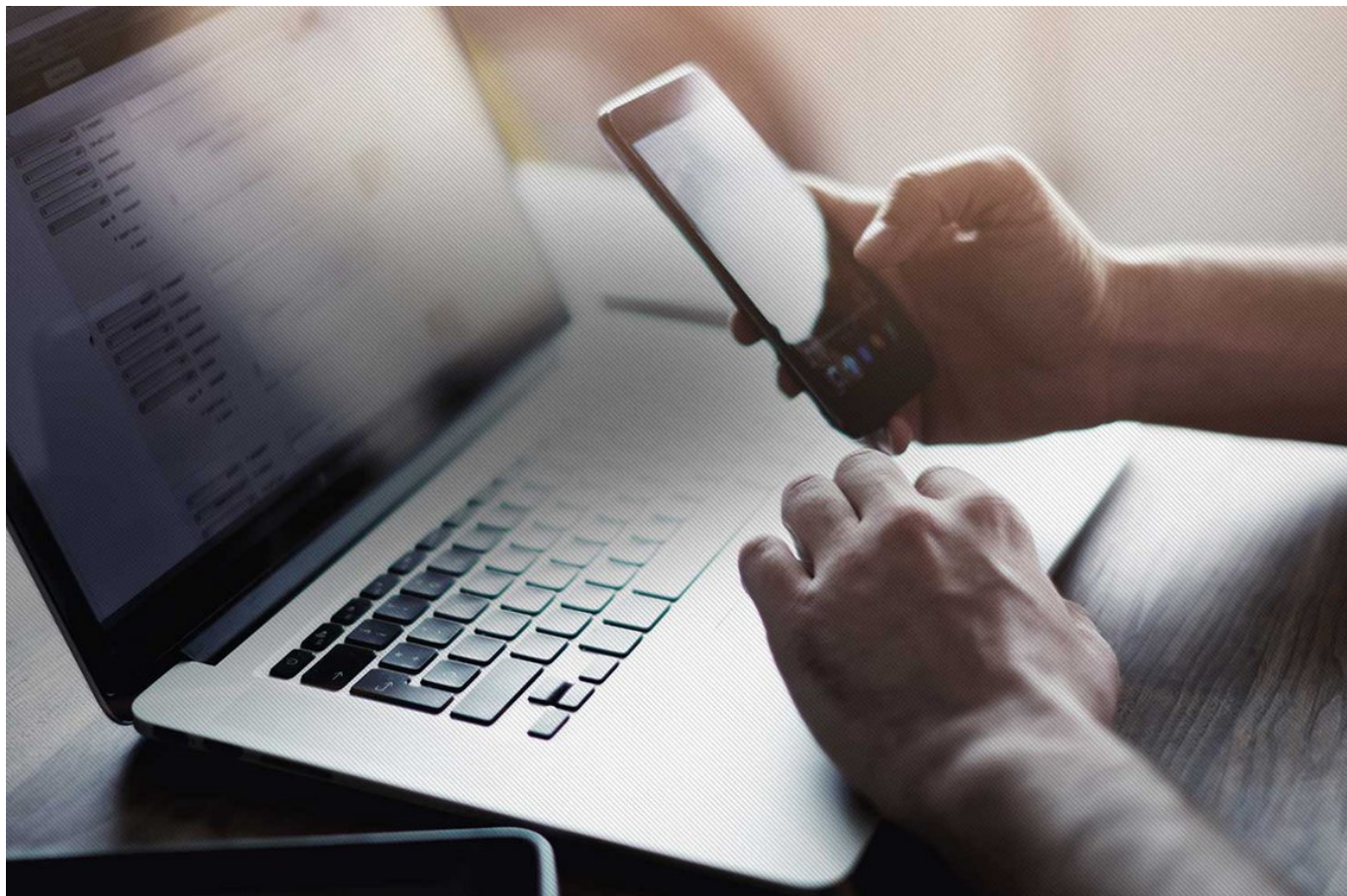
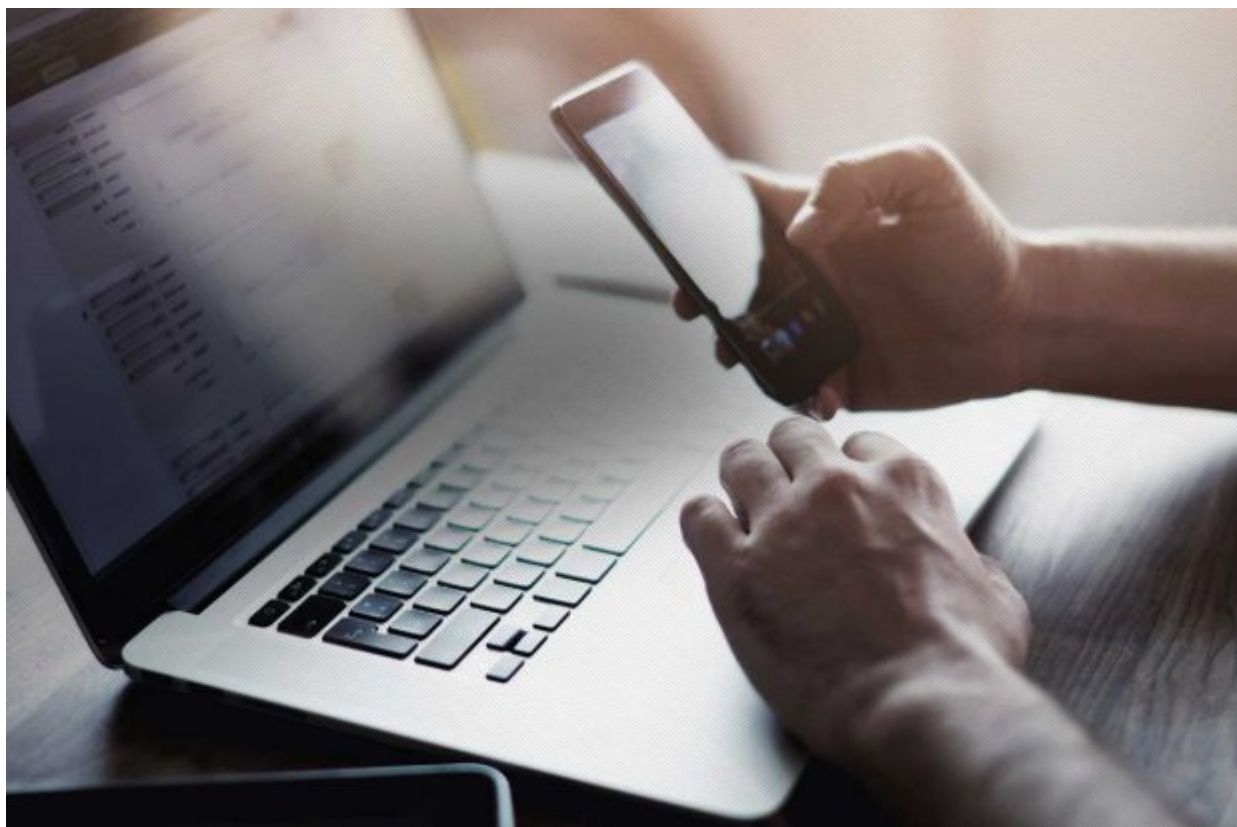


