Συνεδρία 11η
Συστάδα 2: Φυσικές Επιστήμες, Τεχνολογία, Φυσική

Δραστηριότητα4: phishing και pharming

Δραστηριότητες

Εισαγωγή στην εκπαιδευτική αξιοποίηση των ΤΠΕ και στο Β1 επίπεδο επιμόρφωσης.

ΕΠΙΜΟΡΦΩΤΗΣ

ΟΒΑΔΙΑΣ ΣΑΒΒΑΣ

Συνεργατική εργασία συναδέλφων:

Group 1

ΔΗΜΗΤΡΙΟΣ ΚΑΒΑΛΙΕΡΟΣ- ΑΝΤΩΝΙΟΣ ΠΟΡΡΟΣ-ΓΕΩΡΓΙΑ ΜΠΑΛΑΣΗ-ΕΡΑΣΜΙΑ ΛΟΥΚΑ
ΙΩΑΝΝΗΣ ΤΡΙΑΝΤΑΦΥΛΛΟΥ-ΝΙΚΟΛΑΟΣ ΕΠΙΣΚΟΠΟΣ
ΧΡΗΣΤΟΣ ΤΣΑΔΗΜΑΣ

Τι είναι το Phishing;

Το ηλεκτρονικό "ψαρέματος" (phishing) είναι ένα έγκλημα στον κυβερνοχώρο στο οποίο ένας ή περισσότεροι στόχοι επικοινωνούν μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου ή γραπτού μηνύματος από κάποιον που θέτει ως νόμιμο ίδρυμα για να προσελκύσει άτομα να παράσχουν ευαίσθητα δεδομένα, όπως στοιχεία προσωπικής ταυτοποίησης, στοιχεία τραπεζικών και πιστωτικών καρτών και κωδικούς πρόσβασης.

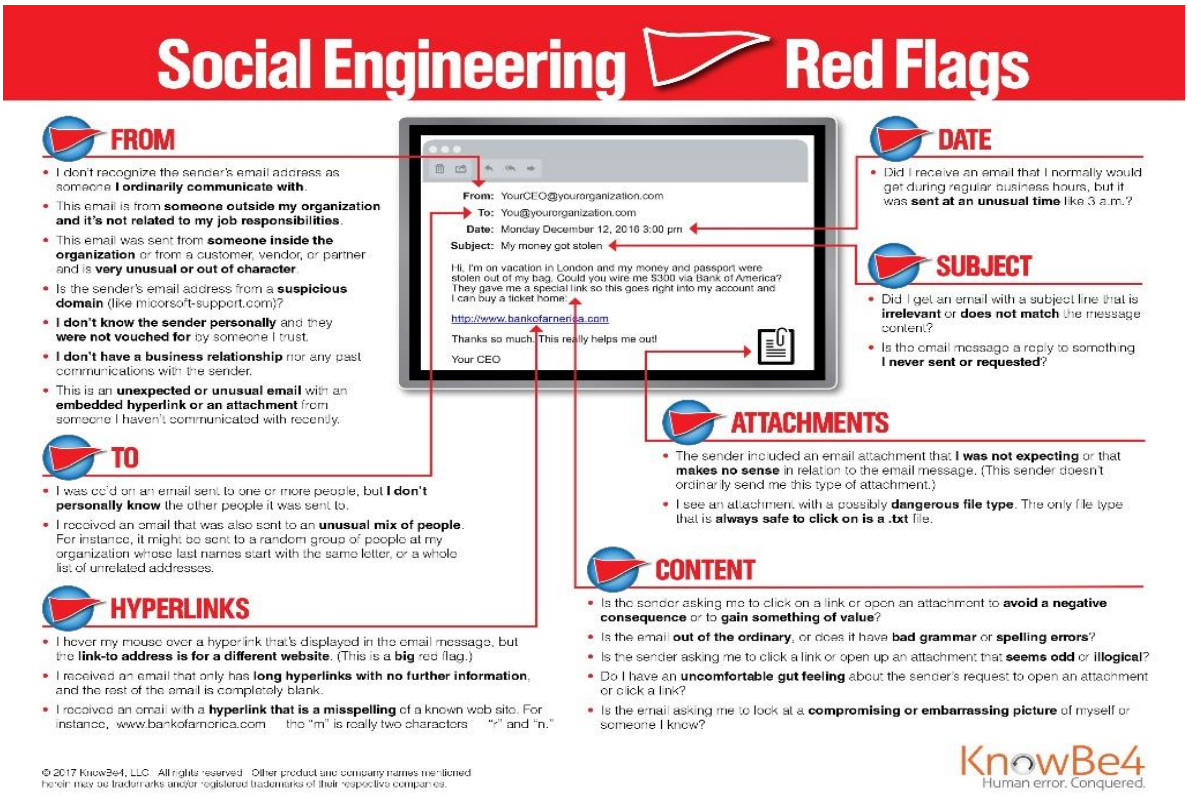
Οι πληροφορίες χρησιμοποιούνται στη συνέχεια για πρόσβαση σε σημαντικούς λογαριασμούς και μπορούν να οδηγήσουν σε κλοπή ταυτότητας και οικονομικές απώλειες.

