τον τρόπο τους ενημερώνουν τους χρήστες για όλα όσα προαναφέρθηκαν παραπάνω, σε μορφή βίντεο και εικόνων.

6 ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία και άρθρα:

[1] Bill Phillips and Brian Hardy (2013), Android Programming: The Big Nerd Ranch Guide, Atlanta.

[2] Paul Deitel, Harvey Deitel and Abbey Deitel (2014), Android for Programmers: An App-Driven Approach, 2nd Edition, Canada.

[3] McAfee (March 2004), Anti-Phishing: Best Practices for Institutions and Consumers".

[4] A. Litan (14 May 2004), "Phishing Victims Likely Will Suffer Identity Theft Fraud", Gartner Research Note.

Ιστοσελίδες:

[1] Anti-Phishing Working Group - http://www.antiphishing.org/

[2] Google developer guide - http://developer.android.com/guide/index.html

[3] Google developer guide(activities) - http://developer.android.com/guide/components/activities.html

[4] Google developer guide(fragments) - http://developer.android.com/guide/components/fragments.html

[5] Microsoft safety and security center - http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

[6] Google support - https://support.google.com/chrome/answer/99020?hl=el

[7] Norton security - http://us.norton.com/security_response/phishing.jsp

[8] Phishing general - https://en.wikipedia.org/wiki/Phishing