CYPRUS COMPUTER SOCIETY

CYPRUS COMPUTER SOCIETY

ΣΥΜΒΟΥΛΕΣ ΠΡΟΣΤΑΣΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΑΠΡΙΛΙΟΣ 2023

P.O.BOX 27038 : 1641 NICOSIA : CYPRUS : **TEL**: +357 22460680 : **FAX**: +357 22767349
e-mail: info@ccs.org.cy : **Web**: www.ccs.org.cy

ΣΥΜΒΟΥΛΕΣ ΠΡΟΣΤΑΣΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ!!

Εισαγωγή

Είναι γνωστό σε όλους ότι οι προσπάθειες εξαπάτησης του κοινού στον κυβερνοχώρο έχουν γίνει μια καθημερινή απειλή τόσο για άτομα όσο και για οργανισμούς. Αυτές έχουν σαν στόχο να κλέψουν ευαίσθητες πληροφορίες, να παραβιάσουν την ασφάλεια συστημάτων και να εξαπατήσουν τα θύματα για να αποσπάσουν κατά κύριο λόγο χρήματα.

Οι απατεώνες επινοούν ολοένα και πιο ευρηματικά και περίπλοκα σχέδια και προσεγγίσεις για να εξαπατήσουν και να επωφεληθούν από ανυποψίαστα θύματα στοχεύοντας εκμεταλλευτούν την άγνοια, τους φόβους, τις ανασφάλειες αλλά και την απληστία των ανθρώπων. Τέτοιες προσεγγίσεις αποτελούνται από ψεύτικα email που ισχυρίζονται ότι προέρχονται από διάφορες αρχές και οργανισμούς μέχρι ψεύτικους ιστότοπους διαδικτυακών αγορών που προσφέρουν διάφορα προϊόντα, μέχρι απίστευτα καλές επενδυτικές ευκαιρίες ή προτάσεις για εργοδότηση. Επίσης πιθανό να προσεγγίσουν υποψήφια θύματα τηλεφωνικά όπου με διάφορες αληθοφανείς προφάσεις προσπαθούν να τα εξαπατήσουν.

Με την κατανόηση των τακτικών που χρησιμοποιούν οι απατεώνες, όπως όπως phishing, κοινωνική μηχανική και κακόβουλο λογισμικό, με την εξοικείωση μας με τις κοινές κόκκινες σημαίες και με την υιοθέτηση καλών πρακτικών κυβερνοασφάλειας, όπως η χρήση ισχυρών κωδικών πρόσβασης, η ενημέρωση του λογισμικού και η αποφυγή ύποπτων συνδέσμων και συνημμένων, μπορούμε να μειώσουμε σημαντικά τον κίνδυνο να πέσουμε θύματα.

Σημείωση: Στο τέλος αυτού του κειμένου υπάρχει μια σύντομη επεξήγηση διαφόρων όρων που χρησιμοποιούνται. Πιθανό να σας είναι χρήσιμο να διαβάσετε πρώτα αυτές τις επεξηγήσεις πριν συνεχίσετε.

Τι πρέπει να έχουμε υπόψη

Για καλύτερη προστασία μας θα ήταν καλό, ως άτομα, να έχουμε υπόψη τα πιο κάτω τα οποία πρέπει να συνδυάζουμε όποτε είμαστε σε αμφιβολία για την αυθεντικότητα κάποιου μηνύματος:

Αναγνώριση κακόβουλων μηνυμάτων: Πρέπει πάντα να είμαστε προσεκτικοί και να προσπαθούμε να αναγνωρίζουμε τα ανεπιθύμητα μηνύματα. Πρέπει να έχουμε συνέχεια στο μυαλό μας ότι οι απατεώνες στέλνουν συχνά ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που μοιάζουν σαν να προέρχονται από νόμιμη πηγή. Μπορεί να ισχυρίζονται ότι είναι χρηματοπιστωτικό ίδρυμα, κρατική υπηρεσία ή εταιρεία με την οποία συνεργάζεστε. Για να διαπιστώσετε κατά πόσο μήνυμα είναι νόμιμο ή όχι, αναζητήστε τυχόν ορθογραφικά ή γραμματικά λάθη στο μήνυμα. Οι νόμιμοι οργανισμοί έχουν συνήθως επαγγελματική επικοινωνία και δεν κάνουν τέτοιου είδους λάθη. Βέβαια και οι απατεώνες εξελίσσονται και στέλνουν μηνύματα που δεν διαφέρουν και πολύ από το λεκτικό που χρησιμοποιούν οι

νόμιμοι οργανισμοί. Επίσης υπάρχουν και τα παλιά κόλπα όπου σας πληροφορούν ότι ένα μεγάλο ποσό (λαχείο, κληρονομιά κλπ κλπ), είναι κάπου και περιμένει εσάς να το πάρετε!!!