Η πρώτη αγωγή τύπου phishing **κατατέθηκε το 2004 εναντίον ενός εφήβου της Καλιφόρνιας που δημιούργησε τη μίμηση της ιστοσελίδας "America Online". Με αυτόν τον ψεύτικο ιστότοπο, κατάφερε να αποκτήσει ευαίσθητες πληροφορίες από τους χρήστες και να αποκτήσει πρόσβαση στα στοιχεία της πιστωτικής κάρτας για να αποσύρει χρήματα από τους λογαριασμούς του. Εκτός από e-mail και phishing ιστοσελίδα, υπάρχει επίσης «vishing» (φωνή phishing), «smishing» (SMS Phishing) και πολλά άλλα phishing τεχνικές κυβερνοεγκληματίες έχουν συνεχώς έρχονται με.**

Κοινά χαρακτηριστικά ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος"

1. **Πάρα πολύ καλό να είσαι αληθινός - Οι** προσοδοφόρες προσφορές και οι εντυπωσιακές και προσεκτικές δηλώσεις έχουν σχεδιαστεί για να προσελκύσουν άμεσα την προσοχή των ανθρώπων. Για παράδειγμα, πολλοί ισχυρίζονται ότι έχετε κερδίσει ένα iPhone, μια λαχειοφόρο αγορά ή κάποιο άλλο πλούσιο βραβείο. Απλά μην κάνετε κλικ σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Θυμηθείτε ότι αν φαίνεται καλό να είναι αλήθεια, είναι πιθανότατα!
2. **Αίσθηση επείγουσας ανάγκης -** Μια αγαπημένη τακτική μεταξύ των εγκληματιών στον κυβερνοχώρο είναι να σας ζητήσουμε να ενεργήσετε γρήγορα επειδή οι σούπερ προσφορές είναι μόνο για περιορισμένο χρονικό διάστημα. Ορισμένοι από αυτούς θα σας ενημερώσουν ότι έχετε μόνο λίγα λεπτά για να απαντήσετε. Όταν συναντήσετε αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου, είναι καλύτερο να τα αγνοήσετε. Μερικές φορές, θα σας ενημερώσουν ότι ο λογαριασμός σας θα διακοπεί αν δεν ενημερώσετε αμέσως τα προσωπικά σας στοιχεία. Οι πιο αξιόπιστοι οργανισμοί δίνουν αρκετό χρόνο πριν τερματίσουν έναν λογαριασμό και ποτέ δεν ζητούν από τους προστάτες να ενημερώσουν τα προσωπικά τους στοιχεία μέσω του Διαδικτύου. Σε περίπτωση αμφιβολίας, επισκεφθείτε την πηγή απευθείας αντί να κάνετε κλικ σε ένα σύνδεσμο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.
3. **Υπερσύνδεσμοι -** Ο σύνδεσμος μπορεί να μην είναι το μόνο που φαίνεται να είναι. Τοποθετώντας το δείκτη του ποντικιού πάνω σε έναν σύνδεσμο, εμφανίζεται η πραγματική διεύθυνση URL, στην οποία θα κατευθυνθείτε όταν κάνετε κλικ σε αυτό. Θα μπορούσε να είναι εντελώς διαφορετική ή θα μπορούσε να είναι ένας δημοφιλής ιστότοπος με ορθογραφικό λάθος, για παράδειγμα www.bankofarnerica.com - το 'm' είναι στην πραγματικότητα ένα 'r' και ένα 'n', οπότε κοιτάξτε προσεκτικά.
4. **Συνημμένα -** Αν βλέπετε ένα συνημμένο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που δεν περίμενε κανείς ή δεν έχει νόημα, μην το ανοίξεις! Συχνά περιέχουν ωφέλιμα φορτία όπως ransomware ή άλλους ιούς. Ο μόνος τύπος αρχείου που είναι πάντα ασφαλής να κάνετε κλικ είναι ένα αρχείο .txt.
5. **Ασυνήθιστος αποστολέας -** Είτε πρόκειται για κάποιον που δεν γνωρίζετε, είτε για κάποιον που γνωρίζετε, αν κάτι φαίνεται ξεπερασμένο, απροσδόκητο, από χαρακτήρα ή απλώς ύποπτο γενικά, μην κάνετε κλικ σε αυτό!

