Ονοματεπώνυμο: Αλέξης Παπούλιας

ΑΜ: ice19390186

Περιεχόμενα

Εισαγωγή

Στη σημερινή εποχή της τεχνολογίας, η άνοδος του ηλεκτρονικού εγκλήματος έχει γίνει μείζον ζήτημα για τις επιχειρήσεις, τους ιδιώτες, ακόμη και τις κυβερνήσεις. Οι εγκληματίες του κυβερνοχώρου έχουν γίνει πιο εξελιγμένοι στις μεθόδους τους για την απόσπαση εμπιστευτικών δεδομένων και τη διάπραξη απάτης. Τρεις από τις πιο συνηθισμένες μορφές εγκλήματος στον κυβερνοχώρο είναι το smishing, το phishing και το vishing. Αυτές οι τρεις μορφές εγκλήματος στον κυβερνοχώρο περιλαμβάνουν τη χρήση τακτικών κοινωνικής μηχανικής για να εξαπατήσουν τα άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες. Το παρόν έγγραφο θα παράσχει μια ολοκληρωμένη επισκόπηση του smishing, του phishing και του vishing και θα τονίσει τις διαφορές, τις ομοιότητές τους και τα μέτρα που μπορεί να λάβει κανείς για να προστατευτεί από το να πέσει θύμα αυτών των τύπων εγκλήματος στον κυβερνοχώρο.

1. Τι είναι το Vishing[1]

Το Vishing (φωνητικό ψάρεμα) είναι ένας τύπος επίθεσης κοινωνικής μηχανικής όπου οι απατεώνες χρησιμοποιούν μεθόδους φωνητικής επικοινωνίας, όπως τηλεφωνικές κλήσεις, για να χειραγωγήσουν τα άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να εκτελέσουν ορισμένες ενέργειες. Οι επιθέσεις Vishing συνήθως περιλαμβάνουν τον απατεώνα που υποδύεται μια αξιόπιστη οντότητα, όπως μια τράπεζα ή μια κυβερνητική υπηρεσία, και χρησιμοποιεί διάφορες τακτικές για να πείσει το θύμα να αποκαλύψει εμπιστευτικές πληροφορίες, όπως στοιχεία τραπεζικού λογαριασμού, κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών.

Οι επιτιθέμενοι συχνά χρησιμοποιούν προηγμένες τεχνικές, όπως η παραποίηση της ταυτότητας καλούντος ή αυτοματοποιημένα φωνητικά μηνύματα, για να κάνουν τις κλήσεις τους να φαίνονται νόμιμες και να αυξήσουν τις πιθανότητες επιτυχίας τους. Οι επιθέσεις Vishing μπορεί επίσης να περιλαμβάνουν τη χρήση ψεύτικων ιστότοπων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου για να παρασύρουν τα θύματα στην αποκάλυψη ευαίσθητων πληροφοριών. Για να προστατευτείτε από τις επιθέσεις vishing, είναι σημαντικό να είστε προσεκτικοί απέναντι σε ανεπιθύμητες τηλεφωνικές κλήσεις ή μηνύματα, ειδικά αν ζητούν ευαίσθητες πληροφορίες. Δεν θα πρέπει ποτέ να αποκαλύπτετε προσωπικές πληροφορίες μέσω τηλεφώνου, εκτός εάν είστε σίγουροι για την ταυτότητα του καλούντος, και θα πρέπει πάντα να επαληθεύετε τη γνησιότητα οποιουδήποτε αιτήματος πριν προβείτε σε οποιαδήποτε ενέργεια.

1.1 Δημοφιλείς απάτες Vishing

Η Ομοσπονδιακή Επιτροπή Εμπορίου λαμβάνει περίπου το 75% των καταγγελιών για απάτη που περιλαμβάνουν τηλεφωνική επαφή με πελάτες. Αυτά είναι μερικά από τα επαναλαμβανόμενα θέματα:

1. **"Υπονομευμένη" πιστωτική κάρτα ή τραπεζικός λογαριασμός**
   Θα ενημερωθείτε ότι υπάρχει πρόβλημα με τον λογαριασμό σας ή με μια πληρωμή που κάνατε, είτε πρόκειται για ζωντανό πρόσωπο είτε για προηχογραφημένο μήνυμα στην άλλη άκρη. Για να διορθώσετε το πρόβλημα, μπορεί να σας ζητηθεί να δώσετε τα στοιχεία σύνδεσής σας ή να σας ζητηθεί να υποβάλετε μια νέα πληρωμή. Κλείστε το τηλέφωνο και καλέστε το χρηματοπιστωτικό σας ίδρυμα στη γραμμή που είναι διαθέσιμη στο κοινό αντί να δώσετε τα στοιχεία σας.

2. **Φορολογική απάτη**
   Αν και υπάρχουν διάφορες ποικιλίες αυτής της απάτης, συνήθως θα ακούσετε ένα προετοιμασμένο μήνυμα. Σας ενημερώνει ότι υπάρχει πρόβλημα με τη φορολογική σας δήλωση και ότι θα εκδοθεί ένταλμα σύλληψής σας εάν δεν καλέσετε ξανά. Αυτό συνήθως συνδυάζεται από τους απατεώνες με ένα ψεύτικο αναγνωριστικό κλήσης που κάνει να φαίνεται ότι η κλήση προέρχεται από την εφορία. Η κατανόηση του τι μπορεί και τι δεν μπορεί να κάνει η IRS όταν χρειάζεται να επικοινωνήσει μαζί σας είναι σημαντική πριν προχωρήσετε.

