ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
4η Δ.Υ.ΠΕ. ΜΑΚΕΔΟΝΙΑΣ & ΘΡΑΚΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ
ΑΛΕΞΑΝΔΡΟΥΠΟΛΗΣ

ΥΠΟΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αλεξ/πολη , 19.08.2019

Αρ. Πρωτ. 14432

ΠΡΟΣ: όλο το προσωπικό του Νοσοκομείου που έχει πρόσβαση στους υπολογιστές του ΠΓΝΑ

Πληροφορίες: κ. Κάρμεν Κοντογιαννίδη
Τηλέφωνο: (25513)53603
Fax: (25513) 53602
E-mail: kkont@pgna.gr

Επείγων

ΘΕΜΑ: *Προστασία από μηνύματα ηλεκτρονικού ταχυδρομείου με εκβιαστικό περιεχόμενο*

Σας ενημερώνω ότι στις τελευταίες ημέρες παρατηρείται μια νέα μορφή απάτης διεθνώς, για προσπάθεια οικονομικής εξαπάτησης, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου εκβιαστικού περιεχομένου, γνωστή ως απάτη μέσω σεξουαλικής εκβίασης “sextortion scam”, που εκδηλώνεται με μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου σε διάφορους αποδέκτες ανεξαρτήτου φύλου και ηλικίας, με σκοπό την εξαπάτησή τους.

Ειδικότερα άγνωστοι δράστες με τη χρήση απατηλών λογαριασμών ηλεκτρονικού ταχυδρομείου, στέλνουν μαζικά μηνύματα σε αποδέκτες και τους ενημερώνουν ότι διαθέτουν πρόσβαση στη συσκευή τους και το μήνυμα έχει αποσταλεί από τον προσωπικό τους λογαριασμό.
Παράλληλα τους γνωστοποιούν ότι έχει εγκατασταθεί κακόβουλο λογισμικό, μετά από την επίσκεψή τους σε κάποιον ιστότοπο, το οποίο έχει ενεργοποιήσει την κάμερα και τους έχει καταγράψει σε προσωπικές στιγμές.

Στη συνέχεια αναφέρεται ότι το κακόβουλο λογισμικό έχει συλλέξει όλες τις επαφές των χρηστών από τα μέσα κοινωνικής δικτύωσης και οι δράστες απειλούν με την αποστολή του επίμαχου υλικού στις επαφές τους, σε περίπτωση που δεν λάβουν bitcoins.
Η προσπάθεια εκβίασης των θυμάτων με την απειλή δημοσιοποίησης αρχείων ερωτικού περιεχομένου αναφέρεται διεθνώς ως σεξουαλική εκβίαση “sextortion”.

Σημειώνεται ότι τα εκβιαστικά αυτά μηνύματα ηλεκτρονικού ταχυδρομείου έχουν κυρίως τις παρακάτω μορφές και περιεχόμενο, ενώ η αναφορά σε πραγματικούς κωδικούς γίνεται ώστε οι χρήστες να πεισθούν για το αληθινό της απειλής.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, με αφορμή τα παραπάνω περιστατικά, προτρέπει τους παραλήπτες των απατηλών αυτών μηνυμάτων να:
- αγνοούν τα μηνύματα και να μην καταθέτουν χρήματα στους λογαριασμούς, που τους παραθέτει ο δράστης,
- μην ανοίγουν τυχόν συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς,
- μην επικοινωνούν ποτέ και για κανένα λόγο με τους εκβιαστές,
- αλλάζουν άμεσα κάθε κωδικό ασφαλείας (password) που νομίζουν ότι διακυβεύεται,
- αξιολογούν τις ρυθμίσεις ασφαλείας του υπολογιστή τους.

Υπενθυμίζεται ότι οι πολίτες μπορούν να επικοινωνούν, ανώνυμα ή επώνυμα, με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προκειμένου να παρέχουν πληροφορίες ή να καταγγέλλουν παράνομες ή επίμεμπτες πράξεις ή δραστηριότητες που τελούνται μέσω Διαδικτύου, στα ακόλουθα στοιχεία επικοινωνίας:
Τηλεφωνικά : 111 88
Στέλνοντας e – mail : ccu@cybercrimeunit.gov.gr
Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones), με λειτουργικό σύστημα iOS – A ndroid : FEELSAFE E – COMMERCE
Μέσω Twitter « Γραμμή SOS Cyber Alert»: https://twitter.com/CyberAlertGR
Επίσης, στην ιστοσελίδα της Ελληνικής Αστυνομίας www.hellenicpolice.gr στην ενότητα «Οδηγός του Πολίτη», θα βρείτε αναρτημένες γενικές και ειδικότερες συμβουλές για την αποφυγή εξαπάτησης.

Η Υποδιευθύντρια της
Υπηρεσίας Πληροφορικής

Κοντογιαννίδη Κάρμεν