Εδώ είναι ένας μεγάλος πόρος KnowBe4 που περιγράφει 22 κόκκινες σημαίες κοινωνικής μηχανικής που συνήθως εμφανίζονται στα ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος" (phishing). Σας συνιστούμε να εκτυπώσετε αυτό το PDF για να περάσετε στην οικογένεια, τους φίλους και τους συναδέλφους σας.



[Κάντε κλικ για μεγαλύτερη προβολή]

Αποτροπή επιθέσεων ηλεκτρονικού "ψαρέματος":

Παρόλο που οι χάκερ συνεχώς έρχονται με νέες τεχνικές, υπάρχουν μερικά πράγματα που μπορείτε να κάνετε για να προστατεύσετε τον εαυτό σας και τον οργανισμό σας:

- Για την προστασία από μηνύματα spam, μπορούν να χρησιμοποιηθούν φίλτρα ανεπιθύμητης αλληλογραφίας. Γενικά, τα φίλτρα εκτιμούν την προέλευση του μηνύματος, το λογισμικό που χρησιμοποιείται για την αποστολή του μηνύματος και την εμφάνιση του μηνύματος για να προσδιορίσει εάν είναι spam. Περιστασιακά, τα φίλτρα ανεπιθύμητης αλληλογραφίας ενδέχεται να μπλοκάρουν ακόμα και τα μηνύματα ηλεκτρονικού ταχυδρομείου από νόμιμες πηγές, επομένως δεν είναι πάντα 100% ακριβή.
- Οι ρυθμίσεις του προγράμματος περιήγησης θα πρέπει να αλλάξουν για να αποτρέψουν το άνοιγμα των πλαστών ιστοτόπων. Τα προγράμματα περιήγησης διατηρούν μια λίστα ψεύτικων ιστότοπων και όταν προσπαθείτε να αποκτήσετε πρόσβαση στον ιστότοπο, η διεύθυνση αποκλείεται ή εμφανίζεται ένα μήνυμα προειδοποίησης. Οι ρυθμίσεις του προγράμματος περιήγησης πρέπει να επιτρέπουν τη δημιουργία αξιόπιστων ιστότοπων.
- Πολλοί ιστότοποι απαιτούν από τους χρήστες να εισάγουν πληροφορίες σύνδεσης ενώ εμφανίζεται η εικόνα του χρήστη. Αυτός ο τύπος συστήματος μπορεί να είναι ανοικτός σε επιθέσεις ασφαλείας. Ένας τρόπος για να διασφαλίσετε την ασφάλεια είναι να αλλάζετε κωδικούς πρόσβασης σε τακτική