3. **Προτάσεις ανεπιθύμητων δανείων ή επενδύσεων**
   Οι απατεώνες τηλεφωνούν και κάνουν προσφορές που φαίνονται εξωπραγματικές. Για παράδειγμα, θα ισχυριστούν ότι μπορείτε να εξοφλήσετε όλα τα χρέη σας με μια μόνο

[1] Jennifer van der Kleut, 2018

γρήγορη επισκευή, να βγάλετε εκατομμύρια δολάρια με μια μόνο μικροσκοπική επένδυση ή να σας διαγραφούν όλα τα χρέη σας στο πανεπιστήμιο με τη μία. Συνήθως, θα πρέπει να "δράσετε τώρα" και να πληρώσετε ένα μικρό αντίτιμο. Αποφύγετε να την πατήσετε. Αυτού του είδους οι προτάσεις και οι απροσδόκητες επαφές δεν γίνονται από νόμιμους δανειστές και επενδυτές ούτε ξεκινούν από αυτούς.

4. **Απάτη κοινωνικής ασφάλισης ή Medicare**
   Σύμφωνα με την Ομοσπονδιακή Επιτροπή Εμπορίου, οι τηλεφωνικές κλήσεις σε ηλικιωμένους είναι ο προτιμώμενος τρόπος επικοινωνίας των απατεώνων. Προκειμένου να αποκτήσουν οικονομικές πληροφορίες από το θύμα, όπως τον αριθμό Medicare ή τα στοιχεία του τραπεζικού λογαριασμού του, οι κλέφτες συχνά παριστάνουν τους εκπροσώπους του Medicare κατά τη διάρκεια της περιόδου ανοικτής εγγραφής στο Medicare. Στη συνέχεια, ο απατεώνας είτε κλέβει τα χρήματα του θύματος είτε χρησιμοποιεί με δόλιο τρόπο τις παροχές του Medicare. Ο αριθμός κοινωνικής ασφάλισης του θύματος μπορεί να ανασταλεί ή να ακυρωθεί από απατεώνες που απειλούν να το πράξουν, ενώ παριστάνουν τους εκπροσώπους της Διοίκησης Κοινωνικής Ασφάλισης.

1.2 Πώς να αναγνωρίσετε μια απάτη Vishing

Ακολουθούν ορισμένα προειδοποιητικά σήματα μιας απάτης vishing:

1. Ο καλούντας ισχυρίζεται ότι μιλάει για τη Διοίκηση Κοινωνικής Ασφάλισης, το Medicare ή την IRS. Καμία από αυτές τις κυβερνητικές υπηρεσίες δεν θα έρθει ποτέ σε επαφή μαζί σας μέσω ηλεκτρονικού ταχυδρομείου, κειμένου ή μέσων κοινωνικής δικτύωσης για να σας ζητήσει προσωπικές ή οικονομικές πληροφορίες, εκτός αν το ζητήσετε ρητά. Στην πραγματικότητα, να είστε επιφυλακτικοί με οποιονδήποτε σας τηλεφωνεί και σας κάνει μια προσφορά.

2. Υπάρχει μια απελπισμένη αίσθηση αναγκαιότητας. Οι απατεώνες θα χρησιμοποιήσουν απειλές για εντάλματα σύλληψης και ζητήματα με τον λογαριασμό σας για να προσπαθήσουν να απευθυνθούν στο αίσθημα τρόμου που έχετε. Εάν λάβετε ένα από αυτά τα τηλεφωνήματα, μην πανικοβληθείτε και αποφύγετε να δώσετε τα δικά σας στοιχεία. Κλείστε το τηλέφωνο και κάντε τη δική σας έρευνα.

1.3 Πώς να αποφύγετε να πέσετε θύμα Vishing

Εκτός από την κατανόηση του τρόπου λειτουργίας του vishing και την παρακολούθηση των προειδοποιητικών σημάτων, μπορείτε επίσης:

1. Να εγγραφείτε στην εθνική λίστα μη τηλεφωνικών κλήσεων. Δεν κοστίζει τίποτα να προσθέσετε τον αριθμό του σπιτιού ή του κινητού σας τηλεφώνου σε αυτό το μητρώο, το οποίο ενημερώνει τους τηλεπωλητές ότι δεν επιθυμείτε να λαμβάνετε τις κλήσεις τους. Αυτό δεν θα σταματήσει κανέναν από το να τηλεφωνεί παράνομα στον αριθμό σας, αν και ορισμένοι οργανισμοί, όπως φιλανθρωπικές οργανώσεις και πολιτικές οργανώσεις, ενδέχεται να εξακολουθούν να σας τηλεφωνούν.

2. Αρνηθείτε να απαντήσετε στο τηλέφωνο. Αν και μπορεί να είναι δελεαστικό, αφήστε τον τηλεφωνητή να αναλάβει τις εισερχόμενες κλήσεις. Είναι πιθανό οι ταυτότητες καλούντος να είναι παραποιημένες, οπότε μπορεί να μην αναγνωρίσετε τον καλούντα.

Μπορείτε να επιλέξετε αν θα καλέσετε ξανά το άτομο αφού ακούσετε τα μηνύματά σας.

3. Αφήστε το τηλέφωνο κάτω. Μην αισθάνεστε υποχρεωμένοι να συνεχίσετε μια ευγενική συζήτηση αν έχετε λόγους να πιστεύετε ότι η τηλεφωνική επαφή είναι απάτη. Απλώς τερματίστε την κλήση και μπλοκάρετε τον αριθμό.

4. Μην πατάτε κουμπιά και μην απαντάτε σε ερωτήσεις. Μην πατάτε κουμπιά και μην δίνετε απαντήσεις σε ερωτήσεις, αν λάβετε ένα αυτοματοποιημένο μήνυμα που σας το ζητά. Για παράδειγμα, στο μήνυμα μπορεί να λέτε "ναι" για να μιλήσετε με έναν χειριστή ή "Πατήστε 2 για να διαγραφείτε από τη λίστα μας". Αυτές οι τεχνικές χρησιμοποιούνται συχνά από επιτήδειους για να βρουν νέους στόχους για ρομποτικές κλήσεις.

