17 Οκτωβρίου 2018

ΔΕΛΤΙΟ ΤΥΠΟΥ

Πατήστε εδώ και δείτε τα χρήματα σας να εξαφανίζονται- εγκληματικά #CyberScams του 21ου αιώνα

Η Europol και η Ευρωπαϊκή Τραπεζική Ομοσπονδία ξεκινούν εκστρατεία ενημέρωσης και ευαισθητοποίησης για τις 7 συχνότερες διαδικτυακές οικονομικές απάτες

Βρυξέλλες / Χάγη - Το Ευρωπαϊκό Κέντρο Καταπολέμησης Κυβερνοεγκλημάτων (EC3) της Europol, η Ευρωπαϊκή Τραπεζική Ομοσπονδία και οι συνεργάτες τους από τον δημόσιο και τον ιδιωτικό τομέα εγκαινιάζουν σήμερα την εκστρατεία ευαισθητοποίησης #CyberScams στο πλαίσιο του Ευρωπαϊκού Μήνα Ασφάλειας στον κυβερνοχώρο.

Κατά τη διάρκεια της εβδομάδας που ξεκινά από σήμερα, 17 Οκτωβρίου 2018, οι αρμόδιες αρχές επιβολής του νόμου από τα **28 κράτη μέλη της ΕΕ, 5 κράτη μέλη εκτός ΕΕ[1], 24 εθνικές τραπεζικές ενώσεις** και τράπεζες και πολλοί άλλοι φορείς καταπολέμησης της εγκληματικότητας στον κυβερνοχώρο θα αυξήσουν την ευαισθητοποίηση όλων σχετικά με αυτό το εγκληματικό φαινόμενο. Αυτή η πανευρωπαϊκή προσπάθεια θα υλοποιηθεί μέσω μιας επικοινωνιακής εκστρατείας, την αξιοποίηση των μέσων κοινωνικής δικτύωσης, των εθνικών αρμόδιων αρχών επιβολής του νόμου, των τραπεζικών ενώσεων και των χρηματοπιστωτικών ιδρυμάτων.

Σύμφωνα με τις συστάσεις του IOCTA 2018, η αποτελεσματικότερη άμυνα κατά της κοινωνικής μηχανικής (social engineering) είναι η εκπαίδευση των δυνητικών θυμάτων - που μπορεί να είναι οποιοσδήποτε από εμάς όταν χρησιμοποιούμε το διαδίκτυο. Η ευαισθητοποίηση του κοινού σχετικά με τον τρόπο εντοπισμού τέτοιων τεχνικών εξαπάτησης θα βοηθήσει να παραμείνουν τόσο οι ίδιοι όσο και τα οικονομικά τους ασφαλή κατά την περιήγησή τους στο διαδίκτυο.

Για αυτήν την εκστρατεία, το υλικό ευαισθητοποίησης συντάχθηκε **σε 27 γλώσσες**, διαθέσιμες στην ακόλουθη ηλεκτρονική διεύθυνση της Europol και περιλαμβάνει πληροφορίες σχετικά με τις 7 συνηθέστερες περιπτώσεις ηλεκτρονικής απάτης και πώς μπορούν αυτές να αποφευχθούν:

- **Απάτη CEO**: οι απατεώνες (scammers) προσποιούνται ότι είναι ο Διευθύνων Σύμβουλος ή κάποιος προϊστάμενος στον οργανισμό σας και σας παρασύρουν να πληρώσετε ένα ψεύτικο τιμολόγιο ή να πραγματοποιήσετε μια μη εξουσιοδοτημένη μεταφορά ποσού από τον εταιρικό λογαριασμό.
- **Απάτη τιμολογίων**: προσποιούνται ότι είναι ένας από τους πελάτες / προμηθευτές σας και σας παρασύρουν να πληρώσετε μελλοντικά τιμολόγια σε διαφορετικό τραπεζικό λογαριασμό.
- **Απάτη με e-mails/sms/τηλεφωνικές κλήσεις**: σας τηλεφωνούν, σας στέλνουν ένα μήνυμα κειμένου (sms) ή ένα μήνυμα ηλεκτρονικού

[1] Ελβετία, Κολομβία, Λιχτενστάιν, Νορβηγία και Ουκρανία.

ταχυδρομείου για να σας παρασύρουν να μοιραστείτε τις προσωπικές και οικονομικές σας πληροφορίες ή τους κωδικούς ασφαλείας σας (User name, Password, PIN, κ.λπ).