βάση και ποτέ να μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς. Είναι επίσης μια καλή ιδέα για τους ιστοτόπους να χρησιμοποιούν ένα σύστημα CAPTCHA για πρόσθετη ασφάλεια.

- Οι τράπεζες και οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν συστήματα παρακολούθησης για την αποτροπή του phishing. Τα άτομα μπορούν να αναφέρουν το phishing σε ομάδες της βιομηχανίας όπου μπορούν να αναληφθούν νομικές ενέργειες εναντίον αυτών των πλαστών ιστοτόπων. Οι οργανισμοί θα πρέπει να παρέχουν κατάρτιση ευαισθητοποίησης για την ασφάλεια των εργαζομένων ώστε να αναγνωρίζουν τους κινδύνους.
- Απαιτούνται αλλαγές στις συνήθειες περιήγησης για την αποτροπή του phishing. Εάν απαιτείται επαλήθευση, επικοινωνήστε πάντα με την εταιρεία προσωπικά πριν εισαγάγετε οποιαδήποτε στοιχεία στο διαδίκτυο.
- Αν υπάρχει σύνδεσμος σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, τοποθετήστε πρώτα το δείκτη του ποντικιού πάνω από τη διεύθυνση URL. Οι ασφαλείς ιστότοποι με ένα έγκυρο πιστοποιητικό SSL (Secure Socket Layer) αρχίζουν με "https". Τελικά όλοι οι ιστότοποι θα πρέπει να έχουν έγκυρο SSL .

Γενικά, τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από έναν κυβερνοεγκληματία καλύπτονται έτσι ώστε να φαίνονται να αποστέλλονται από μια επιχείρηση των οποίων οι υπηρεσίες χρησιμοποιούνται από τον παραλήπτη. Μια τράπεζα δεν θα ζητήσει προσωπικές πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου ή θα αναστείλει τον λογαριασμό σας εάν δεν ενημερώσετε τα προσωπικά σας στοιχεία εντός συγκεκριμένης χρονικής περιόδου. Οι περισσότερες τράπεζες και χρηματοπιστωτικά ιδρύματα παρέχουν επίσης συνήθως έναν αριθμό λογαριασμού ή άλλα προσωπικά στοιχεία εντός του ηλεκτρονικού ταχυδρομείου, γεγονός που εξασφαλίζει ότι προέρχεται από αξιόπιστη πηγή.

Σχετικές σελίδες: Ιστορία phishing , τεχνικές ηλεκτρονικού "ψαρέματος" (phishing) , 10 τρόποι αποφυγής απάτης phishing

Τι είναι η Pharming & πώς να την αποτρέψετε;