5. Διαπιστώστε τη νομιμότητα του καλούντος. Εάν ο καλών σας δώσει αριθμό επανάκλησης, μην τον χρησιμοποιήσετε, διότι μπορεί να αποτελεί μέρος της απάτης. Αντ' αυτού, αναζητήστε τον επίσημο δημόσιο αριθμό τηλεφώνου της εταιρείας και καλέστε την.

1.4 Πώς να ανακάμψετε από μια επίθεση Vishing

Καλέστε πρώτα το χρηματοπιστωτικό σας ίδρυμα, αν δώσατε τις οικονομικές σας πληροφορίες σε κάποιον που στη συνέχεια συνειδητοποιήσατε ότι είναι απατεώνας. Καλέστε την εταιρεία πιστωτικών καρτών, την τράπεζα ή την επαφή σας με το Medicare και ρωτήστε σχετικά με την απαγόρευση μελλοντικών χρεώσεων και την ακύρωση δόλιων συναλλαγών. Για να διασφαλίσετε ότι κανείς δεν θα χρησιμοποιήσει τους υπάρχοντες λογαριασμούς σας, ίσως χρειαστεί επίσης να αλλάξετε τους αριθμούς των λογαριασμών σας. Οι πιστωτικές σας αναφορές μπορούν να κλειδωθούν, εμποδίζοντας οποιονδήποτε να ανοίξει νέους λογαριασμούς στο όνομά σας. στη συνέχεια, υποβάλετε καταγγελία στο Κέντρο Καταγγελιών για Εγκλήματα στο Διαδίκτυο του FBI ή στην Ομοσπονδιακή Επιτροπή Εμπορίου. Οι επιθέσεις Vishing έχουν σχεδιαστεί για να σας ξεγελάσουν, αλλά μπορείτε να αναγνωρίσετε τα προειδοποιητικά σημάδια πριν απαντήσετε στο τηλέφωνο, ευαισθητοποιούμενοι. Αποφύγετε να σας προλάβουν οι εγκληματίες του κυβερνοχώρου που προσπαθούν να υποκλέψουν τις προσωπικές σας πληροφορίες μέσω τηλεφώνου.

2. Τι είναι το Phishing[2]

Το "ψάρεμα" είναι ένας τύπος κυβερνοεπίθεσης κατά την οποία ο επιτιθέμενος προσπαθεί να εξαπατήσει τα άτομα ώστε να δώσουν ευαίσθητες πληροφορίες, όπως στοιχεία σύνδεσης, αριθμούς πιστωτικών καρτών ή άλλα προσωπικά δεδομένα. Αυτό συνήθως γίνεται με την αποστολή απατηλών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή μηνυμάτων που φαίνεται να προέρχονται από μια αξιόπιστη πηγή, όπως μια τράπεζα ή μια γνωστή εταιρεία.

Σκοπός του phishing είναι η απόκτηση ευαίσθητων πληροφοριών που μπορούν να χρησιμοποιηθούν για δόλιους σκοπούς, όπως η κλοπή χρημάτων ή ταυτοτήτων. Ο επιτιθέμενος συχνά χρησιμοποιεί τακτικές κοινωνικής μηχανικής για να κάνει το μήνυμα ηλεκτρονικού ταχυδρομείου ή το μήνυμα να φαίνεται επείγον ή σημαντικό και μπορεί να περιλαμβάνει

[2] Coolweb.gr, 2022

συνδέσμους προς ψεύτικους ιστότοπους ή φόρμες όπου το θύμα καλείται να εισάγει τις προσωπικές του πληροφορίες.

Οι επιθέσεις phishing μπορεί να είναι δύσκολο να εντοπιστούν, καθώς συχνά φαίνονται νόμιμες και προέρχονται από αξιόπιστη πηγή. Είναι σημαντικό να είστε προσεκτικοί όταν λαμβάνετε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα και να επαληθεύετε τη γνησιότητα οποιουδήποτε αιτήματος για προσωπικές πληροφορίες πριν τις παράσχετε.

2.1 Πως λειτουργεί το Phishing

Η ακόλουθη είναι η πιο τυπική μέθοδος κλοπής προσωπικών πληροφοριών. Για να δελεάσουν τα δυνητικά θύματά τους, οι απατεώνες (γνωστοί και ως phishers στην προκειμένη περίπτωση) δημιουργούν έναν ψεύτικο ιστότοπο-κλώνο που αποτελεί αντίγραφο της αυθεντικής σελίδας ενός γνωστού οργανισμού (όπως το PayPal, ιστοσελίδες τραπεζών, το Facebook, το Amazon, το eBay κ.λπ.).

Στη συνέχεια, στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου σε πιθανούς επισκέπτες αυτής της σελίδας, παρακαλώντας τους να εισάγουν τα προσωπικά τους στοιχεία επειδή, σύμφωνα με τα μηνύματα, κάτι δεν πάει καλά με τον λογαριασμό τους ή ότι έχουν πέσει θύματα απάτης και πρέπει να αποκαλύψουν τα πραγματικά τους στοιχεία.

Στην πραγματικότητα δεν έχει συμβεί τίποτα και αυτό ακριβώς είναι το μήνυμα της απάτης. Τώρα, αν το θύμα έχει τσιμπηθεί, η διαδικασία εξελίσσεται κάπως έτσι:

1. Ο ψεύτικος ιστότοπος καταγράφει το όνομα χρήστη και τον κωδικό πρόσβασής σας όταν προσπαθείτε να συνδεθείτε στην προσποιητή σελίδα, όπως το web banking της τράπεζάς σας.

