Σιούφας και Συνεργάτες
Δικηγορική Εταιρεία

ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ - PHISHING

Η μεγάλη αύξηση της χρήσης ψηφιακών εφαρμογών και υπηρεσιών σε συνδυασμό με την τεράστια έξαρση των κρουσμάτων ηλεκτρονικής απάτης και ιδιαίτερα με τη χρήση τεχνικών ηλεκτρονικού ψαρέματος «phishing[1]», με τις οποίες σκοπείται κυρίως **η απόσπαση απόρρητων προσωπικών και οικονομικών δεδομένων ή κωδικών ασφαλείας** για τη πραγματοποίηση οικονομικών συναλλαγών μη εξουσιοδοτημένων με αποτέλεσμα την πρόκληση οικονομικής ζημίας, κατόπιν και της δημοσίευσης την 17.04.2019 της **2019/713 Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης** σχετικά με την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών, αλλά και του από 11.11.2020 ενημερωτικού **Δελτίου Τύπου της Διεύθυνσης Δίωξης ηλεκτρονικού εγκλήματος**, οδήγησε **το Υπουργείο Προστασίας του Πολίτη, στο από 3 Φεβρουαρίου 2022 Δελτίο Τύπου** με το οποίο αξιολογήθηκαν τα μέχρι σήμερα υφιστάμενα

[1] Ο όρος **"phishing**" που αποτελεί μορφή διαδικτυακής εξαπάτησης χρησιμοποιήθηκε για πρώτη φορά το 1987 από τους Jerry Felix και Chris Hauck στην εργασία τους «Security System:A hacker's perspective», όπου αναλύθηκε η τεχνική εισβολέα που μιμείται αξιόπιστη οντότητα ή υπηρεσία. Ο όρος είναι **ομόηχος της λέξης fishing, καθώς χρησιμοποιείται η λογική του δολώματος-αλίευσης,** ενώ το «ph» προέρχεται από **την αναφορά στους phreaks,** ομάδα hackers, που διερεύνησαν παράνομα τηλεπικοινωνιακά συστήματα στη δεκαετία του 1990.

μέτρα, ενώ αποφασίστηκαν και τα επόμενα βήματα προς ελαχιστοποίηση και ορθή αντιμετώπιση των σχετικών κινδύνων.

- **ΕΝΝΟΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΨΑΡΕΜΑΤΟΣ-PHISHING**

Αποτελεί μορφή σύγχρονης διαδικτυακής απάτης μέσω κυρίως μηνυμάτων ηλεκτρονικού ταχυδρομείου (ή και άλλης μορφής ηλεκτρονικής υπηρεσίας) που αποστέλλονται μαζικά προς τους χρήστες σε ένα (παραποιημένο) γνωστό προς τους χρήστες ηλεκτρονικό περιβάλλον (όπως π.χ. τράπεζας ή άλλου φορέα ή υπηρεσίας) με σκοπό **την υποκλοπή δεδομένων προσωπικού χαρακτήρα** (π.χ. τραπεζικών λογαριασμών, πιστωτικών/χρεωστικών καρτών, κωδικών πρόσβασης) **και την επιδίωξη παράνομου οικονομικού κέρδους**.

- **ΤΕΧΝΙΚΕΣ**

SIM SWAPPING. Τεχνική με την οποία άγνωστοι προσπαθούν να εξαπατήσουν παρόχους κινητής τηλεφωνίας για να αποκτήσουν νέα κάρτα SIM- προς αντικατάσταση αυτής που ήδη έχει ο νόμιμος κάτοχος- με την ενεργοποίηση της οποίας μπορεί να λαμβάνει κλήσεις και μηνύματα του κατόχου προς εκτέλεση παράνομων δραστηριοτήτων.

SMISHING. Αποστολή ψεύτικων γραπτών μηνυμάτων SMS σε κινητά τηλέφωνα υποψηφίων θυμάτων προς εκτέλεση παράνομων εντολών.

VISHING. Τεχνική παραπλάνησης μέσω τηλεφωνικής κλήσης (voice phishing). Συχνή η εξαπάτηση μέσω υποτιθέμενης επιδιόρθωσης συσκευής (π.χ. ηλεκτρονικού υπολογιστή, smartphone) του θύματος από (γνωστή) εταιρεία Πληροφορικής, εγκαθιστώντας σε αυτή εφαρμογές που τους δίνουν τον έλεγχο της συσκευής για να υποκλέψουν προσωπικά δεδομένα.

PHARMING. Τεχνική με την οποία οι hackers ή κάποιο malware που έχει εγκατασταθεί στον υπολογιστή του θύματος μέσω του browser τον κατευθύνει σε κάποια εικονική ιστοσελίδα.