Επαληθεύστε την πηγή του μηνύματος: Πριν κάνετε κλικ σε οποιονδήποτε σύνδεσμο ή ανοίξετε ένα συνημμένο, επαληθεύστε ΠΟΛΥ ΠΡΟΣΕΚΤΙΚΑ τη διεύθυνση email του αποστολέα ή το προφίλ των μέσων κοινωνικής δικτύωσης. Οι απατεώνες χρησιμοποιούν συχνά παραποιημένες διευθύνσεις email ή προφίλ που μοιάζουν σαν να προέρχονται από νόμιμη πηγή. Ελέγξτε τον σύνδεσμο προς τον ιστότοπο που σας προτρέπουν να πάτε ή του προφίλ για να δείτε εάν σχετίζεται με τον οργανισμό από τον οποίο ισχυρίζεται ότι είναι ο αποστολέας.

Μην κάνετε κλικ σε ύποπτους συνδέσμους ή συνημμένα: Οι απατεώνες χρησιμοποιούν συχνά συνδέσμους με σκοπό το ψάρεμα (phishing) ή συνημμένα για να εξαπατήσουν τους χρήστες να κατεβάσουν κακόβουλο λογισμικό ή να εισαγάγουν προσωπικές πληροφορίες. Αναζητήστε τυχόν σημάδια ότι ο σύνδεσμος ή το συνημμένο μπορεί να είναι ύποπτα, όπως ένα άγνωστο domain, ορθογραφικά λάθη ή ένα γενικό μήνυμα αντί για εξατομικευμένο.

Μην δίνετε ΠΟΤΕ προσωπικά στοιχεία: Οι απατεώνες μπορεί να ζητήσουν προσωπικές πληροφορίες, όπως τον κωδικό πρόσβασής σας, τα στοιχεία της πιστωτικής σας κάρτας ή τον αριθμό ταυτότητας ή κοινωνικών ασφαλίσεων. Οι πραγματικοί οργανισμοί δεν θα ζητήσουν αυτές τις πληροφορίες μέσω email ή μέσων κοινωνικής δικτύωσης. Εάν λάβετε ένα μήνυμα που ζητά αυτές τις πληροφορίες, μην απαντήσετε και μην δώσετε καμία πληροφορία.

Κάνετε χρήση του ελέγχου ταυτότητας δύο παραγόντων: Ο έλεγχος ταυτότητας δύο παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας στους λογαριασμούς σας, απαιτώντας μια δεύτερη μορφή επαλήθευσης. Αυτό μπορεί να βοηθήσει στην προστασία από μη εξουσιοδοτημένη πρόσβαση στους λογαριασμούς σας. Αναζητήστε επιλογές ελέγχου ταυτότητας δύο παραγόντων στις ρυθμίσεις του λογαριασμού σας ή στον ιστότοπο των οργανισμών με τους οποίους συνεργάζεστε.

Να είστε προσεκτικοί με τις τηλεφωνικές κλήσεις: Οι απατεώνες μπορεί να καλέσουν και να ισχυριστούν ότι προέρχονται από έναν νόμιμο οργανισμό, όπως η τράπεζά σας ή μια κρατική υπηρεσία ή πάροχο τηλεπικοινωνιών. Πιθανόν να ζητήσουν προσωπικά στοιχεία ή να απειλήσουν με νομικές ενέργειες / συνέπειες εάν δεν συμμορφωθείτε. Για να διαπιστώσετε εάν η κλήση είναι νόμιμη, ρωτήστε τον καλούντα για το όνομά του και τον οργανισμό από τον οποίο καλεί. Αναζητήστε τον αριθμό τηλεφώνου του οργανισμού ανεξάρτητα και καλέστε ξανά για να επαληθεύσετε την ταυτότητα του καλούντος.

Εμπιστευτείτε το ένστικτό σας: Εάν κάτι σας φαίνεται πολύ καλό για να είναι αληθινό ή δεν είστε σίγουροι για τη νομιμότητα ενός μηνύματος ή κλήσης, εμπιστευτείτε το ένστικτό σας και γίνετε προσεκτικοί και δύσπιστοι. Κάντε ένα βήμα πίσω και αξιολογήστε την κατάσταση πριν προβείτε σε οποιαδήποτε ενέργεια.

Εάν δεν είστε βέβαιοι εάν ένα μήνυμα είναι νόμιμο ή όχι, επικοινωνήστε απευθείας με τον οργανισμό για να επαληθεύσετε το μήνυμα.