2. Μόλις ο απατεώνας αποκτήσει τη σύνδεση και τον κωδικό πρόσβασής σας, μπορεί να αποκτήσει πρόσβαση στο λογαριασμό σας και σε όλα όσα τον συνοδεύουν.

2.2 Πώς να προστατευτείτε από το Phishing [3]

Ευτυχώς, υπάρχουν μέτρα που μπορούμε να λάβουμε για να προφυλαχθούμε από αυτό το επικίνδυνο περιστατικό, αρκεί να έχουμε υπόψη μας τις παρακάτω συμβουλές.

1. Καμία τράπεζα, και πιθανότατα καμία αξιοσέβαστη επιχείρηση, δεν θα σας στείλει μήνυμα ηλεκτρονικού ταχυδρομείου ή θα σας καλέσει για να σας ζητήσει προσωπικές πληροφορίες όπως ονόματα χρηστών ή αριθμούς τηλεφώνου.

2. Αποφύγετε να ανοίγετε μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου. Ίσως έχετε παρατηρήσει ότι κατά καιρούς λαμβάνετε πλασματικά μηνύματα ηλεκτρονικού ταχυδρομείου από τράπεζες με τις οποίες δεν έχετε καμία σχέση.

3. Απομακρύνουμε αμέσως οτιδήποτε "περίεργο" λαμβάνουμε, ειδικά αν βρίσκεται στο φάκελο ανεπιθύμητων μηνυμάτων.

[3] Federal Trade Commission Consumer Advice, September 2022

4. Ακόμα και αν ένα email φαίνεται να προέρχεται από την τράπεζά μας ή την PayPal, αυτό δεν σημαίνει απαραίτητα ότι προέρχεται.

5. Τα ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος", όπως είναι γνωστά, είναι συχνά κακογραμμένα, γενικά και γεμάτα ορθογραφικά λάθη.

6. Ποτέ δεν κάνουμε κλικ σε συνδέσμους σε τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου, αν τα ανοίξουμε. Είναι προτιμότερο να πληκτρολογούμε τη διεύθυνση με το χέρι.

7. Πριν να χρησιμοποιήσουμε τέτοιες υπηρεσίες, βεβαιωνόμαστε ότι η σύνδεση είναι κρυπτογραφημένη, ότι βρισκόμαστε στο σωστό μέρος και ότι υπάρχει το απαραίτητο πιστοποιητικό ασφαλείας, κοιτάζοντας τη γραμμή URL.

8. Προκειμένου να διασφαλίσουμε τους άλλους χρήστες, πατάμε αμέσως "αναφορά" αν διαπιστώσουμε ότι μια επικοινωνία δεν προέρχεται από τον υποτιθέμενο αποστολέα.

3. Τι είναι το Smishing[4]

Το Smishing είναι ένας τύπος κυβερνοεπίθεσης που χρησιμοποιεί μηνύματα κειμένου (SMS) για να εξαπατήσει τους ανθρώπους ώστε να παράσχουν προσωπικές πληροφορίες ή να κατεβάσουν κακόβουλο λογισμικό στις συσκευές τους. Ο όρος "smishing" είναι ένας συνδυασμός των λέξεων "SMS" και "phishing".

Σε μια επίθεση smishing, οι απατεώνες συνήθως στέλνουν μηνύματα κειμένου στα θύματα ισχυριζόμενοι ότι προέρχονται από μια αξιόπιστη εταιρεία ή οργανισμό, όπως μια τράπεζα ή μια κυβερνητική υπηρεσία. Το μήνυμα συχνά περιέχει έναν σύνδεσμο που, όταν πατηθεί, οδηγεί το θύμα σε έναν ψεύτικο ισότοπο σχεδιασμένο να μοιάζει με τον νόμιμο. Στη συνέχεια, το θύμα καλείται να εισάγει τις προσωπικές ή οικονομικές του πληροφορίες, τις οποίες στη συνέχεια συλλέγουν οι απατεώνες.

Το Smishing μπορεί επίσης να περιλαμβάνει τη χρήση κακόβουλου λογισμικού ή ιών που μεταμφιέζονται σε ακίνδυνους συνδέσμους ή συνημμένα αρχεία σε μηνύματα κειμένου. Όταν το θύμα κάνει κλικ στο σύνδεσμο ή ανοίγει το συνημμένο, το κακόβουλο λογισμικό μολύνει τη συσκευή του, επιτρέποντας στον επιτιθέμενο να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες ή τον έλεγχο της συσκευής.

3.1 Πως λειτουργεί το Smishing

Τα θεμελιώδη στοιχεία κάθε επίθεσης SMS phishing είναι η εξαπάτηση και η απάτη. Είστε πιο πρόθυμοι να συμμορφωθείτε με τις απαιτήσεις του επιτιθέμενου επειδή υιοθετεί μια προσωπικότητα που μπορεί να εμπιστεύεστε.

Χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής, οι επιτιθέμενοι στο smishing μπορούν να επηρεάσουν την κρίση του θύματος. Αυτή η ψευδαίσθηση υποκινείται από τρία πράγματα:

1. Εμπιστοσύνη: Οι εγκληματίες του κυβερνοχώρου αυξάνουν το επίπεδο εμπιστοσύνης του στόχου τους μεταμφιέζοντας τους εαυτούς τους σε αξιόπιστους ανθρώπους και

[4] Kaspersky, 2022

επιχειρήσεις. Όντας μια πιο ιδιωτική μορφή επικοινωνίας, τα μηνύματα SMS μειώνουν επίσης εγγενώς την άμυνα ενός ατόμου έναντι απειλών.