Το Pharming, ένα χαρτοφυλάκιο των λέξεων "phishing" και "γεωργία", είναι ένα είδος εγκλήματος στον κυβερνοχώρο παρόμοιο με το ηλεκτρονικό ψάρεμα (phishing), όπου η κυκλοφορία ενός ιστοτόπου χειραγωγείται και κλέβονται εμπιστευτικές πληροφορίες. Η Pharming εκμεταλλεύεται το θεμέλιο του τρόπου με τον οποίο λειτουργεί η περιήγηση στο Διαδίκτυο - δηλαδή, ότι η ακολουθία των γραμμάτων που σχηματίζουν μια διεύθυνση στο Internet, όπως το www.google.com, πρέπει να μετατραπούν σε διεύθυνση IP από έναν διακομιστή DNS για να συνεχιστεί η σύνδεση. Αυτή η εκμετάλλευση προσβάλλει αυτή τη διαδικασία με έναν από τους δύο τρόπους. Πρώτον, ένας χάκερ μπορεί να εγκαταστήσει έναν ιό ή έναν Trojan στον υπολογιστή ενός χρήστη που αλλάζει το αρχείο hosts του υπολογιστή για να κατευθύνει την κυκλοφορία μακριά από τον επιδιωκόμενο στόχο και προς έναν ψεύτικο ιστότοπο. Δεύτερον, ο χάκερ μπορεί να δηλητηριάσει έναν διακομιστή DNS, προκαλώντας πολλαπλούς χρήστες να επισκεφθούν αθέλητα την ψεύτικη τοποθεσία. Οι ψεύτικες ιστοσελίδες μπορούν να χρησιμοποιηθούν για την εγκατάσταση ιών ή trojans στον υπολογιστή του χρήστη ή θα μπορούσαν να είναι μια προσπάθεια συλλογής προσωπικών και οικονομικών πληροφοριών για χρήση στην κλοπή ταυτότητας.

Η Pharming είναι μια ιδιαίτερα ανησυχητική μορφή εγκληματικότητας στον κυβερνοχώρο, επειδή σε περιπτώσεις δηλητηριάσεων διακομιστή DNS, ο επηρεαζόμενος χρήστης μπορεί να έχει έναν υπολογιστή χωρίς κακόβουλο λογισμικό και να γίνει ακόμα θύμα. Ακόμη και η λήψη προφυλάξεων όπως η μη αυτόματη εισαγωγή στη διεύθυνση του ιστότοπου ή η χρήση πάντα αξιόπιστων σελιδοδεικτών δεν αρκεί, επειδή η κακή μετακίνηση συμβαίνει μετά την αποστολή ενός αιτήματος σύνδεσης από τον υπολογιστή.

Προστατεύοντας τον εαυτό σας από αυτούς τους τύπους απάτης ξεκινάει με την εγκατάσταση μιας ισχυρής λύσης προστασίας από κακόβουλο λογισμικό και antivirus, που χρησιμοποιείται σε συνδυασμό με πρακτικές έξυπνων υπολογιστών, όπως η αποφυγή ύποπτων ιστότοπων και η σύνδεση με μηνύματα ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Αυτά τα βήματα θα αποτρέψουν την πρόσβαση των περισσότερων κακόβουλων προγραμμάτων στον υπολογιστή σας και την αλλαγή του αρχείου hosts.

Ωστόσο, αυτό είναι μόνο μέρος της απειλής, έτσι πρέπει επίσης να είστε έξυπνοι για τις ιστοσελίδες που επισκέπτεστε - ειδικά αυτές που περιέχουν τα προσωπικά ή οικονομικά σας στοιχεία. Αν ο ιστότοπος φαίνεται παράξενος, η διεύθυνση στη γραμμή διευθύνσεων φαίνεται ή το site αρχίζει να ζητά πληροφορίες που κανονικά δεν το κάνει, ελέγξτε για να βεβαιωθείτε ότι υπάρχει ένα εικονίδιο κλειδώματος στη γραμμή διευθύνσεων, δηλώνοντας έναν ασφαλή ιστότοπο και πατήστε το κλείδωμα για να βεβαιωθείτε ότι ο ιστότοπος διαθέτει αξιόπιστο, ενημερωμένο πιστοποιητικό. Εκείνοι που εκτελούν διακομιστές DNS έχουν στη διάθεσή τους μερικές πολύ εξελιγμένες τεχνικές κατά της φαρμακοποιίας, αλλά ο κίνδυνος να παραβιαστεί είναι πάντα εκεί, οπότε μπορείτε να μετριάσετε τους κινδύνους μόνο μέσω ενός συνδυασμού προσωπικής προστασίας και ευαισθητοποίησης στο Internet.