SPEAR PHISHING. Προηγμένη τεχνική με την οποία φαινομενικά αυθεντικά μηνύματα ηλεκτρονικού ταχυδρομείου καταφτάνουν στα εισερχόμενα μηνύματα συγκεκριμένων ομάδων ή μεμονωμένων ατόμων – ο εντοπισμός του δόλιου χαρακτήρα των οποίων είναι εξαιρετικά δύσκολος- που πολλές φορές περιέχουν links που οδηγούν σε ιστοσελίδες προς συμπλήρωση στοιχείων σε λογαριασμούς online.

WHALING. Τεχνική που απευθύνεται σε μεγάλους στόχους (π.χ. πολιτικούς).

CLONE PHISING. Εξελιγμένη τεχνική παρεμβολής στην πραγματική αλληλογραφία με την οποία ο εισβολέας κλωνοποιεί από μία αξιόπιστη πηγή ένα νόμιμο ηλεκτρονικό μήνυμα, το οποίο φαίνεται να αποτελεί συνέχεια της συνομιλίας του, αλλά ενδέχεται να περιέχει κακόβουλο σύνδεσμο.

➢ **ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ**

- **Ελέγχουμε το όνομα του αποστολέα και κυρίως την κατάληξη του domain** και εφόσον η κατάληξη δεν είναι γνωστή ή δεν υπάρχει σε μηχανή αναζήτησης τότε είναι πιθανότατα κακόβουλη.
- **Παρατηρούμε προσεκτικά το θέμα του μηνύματος**, καθώς συχνά οι επιτήδειοι χρησιμοποιούν παραπλανητικούς τίτλους (π.χ. δήθεν οφειλή μας, ύπαρξη ιού στο λογισμικό του υπολογιστή μας, δήθεν κληρονομιά ή κατάθεση μεγάλου ποσού)
- **Ελέγχουμε πάντα τον τρόπο γραφής, την ορθογραφία του κειμένου και του email**
- **Δεν ανοίγουμε τους προτεινόμενους συνδέσμους που επισυνάπτουν, δεν απαντούμε σε μηνύματα τέτοιου περιεχομένου, δεν καταχωρούμε και δεν στέλνουμε προσωπικά δεδομένα και στοιχεία προσωπικών καρτών,** καθώς καμία Τράπεζα ή εταιρεία δεν ζητά προσωπικά στοιχεία μέσω mail ή τηλεφώνου.
- **Διαγράφουμε το επικίνδυνο μήνυμα, ώστε να αποφευχθεί μελλοντικός κίνδυνος.**
- **Καταγγέλλουμε αμέσως πατώντας «αναφορά» και στις περιπτώσεις που αποστολέας είναι κάποια Τράπεζα, την ενημερώνουμε ώστε να λάβει τα απαραίτητα μέτρα για την προστασία των χρηστών[2].**

➢ **ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΜΕΤΡΩΝ ΑΠΟ ΤΟ ΥΠΟΥΡΓΕΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ**

- Η συνεχής ενημέρωση του κοινού τους επόμενους μήνες με νέο τηλεοπτικό και ραδιοφωνικό ενημερωτικό υλικό
- Η θέσπιση θεσμικών και νομοθετικών μέτρων ώστε οι τράπεζες να έχουν τον αναγκαίο χρόνο απόκρισης και τα πρόσφορα μέτρα για βοήθεια σε θύματα απάτης.
- Η εντατικοποίηση της συνεργασίας Χρηματοπιστωτικών Ιδρυμάτων και Αρχών επιβολής του νόμου (πχ Αστυνομία, Ευρωπαϊκές Δικαστικές Αρχές)

**Σημειώνεται πως σύμφωνα με την ανωτέρω ευρωπαϊκή Οδηγία 2019/713 συστήνεται στα κράτη μέλη να λαμβάνουν τα αναγκαία μέτρα για την απάτη που συνδέεται με τα συστήματα πληροφοριών, προβλέποντας συγκεκριμένες ποινές και κυρώσεις για τους υπευθύνους, και παρέχοντας συνδρομή στα θύματα.*

Ελεονώρα Αναγνώστου

Δικηγόρος

D.E.A. Droit Economique et Social

Université Paris IX – Dauphine

[2] Οι πολίτες μπορούν να επικοινωνούν με τη Διεύθυνση Δίωξης ηλεκτρονικού εγκλήματος για πληροφορίες ή για να καταγγέλλουν παράνομες πράξεις που επιτελούνται μέσω **διαδικτύου στο email: ccu@cybercrimeunit.gov.gr ή στο τηλέφωνο: 11188 ή μέσω της πύλης https://portal.astynomia.gr**