2. Πλαίσιο: Ένας επιτιθέμενος μπορεί να δημιουργήσει μια πειστική μεταμφίεση χρησιμοποιώντας μια κατάσταση που μπορεί να είναι σχετική με το θύμα του. Η προσωπική πινελιά του μηνύματος βοηθά να διαλυθούν τυχόν ανησυχίες ότι μπορεί να πρόκειται για ανεπιθύμητη αλληλογραφία.

3. Συναίσθημα: Οι επιτιθέμενοι μπορούν να εξουδετερώσουν την κριτική σκέψη του στόχου τους και να τον ωθήσουν σε γρήγορη δράση προκαλώντας τα συναισθήματά του.

Χρησιμοποιώντας αυτές τις μεθόδους, οι επιτιθέμενοι γράφουν μηνύματα που θα κάνουν τον παραλήπτη να αναλάβει δράση.

Συνήθως, οι επιτιθέμενοι ζητούν από τον παραλήπτη να κάνει κλικ σε έναν σύνδεσμο URL μέσα στο μήνυμα κειμένου, ο οποίος τον κατευθύνει σε ένα εργαλείο phishing που του ζητά τα προσωπικά του δεδομένα. Ένας ιστότοπος ή μια εφαρμογή που αναλαμβάνει επίσης μια ψεύτικη ταυτότητα χρησιμεύει συχνά ως αυτό το όπλο phishing.

Οι στόχοι επιλέγονται με διάφορους τρόπους, αλλά συνήθως επιλέγονται με βάση τους περιφερειακούς ή οργανωτικούς δεσμούς τους. Στους στόχους μπορεί να περιλαμβάνονται όσοι εργάζονται ή χρησιμοποιούν μια συγκεκριμένη επιχείρηση, χρήστες δικτύων κινητής τηλεφωνίας, φοιτητές, ακόμη και ντόπιοι.

Συνήθως, η μεταμφίεση ενός επιτιθέμενου αντιστοιχεί στην εγκατάσταση στην οποία προσπαθεί να εισέλθει. Οποιαδήποτε μεταμφίεση, ωστόσο, έχει τη δυνατότητα να τους βοηθήσει να αποκτήσουν την ταυτότητά σας ή τις οικονομικές σας πληροφορίες.

Η πλαστογράφηση επιτρέπει σε έναν επιτιθέμενο να αποκρύψει τον πραγματικό του αριθμό τηλεφώνου πίσω από έναν ψεύτικο. Για να αποκρύψουν περαιτέρω την πηγή της επίθεσης, οι επιτιθέμενοι στο smishing μπορούν επίσης να χρησιμοποιήσουν "τηλέφωνα καυστήρα", τα οποία είναι φθηνά, προπληρωμένα τηλέφωνα μιας χρήσης. Οι υπηρεσίες email-to-text είναι μια γνωστή τακτική που χρησιμοποιούν οι επιτιθέμενοι για να αποκρύψουν τους τηλεφωνικούς τους αριθμούς.

3.2 Τύποι επιθέσεων Smishing

Παρόμοιες τεχνικές χρησιμοποιούνται σε κάθε επίθεση smishing, ωστόσο η παρουσίαση μπορεί να διαφέρει σημαντικά. Προκειμένου να διατηρήσουν ενδιαφέρουσες αυτές τις επιθέσεις SMS, οι επιτιθέμενοι ενδέχεται να χρησιμοποιούν ένα ευρύ φάσμα ταυτοτήτων και τοποθεσιών.

Δυστυχώς, η συνεχής καινοτομία αυτών των επιθέσεων καθιστά έναν πλήρη κατάλογο των τύπων smishing πρακτικά δύσκολο. Μπορούμε να εντοπίσουμε τα χαρακτηριστικά που θα σας επιτρέψουν να αναγνωρίσετε μια επίθεση smishing πριν την πατήσετε, χρησιμοποιώντας μερικές καθιερωμένες αρχές απάτης.

Ακολουθούν ορισμένες κοινές προϋποθέσεις των επιθέσεων smishing:

1. **COVID-19 Smishing**

   Οι απάτες που αφορούν την επιδημία COVID-19 βασίζονται σε πρωτοβουλίες πραγματικής βοήθειας που έχουν δημιουργηθεί από κυβερνητικά, ιατρικά και

χρηματοπιστωτικά ιδρύματα. Οι επιτιθέμενοι έχουν χειραγωγήσει την οικονομική και σωματική κατάσταση των θυμάτων χρησιμοποιώντας αυτές τις τακτικές σε μια προσπάθεια διάπραξης απάτης. Μεταξύ των προειδοποιητικών δεικτών είναι

a. Παρακολούθηση επαφών που ζητούν προσωπικές πληροφορίες (αριθμός κοινωνικής ασφάλισης, αριθμός πιστωτικής κάρτας κ.λπ.)
b. Οικονομική βοήθεια που βασίζεται σε φόρους, όπως πληρωμές για κίνητρα.
c. Ενημερώσεις σχετικά με τη δημόσια υγεία και ασφάλεια.
d. Αιτήματα για την ολοκλήρωση της απογραφής των ΗΠΑ.

2. Χρηματοοικονομικές υπηρεσίες Smishing

Επιθέσεις όπως το smishing μεταμφιέζονται σε ειδοποιήσεις από χρηματοπιστωτικά ιδρύματα. Δεδομένου ότι σχεδόν όλοι χρησιμοποιούν τραπεζικές υπηρεσίες και υπηρεσίες πιστωτικών καρτών, μπορούν να τους παραδοθούν τόσο γενικά μηνύματα όσο και μηνύματα που αφορούν συγκεκριμένα ιδρύματα. Άλλες τυπικές εγκαταστάσεις σε αυτόν τον τομέα περιλαμβάνουν δάνεια και επενδύσεις. Ως τέλειο καμουφλάζ, ένας επιτιθέμενος υποδύεται μια τράπεζα ή ένα άλλο χρηματοπιστωτικό ίδρυμα για να διαπράξει απάτη με χρήματα. Μια απάτη smishing χρηματοπιστωτικών υπηρεσιών μπορεί να σας ζητήσει να επαληθεύσετε ύποπτη δραστηριότητα στον λογαριασμό σας ή να κάνετε επείγον αίτημα για να ξεκλειδώσετε τον λογαριασμό σας, μεταξύ άλλων.