Να είστε επιφυλακτικοί και δύσπιστοι ως προς τα επείγοντα ή απειλητικά μηνύματα: Οι απατεώνες προσπαθούν συχνά να δημιουργήσουν μια αίσθηση επείγοντος ή φόβου για να σας πανικοβάλουν και να σας κάνουν να ενεργήσετε γρήγορα χωρίς να το σκεφτείτε. Για παράδειγμα, μπορεί να ισχυριστούν ότι ο λογαριασμός σας έχει παραβιαστεί και ότι πρέπει να λάβετε άμεσα μέτρα για να αποτρέψετε περαιτέρω ζημιές. Ή ακόμα ότι ένα αγαπημένο σας πρόσωπο έπαθε κάτι, δεν μπορεί να μιλήσει και έχει απόλυτη και άμεση ανάγκη βοήθειας, όπως ιατρική φροντίδα και χρειάζεται άμεσα χρήματα. Να είστε δύσπιστοι για οποιοδήποτε μήνυμα ή τηλεφώνημα που χρησιμοποιεί φόβο ή επείγουσα ανάγκη για να σας πιέσει να αναλάβετε άμεσα δράση.

Ψάξτε για ασυνέπειες στο μήνυμα: Οι απατεώνες συχνά κάνουν λάθη στα μηνύματά τους που μπορούν να αποκαλύψουν τις πραγματικές τους προθέσεις. Αναζητήστε ασυνέπειες στο μήνυμα, όπως ανορθόγραφες λέξεις ή λανθασμένη γραμματική, που μπορεί να υποδηλώνουν ότι το μήνυμα είναι δόλιο.

Ελέγξτε το πιστοποιητικό ασφαλείας του ιστότοπου: Όταν λαμβάνετε ένα μήνυμα που περιέχει έναν σύνδεσμο προς έναν ιστότοπο, ελέγξτε το πιστοποιητικό ασφαλείας του ιστότοπου για να βεβαιωθείτε ότι είναι νόμιμο. Αναζητήστε ένα εικονίδιο λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης ή μια διεύθυνση URL που ξεκινά με "https://" και όχι με "http://".

Να είστε προσεκτικοί με αιτήματα φίλων μέσων κοινωνικής δικτύωσης: Οι απατεώνες ενδέχεται να δημιουργήσουν ψεύτικα προφίλ και να στείλουν αιτήματα φιλίας για να αποκτήσουν πρόσβαση στα προσωπικά σας στοιχεία ή για να σας στείλουν δόλια μηνύματα. Να είστε προσεκτικοί με αιτήματα φιλίας από άτομα που δεν γνωρίζετε ή από άτομα που έχουν πολύ λίγους φίλους ή οπαδούς.

Ελέγξτε την εικόνα προφίλ του αποστολέα: Οι απατεώνες μπορούν να χρησιμοποιήσουν φωτογραφίες ή εικόνες ελκυστικών ατόμων ελεύθερα διαθέσιμες στο διαδίκτυο για να κάνουν τα ψεύτικα προφίλ τους να φαίνονται πιο αληθοφανή. Αναζητήστε τυχόν σημάδια ότι η φωτογραφία προφίλ μπορεί να είναι ψεύτικη, όπως εάν φαίνεται πολύ τέλεια ή αν είναι γνωστή φωτογραφία.

Να είστε προσεκτικοί με τις προσφορές εργασίας ή τις επενδυτικές ευκαιρίες: Οι απατεώνες μπορεί να στείλουν μηνύματα που προσφέρουν ευκαιρίες εργασίας ή επενδυτικές ευκαιρίες που φαίνονται πολύ καλές για να είναι αληθινές. Να είστε προσεκτικοί με οποιοδήποτε μήνυμα που υπόσχεται υψηλές αποδόσεις ή που απαιτεί από εσάς να κάνετε μια προκαταβολή. Κανόνας: Αν είναι πολύ καλό για να είναι αληθινό τότε ΔΕΝ είναι αληθινό!

Επαληθεύστε τις πληροφορίες απευθείας με τον οργανισμό: Εάν λάβετε ένα μήνυμα που ισχυρίζεται ότι προέρχεται από έναν οργανισμό, επαληθεύστε τις πληροφορίες απευθείας με τον οργανισμό. Αναζητήστε ανεξάρτητα τα στοιχεία επικοινωνίας του

οργανισμού και επικοινωνήστε μαζί τους για να επιβεβαιώσετε εάν το μήνυμα είναι νόμιμο.

Χρήση λογισμικού προστασίας από ιούς: Χρησιμοποιήστε λογισμικό προστασίας από ιούς στις συσκευές σας για προστασία από κακόβουλο λογισμικό και άλλες απειλές. Φροντίστε να διατηρείτε ενημερωμένο το λογισμικό προστασίας από ιούς για να διασφαλίσετε ότι είναι σε θέση να ανιχνεύει τις πιο πρόσφατες απειλές.

Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης: Χρησιμοποιήστε ισχυρούς**, μοναδικούς** κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς σας για να αποτρέψετε την πρόσβαση χάκερ στους λογαριασμούς σας. Βεβαιωθείτε ότι χρησιμοποιείτε συνδυασμό γραμμάτων, αριθμών και συμβόλων και αποφύγετε τη χρήση κοινών φράσεων ή προσωπικών πληροφοριών.