- **Απατηλές ιστοσελίδες τράπεζας**: χρησιμοποιούν μηνύματα με σύνδεσμο (link) προς τον πλαστογραφημένο ιστότοπο. Αφού κάνετε κλικ στον σύνδεσμο, χρησιμοποιούνται διάφορες μέθοδοι για τη συλλογή των οικονομικών και προσωπικών σας πληροφοριών. Ο ιστότοπος θα μοιάζει με τον επίσημο ιστότοπο της τράπεζάς σας, με μικρές ωστόσο διαφορές.
- **Απάτη μέσω διαδικτυακών ραντεβού**: προσποιούνται ότι ενδιαφέρονται για μια ρομαντική σχέση. Συνήθως λαμβάνει χώρα σε ιστοσελίδες γνωριμιών, αλλά οι απατεώνες χρησιμοποιούν συχνά τα μέσα κοινωνικής δικτύωσης ή το ηλεκτρονικό ταχυδρομείο για να έρθουν σε επαφή με το υποψήφιο θύμα τους.
- **Κλοπή προσωπικών δεδομένων**: συλλέγουν τα προσωπικά σας δεδομένα μέσω των καναλιών κοινωνικής δικτύωσης.
- **Απάτες επενδύσεων και ηλεκτρονικών αγορών:** σας κάνουν να νομίζετε ότι σας παρουσιάζεται μια έξυπνη επένδυση ... ή σας παρουσιάζουν μια ψεύτικη προσφορά μέσω διαδικτύου.

Το Διαδίκτυο έχει γίνει πολύ ελκυστικό για τους εγκληματίες του κυβερνοχώρου. Οι επιτιθέμενοι χρησιμοποιούν εξελιγμένα τεχνάσματα και υποσχέσεις για να αποσπάσουν χρήματα ή πολύτιμες οικονομικές πληροφορίες από εσάς. Οι απάτες που χρησιμοποιούν έναν απολεσθέντα συγγενή ή κάποιον Νιγηριανό πρίγκιπα τους οποίους έχετε κληρονομήσει, δεν είναι πλέον τα μόνα διαθέσιμα κόλπα εξαπάτησης. Οι τακτικές που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου γίνονται όλο και πιο πρωτότυπες και δυσκολότερο να εντοπιστούν. Από το να προσποιούνται ότι είναι ο Διευθύνων Σύμβουλος του οργανισμού σας μέχρι το να εκδηλώνουν ρομαντικό ενδιαφέρον, οι σημερινοί διαδικτυακοί απατεώνες θα κάνουν ό,τι χρειάζεται για να πάρουν αυτό που θέλουν - τα χρήματά σας και / ή τα τραπεζικά σας στοιχεία (λογαριασμούς, κωδικούς ασφαλείας, αριθμούς καρτών, κ.λπ).

Όπως επισημάνθηκε στην Εκτίμηση της Απειλής του Οργανωμένου Διαδικτυακού Εγκλήματος (IOCTA) 2018, η κοινωνική μηχανική συνεχίζει να αναπτύσσεται ως η κινητήρια δύναμη πολλών εγκλημάτων στον κυβερνοχώρο, με το phishing (μηνύματα ηλεκτρονικού ταχυδρομείου / e-mails) να έχει τη συχνότερη χρήση. Οι εγκληματίες χρησιμοποιούν την κοινωνική μηχανική για να επιτύχουν μια σειρά στόχων: να αποκτήσουν τα προσωπικά σας δεδομένα, να αποκτήσουν πρόσβαση στους λογαριασμούς σας, να κλέψουν την ταυτότητά σας, να ξεκινήσουν παράνομες πληρωμές ή να σας πείσουν να προχωρήσετε σε οποιαδήποτε άλλη δραστηριότητα ενάντια στο δικό σας συμφέρον, όπως η μεταφορά χρημάτων ή η διακίνηση προσωπικών δεδομένων. Ένα μόνο κλικ μπορεί να είναι αρκετό για να υπονομεύσει ολόκληρο τον οργανισμό σας ή και εσάς προσωπικά.

Διαβάστε περισσότερα σχετικά με το πώς μπορείτε να παραμείνετε προστατευμένοι στην ειδική ιστοσελίδα #CyberScams. Ο Ευρωπαϊκός Μήνας Ασφάλειας στον κυβερνοχώρο (ECMS) είναι μια εκστρατεία ευαισθητοποίησης της ΕΕ που προάγει την ασφάλεια στον κυβερνοχώρο μεταξύ πολιτών και οργανισμών, επισημαίνοντας απλά βήματα που μπορούν να ληφθούν για την προστασία των προσωπικών, οικονομικών και επαγγελματικών δεδομένων τους.

Ακολουθήστε την εκστρατεία **#CyberScams**:

Europol και EC3 Twitter, Facebook, Instagram, Youtube και LinkedIn
EBF Twitter, Facebook και Linkedin