3. Gift Smishing

Το gift smishing αναφέρεται στην προσφορά δωρεάν αγαθών ή υπηρεσιών, συχνά από έναν αξιοσέβαστο έμπορο ή άλλη επιχείρηση. Αυτές μπορεί να είναι δωρεάν προσφορές για αγορές, διαγωνισμοί δώρων ή οποιαδήποτε άλλα πράγματα. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει την έννοια του "δωρεάν" για να αυξήσει τον ενθουσιασμό σας και να ανταποκριθείτε πιο γρήγορα, παρακάμπτοντας τον ορθολογισμό σας. Οι προσφορές περιορισμένης διάρκειας ή μια ειδική ευκαιρία για την επιλογή μιας δωρεάν δωροκάρτας μπορεί να είναι ενδείξεις αυτής της επίθεσης.

4. Τιμολόγιο ή επιβεβαίωση παραγγελίας Smishing

Οι ψευδείς επιβεβαιώσεις πρόσφατων αγορών ή τιμολογίων χρέωσης υπηρεσιών είναι γνωστές ως "confirmation smishing". Μπορεί να προσφερθεί ένας σύνδεσμος παρακολούθησης για να κεντρίσει το ενδιαφέρον σας ή να σας υποχρεώσει σε γρήγορη δράση για να προκαλέσει φόβο για μη εξουσιοδοτημένες χρεώσεις. Αλυσίδες κειμένων επιβεβαίωσης παραγγελίας ή η έλλειψη ονόματος εταιρείας μπορεί να χρησιμεύσουν ως ενδείξεις ότι πρόκειται για απάτη.

5. Υποστήριξη πελατών Smishing

Για να σας βοηθήσουν στην επίλυση ενός προβλήματος, οι επιτιθέμενοι που ασχολούνται με το smishing υποστήριξης πελατών προσποιούνται ότι είναι το προσωπικό υποστήριξης μιας αξιόπιστης εταιρείας. Σε αυτή την υπόθεση, οι εταιρείες τεχνολογίας και ηλεκτρονικού εμπορίου υψηλής χρήσης, όπως η Apple, η Google και η Amazon, αποτελούν χρήσιμα προσχήματα για τους επιτιθέμενους. Ένας επιτιθέμενος συνήθως ισχυρίζεται ότι ο λογαριασμός σας έχει κάποιο πρόβλημα και σας παρέχει οδηγίες για το πώς να το διορθώσετε. Οι απλούστερες απάτες μπορεί να σας προτρέπουν να χρησιμοποιήσετε μια ψεύτικη σελίδα σύνδεσης, ενώ οι πιο εξελιγμένες μπορεί να σας ζητούν να εισαγάγετε έναν πραγματικό κωδικό ανάκτησης λογαριασμού

σε μια προσπάθεια να επαναφέρετε τον κωδικό πρόσβασής σας. Ένα πρόβλημα με την τιμολόγηση, την πρόσβαση στο λογαριασμό, μια περίεργη δραστηριότητα ή η απάντηση στην πιο πρόσφατη καταγγελία του πελάτη σας είναι όλα σημάδια ενός σχεδίου smishing με βάση την υποστήριξη.

3.3 Πώς να προστατευτείτε από το Smishing

Τα καλά νέα είναι ότι είναι απλό να αμυνθείτε απέναντι στις πιθανές συνέπειες αυτών των επιθέσεων. Δεν χρειάζεται να κάνετε τίποτα για να είστε ασφαλείς. Στην ουσία, μπορείτε να πάθετε κακό από τις επιθέσεις μόνο αν δεχτείτε το δόλωμα.

Έχοντας αυτό υπόψη σας, να θυμάστε ότι πολλές επιχειρήσεις και φορείς έχουν νόμιμους τρόπους να επικοινωνούν μαζί σας μέσω γραπτών μηνυμάτων. Παρόλο που ορισμένα μηνύματα δεν πρέπει να αγνοούνται, να απαντάτε πάντα με προσοχή.

Υπάρχουν μερικά πράγματα που πρέπει να έχετε κατά νου και θα σας βοηθήσουν να προστατευτείτε από αυτές τις επιθέσεις.

1. Μην απαντήσετε. Ακόμη και τα αιτήματα για απαντήσεις, όπως η αποστολή μηνύματος "STOP" για την ακύρωση μιας συνδρομής, μπορούν να χρησιμοποιηθούν ως τέχνασμα για τον εντοπισμό ζωντανών τηλεφωνικών αριθμών. Οι επιτιθέμενοι βασίζονται στο ενδιαφέρον ή την ανησυχία σας για το τρέχον θέμα, αλλά έχετε τη δυνατότητα να απομακρυνθείτε.

2. Εάν ένα μήνυμα είναι επείγον, προχωρήστε πιο αργά. Οι προσφορές περιορισμένου χρόνου και οι επείγουσες ενημερώσεις λογαριασμού μπορούν να θεωρηθούν ως προειδοποιητικοί δείκτες για πιθανό smishing. Έχετε ανοιχτό μυαλό και κινηθείτε με προσοχή.