4 Αυγούστου 2018

Συναγερμός για τη Sextortion scam: Η νέα ηλεκτρονική απάτη

/ [Επιστήμες, Τέχνες & Πολιτισμός](#)





Μία νέα μορφή απάτης, διεθνώς γνωστή ως απάτη μέσω σεξουαλικής εκβίασης "sextortion scam" έκανε την εμφάνισή της τις τελευταίες ημέρες.

Η συγκεκριμένη μορφή εκβίασης, όπως ενημερώνει και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, εκδηλώνεται με μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου εκβιαστικού περιεχομένου, σε διάφορους αποδέκτες ανεξαρτήτου φύλου και ηλικίας, με σκοπό την οικονομική εξαπάτησή τους.

Ειδικότερα, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους χρήστες του διαδικτύου ότι άγνωστοι δράστες με τη χρήση απατηλών λογαριασμών ηλεκτρονικού ταχυδρομείου, στέλνουν μαζικά μηνύματα σε αποδέκτες και τους ενημερώνουν ότι γνωρίζουν τους κωδικούς ασφαλείας τους.

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.

Ωστόσο, σύμφωνα με τους καταγγέλλοντες, τις περισσότερες φορές οι κωδικοί αυτοί είναι αρκετά παλαιοί και δεν χρησιμοποιούνται πλέον, γεγονός που καταδεικνύει ότι προέρχονται από παλαιότερη διαρροή δεδομένων.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, με αφορμή τα παραπάνω περιστατικά, προτρέπει τους παραλήπτες των απατηλών μηνυμάτων, εκβιαστικού περιεχομένου να:

1. Αγνοούν τα μηνύματα και να μην καταθέτουν χρήματα στους λογαριασμούς, που τους παραθέτει ο δράστης.
2. Μην ανοίγουν τυχόν συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς.
3. Μην επικοινωνούν ποτέ και για κανένα λόγο με τους εκβιαστές.
4. Αλλάζουν άμεσα κάθε κωδικό ασφαλείας που νομίζουν ότι διακυβεύεται.
5. 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 στον αριθμό 111 88
- Στέλνοντας e-mail: ccu@cybercrimeunit.gov.gr
- Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones), με λειτουργικό σύστημα iOS - Android: 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 της εξαπάτησης σας.

Πηγή: real.gr