Ενημερωθείτε για τις κοινές απάτες: Ενημερωθείτε για τις κοινές απάτες και πώς να τις εντοπίσετε. Μείνετε ενημερωμένοι για τις πιο πρόσφατες τακτικές που χρησιμοποιούν οι απατεώνες και μάθετε πώς να προστατεύεστε από αυτές τις απειλές.

Ακολουθώντας αυτές τις συμβουλές, μπορείτε να συμβάλετε στην περαιτέρω προστασία σας από απάτες και να παραμείνετε ασφαλείς στο διαδίκτυο. Να θυμάστε, να είστε πάντα δύσπιστοι για τα αυτόκλητα μηνύματα και να αφιερώνετε χρόνο για να επαληθεύσετε την πηγή και τη νομιμότητα οποιουδήποτε μηνύματος λαμβάνετε.

Σημειώνεται ότι τα πιο πάνω δεν είναι ένας πλήρης κατάλογος συμβουλών με τη βοήθεια του οποίου θα είστε απόλυτα προστατευμένοι. Θα πρέπει να είστε συνεχώς σε εγρήγορση και να επιδιώκετε τη συνεχή ενημέρωση σας από αξιόπιστες πηγές και να προσαρμόζετε την άμυνα σας.

Σας ευχόμαστε μια ασφαλή και επωφελή παρουσία στον κυβερνοχώρο.

Όρος Έννοια / Επεξήγηση

Πιο κάτω είναι μια σύντομή επεξήγηση διαφόρων όρων που χρησιμοποιούνται στο πιο πάνω κείμενο.

Ψάρεμα (phishing) Ένας τύπος απάτης όπου ένας εισβολέας παρουσιάζεται ως αξιόπιστη οντότητα προκειμένου να αποκτήσει ευαίσθητες πληροφορίες όπως ονόματα χρήστη, κωδικούς πρόσβασης και στοιχεία πιστωτικής κάρτας.

Κακόβουλο λογισμικό Ένας τύπος λογισμικού που έχει σχεδιαστεί για να βλάπτει, να διακόπτει ή να αποκτά μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή ή ένα δίκτυο.

Κοινωνική μηχανική Η χρήση ψυχολογικής χειραγώγησης για να εξαπατήσει τους ανθρώπους να αποκαλύψουν εμπιστευτικές πληροφορίες ή να πραγματοποιήσουν ενέργειες που δεν είναι προς το συμφέρον τους.

Spoofing Η πράξη της συγκάλυψης μιας επικοινωνίας από άγνωστη πηγή για να φαίνεται ότι προέρχεται από γνωστή, αξιόπιστη πηγή, προκειμένου να εξαπατηθεί ένας παραλήπτης να παραιτηθεί από ευαίσθητες πληροφορίες.

Έλεγχος ταυτότητας δύο παραγόντων Ένα μέτρο ασφαλείας που απαιτεί από τους χρήστες να παρέχουν δύο διαφορετικούς τύπους παραγόντων ελέγχου ταυτότητας, όπως έναν κωδικό πρόσβασης και έναν κωδικό επαλήθευσης που αποστέλλεται στο τηλέφωνό τους, για πρόσβαση σε έναν λογαριασμό.

Κρυπτογράφηση Η διαδικασία μετατροπής δεδομένων σε κωδικοποιημένη γλώσσα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή παραβίασης.

Τείχος προστασίας (Firewall) Ένα σύστημα ασφαλείας που βασίζεται σε λογισμικό ή υλικό που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία δικτύου με βάση προκαθορισμένους κανόνες ασφαλείας.

Μήνυμα Ηλεκτρονικού ταχυδρομείου με σκοπό το ψάρεμα (phishing email) Ένα δόλιο email που έχει σχεδιαστεί για να εξαπατήσει τους παραλήπτες να αποκαλύψουν ευαίσθητες πληροφορίες ή να κάνουν κλικ σε έναν κακόβουλο σύνδεσμο.

Απάτη μέσα από μέσα κοινωνικής δικτύωσης: (Social media scam) Ένας τύπος απάτης που στοχεύει χρήστες πλατφορμών μέσων κοινωνικής δικτύωσης, συχνά παριστάνοντας τους φίλους ή γνωστό γνωστού ή διάσημου και στέλνοντας δόλια μηνύματα ή συνδέσμους.

Λογισμικό προστασίας από ιούς:(Anti-virus software) Λογισμικό σχεδιασμένο για τον εντοπισμό, την πρόληψη και την αφαίρεση κακόβουλου λογισμικού (κακόβουλο λογισμικό) από ένα σύστημα υπολογιστή.