3. Αν δεν είστε σίγουροι, επικοινωνήστε αμέσως με την τράπεζά σας ή τον έμπορο λιανικής πώλησης. Οι γνήσιοι οργανισμοί δεν στέλνουν ποτέ γραπτά μηνύματα για ενημερώσεις λογαριασμού ή πληροφορίες σύνδεσης. Επίσης, μπορείτε να ελέγξετε τυχόν επείγουσες ειδοποιήσεις απευθείας στους ηλεκτρονικούς λογαριασμούς σας ή καλώντας μια καθορισμένη τηλεφωνική γραμμή βοήθειας.

4. Δεν πρέπει να χρησιμοποιούνται σύνδεσμοι μηνυμάτων και στοιχεία επικοινωνίας. Με μηνύματα που σας προκαλούν ανησυχία, αποφύγετε τη χρήση συνδέσμων ή στοιχείων επικοινωνίας. Όπου είναι δυνατόν, χρησιμοποιήστε τους επίσημους διαύλους επικοινωνίας.

5. Επαληθεύστε τον αριθμό τηλεφώνου. Ασυνήθιστα εμφανιζόμενοι τηλεφωνικοί αριθμοί, όπως αυτοί με τέσσερα ψηφία, μπορεί να υποδηλώνουν τη χρήση υπηρεσιών μεταβίβασης μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου. Αυτή είναι μία από τις διάφορες στρατηγικές που μπορεί να χρησιμοποιήσει ένας απατεώνας για να αποκρύψει τον πραγματικό του αριθμό τηλεφώνου.

6. Αποφασίστε να μην αποθηκεύετε ποτέ πληροφορίες πιστωτικών καρτών στο τηλέφωνό σας. Το να μην αποθηκεύετε ποτέ οικονομικές πληροφορίες σε ένα ψηφιακό πορτοφόλι είναι η μεγαλύτερη προσέγγιση για να αποτρέψετε την αρπαγή τους.

7. Χρησιμοποιείται έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA). Ένας επιτιθέμενος που επιτίθεται με smishing ενδέχεται να μην είναι σε θέση να αποκτήσει πρόσβαση σε έναν εκτεθειμένο κωδικό πρόσβασης, εάν ο λογαριασμός που έχει παραβιαστεί χρειάζεται ένα δεύτερο "κλειδί" για επαλήθευση. Ο έλεγχος ταυτότητας δύο παραγόντων (2FA), η πιο δημοφιλής παραλλαγή MFA, χρησιμοποιεί συχνά έναν κωδικό επαλήθευσης μέσω μηνύματος κειμένου. Υπάρχουν ισχυρότερες εναλλακτικές λύσεις, όπως η χρήση μιας συγκεκριμένης εφαρμογής για επαλήθευση (όπως το Google Authenticator).

8. Ποτέ μην στέλνετε μήνυμα σε κάποιον τον κωδικό πρόσβασης ή τον κωδικό ανάκτησης λογαριασμού σας. Τόσο οι κωδικοί πρόσβασης όσο και οι κωδικοί ανάκτησης για τον έλεγχο ταυτότητας δύο παραγόντων (2FA) που αποστέλλονται με μήνυμα κειμένου θέτουν τον λογαριασμό σας σε κίνδυνο εάν πέσουν σε λάθος χέρια. Χρησιμοποιήστε αυτές τις πληροφορίες αποκλειστικά σε επίσημους ιστότοπους και μην τις αποκαλύπτετε ποτέ σε κανέναν.

9. Εγκαταστήστε μια εφαρμογή ανίχνευσης κακόβουλου λογισμικού. Εργαλεία όπως το Kaspersky Internet Security for Android βοηθούν στην προστασία από διευθύνσεις URL phishing σε μηνύματα SMS καθώς και από επιβλαβείς εφαρμογές.

10. Αναφέρετε όλες τις απόπειρες ηλεκτρονικού "ψαρέματος" μέσω SMS στις αρμόδιες αρχές.

3.4 Τι να κάνετε αν πέσετε θύμα Smishing

Πρέπει να έχετε μια στρατηγική ανάκτησης, διότι οι επιθέσεις smishing είναι πανούργες και μπορεί να σας έχουν ήδη θυματοποιήσει.

Λάβετε τα παρακάτω κρίσιμα μέτρα για να μειώσετε τις επιπτώσεις μιας επιτυχημένης απόπειρας smishing:

1. Ενημερώστε τυχόν ιδρύματα που μπορούν να σας βοηθήσουν σχετικά με την υποτιθέμενη επίθεση.

2. Για να σταματήσετε την τρέχουσα ή μελλοντική απάτη ταυτότητας, παγώστε την πίστωσή σας.

3. Όπου είναι δυνατόν, αλλάξτε τους κωδικούς PIN των λογαριασμών σας και τυχόν κωδικούς πρόσβασης.

4. Προσέχετε περίεργες τοποθεσίες σύνδεσης και άλλες ενέργειες κατά τον έλεγχο των τραπεζικών, πιστωτικών και διαφόρων λογαριασμών σας στο διαδίκτυο.

4. Ομοιότητες μεταξύ Vishing, Phishing και Smishing

Το smishing, το phishing και το vishing είναι όλοι διαφορετικοί τύποι κυβερνοεπιθέσεων που χρησιμοποιούν τεχνικές κοινωνικής μηχανικής για να κλέψουν προσωπικές πληροφορίες, διαπιστευτήρια ή χρήματα από τα θύματα. Ακολουθούν μερικές από τις ομοιότητες μεταξύ αυτών των τριών τύπων επιθέσεων:

1. Τεχνικές κοινωνικής μηχανικής: Και οι τρεις τύποι επιθέσεων χρησιμοποιούν τεχνικές κοινωνικής μηχανικής για να εξαπατήσουν το θύμα ώστε να αποκαλύψει ευαίσθητες πληροφορίες ή να προβεί σε κάποια ενέργεια που μπορεί να θέσει σε κίνδυνο την ασφάλειά του.

2. Χρήση ηλεκτρονικής επικοινωνίας: Και οι τρεις τύποι επιθέσεων χρησιμοποιούν μεθόδους ηλεκτρονικής επικοινωνίας για να προσεγγίσουν το θύμα. Το smishing χρησιμοποιεί μηνύματα κειμένου, το phishing χρησιμοποιεί μηνύματα ηλεκτρονικού ταχυδρομείου και το vishing χρησιμοποιεί τηλεφωνήματα.

3. Στόχος της κλοπής προσωπικών πληροφοριών: Ο απώτερος στόχος και των τριών επιθέσεων είναι η κλοπή προσωπικών πληροφοριών, όπως διαπιστευτήρια σύνδεσης, στοιχεία πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες.

4. Προσποίηση (Pretexting): Οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν ένα πρόσχημα ή μια ψεύτικη ιστορία για να δελεάσουν το θύμα να παράσχει τις πληροφορίες που αναζητούν.

5. Μιμητισμός: Οι επιτιθέμενοι μπορεί να υποδυθούν μια έμπιστη οντότητα, όπως μια τράπεζα, μια κυβερνητική υπηρεσία ή μια εταιρεία, για να κερδίσουν την εμπιστοσύνη του θύματος.

6. Χρήση επείγοντος ή φόβου: Οι επιτιθέμενοι μπορεί να δημιουργήσουν μια αίσθηση επείγοντος ή φόβου για να πείσουν το θύμα να προβεί σε άμεση ενέργεια, όπως να κάνει κλικ σε έναν σύνδεσμο, να κατεβάσει ένα αρχείο ή να παράσχει ευαίσθητες πληροφορίες.

7. Εκλέπτυνση: Αυτές οι επιθέσεις γίνονται όλο και πιο εξελιγμένες και δύσκολα ανιχνεύσιμες, καθώς οι επιτιθέμενοι χρησιμοποιούν προηγμένες τακτικές και εργαλεία για να παρακάμψουν τα μέτρα ασφαλείας και να στοχεύσουν συγκεκριμένα άτομα ή οργανισμούς.

8. Είναι σημαντικό να παραμείνετε σε εγρήγορση και να είστε προσεκτικοί σε κάθε επικοινωνία που σας φαίνεται ύποπτη ή απαιτεί να προβείτε σε επείγουσες ενέργειες. Πάντα να επαληθεύετε τη νομιμότητα του αιτήματος προτού παρέχετε ευαίσθητες πληροφορίες ή προβείτε σε οποιαδήποτε ενέργεια.

5. Διαφορές μεταξύ Vishing, Phishing και Smishing

Το smishing, το phishing και το vishing είναι όλοι διαφορετικοί τύποι επιθέσεων στον κυβερνοχώρο που χρησιμοποιούν διαφορετικά κανάλια επικοινωνίας για να εξαπατήσουν τους ανθρώπους ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, πληροφορίες τραπεζικών λογαριασμών και προσωπικούς αριθμούς αναγνώρισης (PIN). Ακολουθούν οι διαφορές τους:

1. Smishing: Το Smishing είναι ένας τύπος επίθεσης phishing που χρησιμοποιεί μηνύματα κειμένου (SMS) ή υπηρεσίες άμεσων μηνυμάτων (όπως το WhatsApp) για να εξαπατήσει τους ανθρώπους ώστε να κάνουν κλικ σε έναν κακόβουλο σύνδεσμο ή να κατεβάσουν μια επιβλαβή εφαρμογή. Η ονομασία "smishing" προέρχεται από τον συνδυασμό των λέξεων "SMS" και "phishing".

2. Phishing: Το phishing είναι ένας τύπος επίθεσης στον κυβερνοχώρο που χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο, τα μέσα κοινωνικής δικτύωσης ή άλλες πλατφόρμες ανταλλαγής μηνυμάτων για να εξαπατήσει τους ανθρώπους ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να κάνουν κλικ σε έναν σύνδεσμο που κατεβάζει κακόβουλο λογισμικό ή άλλο κακόβουλο λογισμικό. Ο επιτιθέμενος μπορεί να μεταμφιέσει το μήνυμα ώστε να φαίνεται ότι προέρχεται από μια αξιόπιστη πηγή, όπως μια τράπεζα ή μια εταιρεία μέσων κοινωνικής δικτύωσης.

3. Vishing: Το Vishing (φωνητικό ψάρεμα) είναι ένας τύπος επίθεσης phishing που χρησιμοποιεί τη φωνητική επικοινωνία για να εξαπατήσει τους ανθρώπους ώστε να δώσουν ευαίσθητες πληροφορίες. Ο επιτιθέμενος μπορεί να καλέσει ένα θύμα στο τηλέφωνο και να προσποιηθεί ότι προέρχεται από έναν αξιόπιστο οργανισμό, όπως μια τράπεζα, μια κυβερνητική υπηρεσία ή μια υπηρεσία υποστήριξης πληροφορικής, και να προσπαθήσει να λάβει προσωπικές πληροφορίες, όπως έναν αριθμό κοινωνικής ασφάλισης ή έναν αριθμό τραπεζικού λογαριασμού.

4. Συνοπτικά, η κύρια διαφορά μεταξύ αυτών των τριών επιθέσεων είναι το κανάλι που χρησιμοποιείται για την παράδοση του κακόβουλου περιεχομένου, με το smishing να χρησιμοποιεί SMS, το phishing να χρησιμοποιεί ηλεκτρονικό ταχυδρομείο ή υπηρεσίες ανταλλαγής μηνυμάτων και το vishing να χρησιμοποιεί φωνητική επικοινωνία μέσω τηλεφώνου.

Βιβλιογραφία

https://us.norton.com/blog/online-scams/vishing

https://coolweb.gr/phising-ti-einai-prostasia/

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it