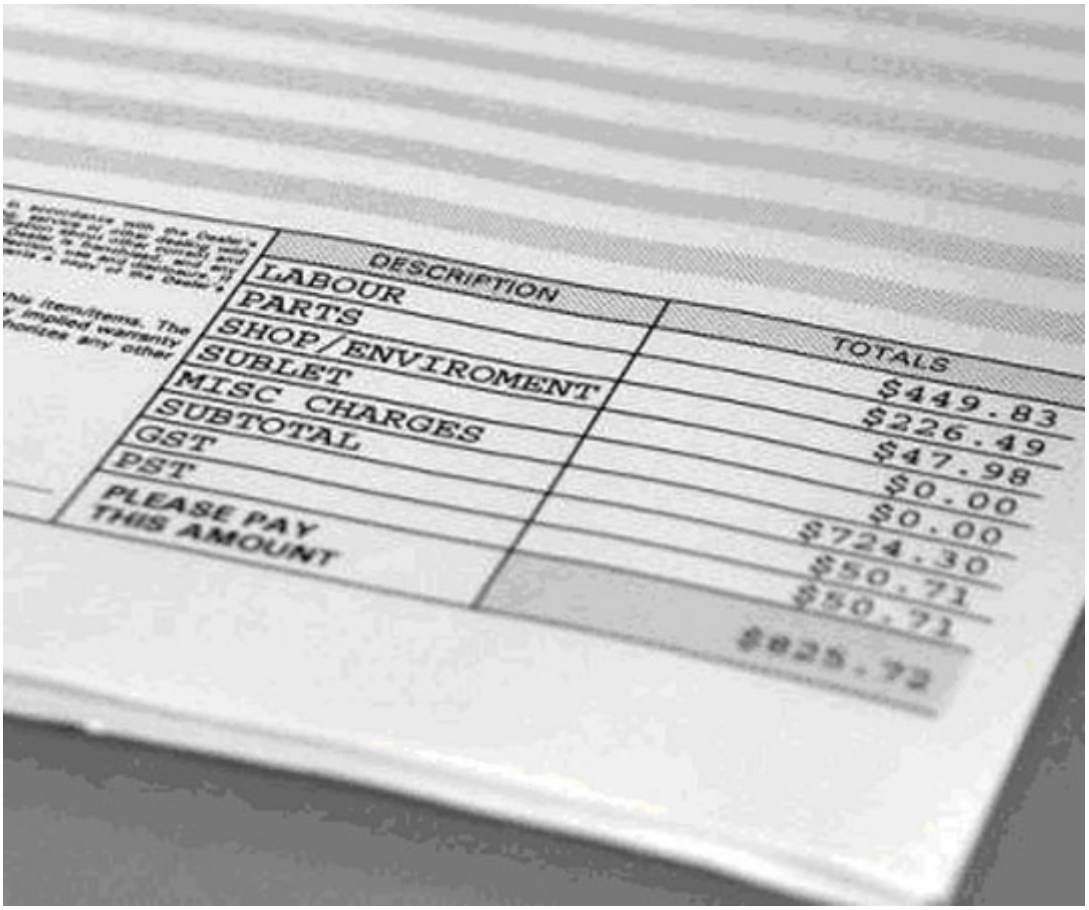
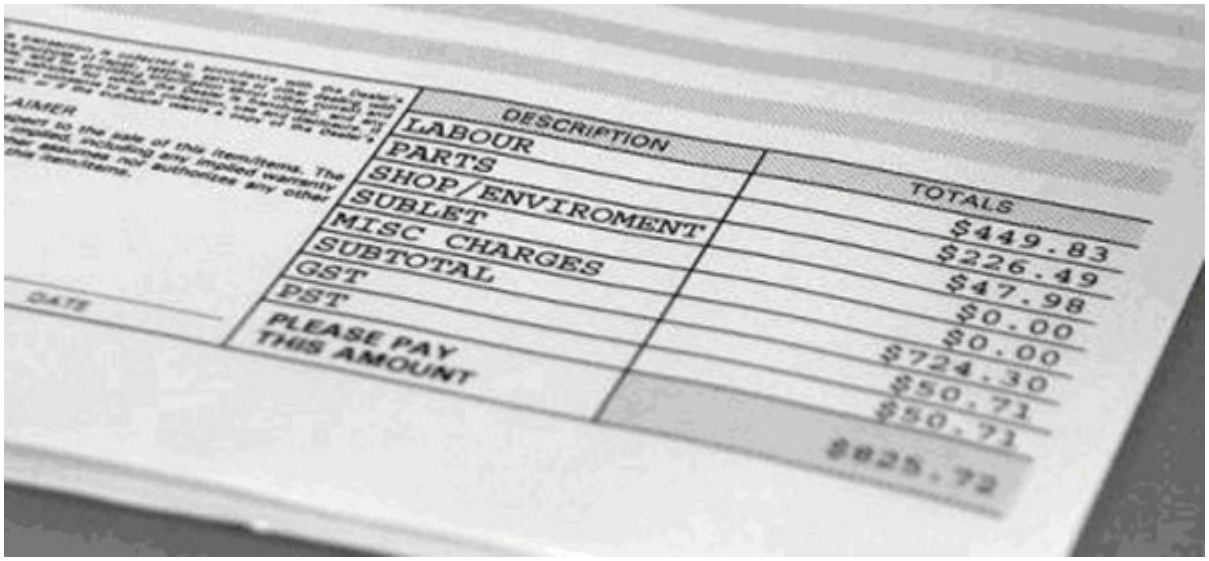
5 Φεβρουαρίου 2015

Απάτες στο ίντερνετ αποφέρουν 215 εκατομμύρια δολλάρια

/ Πεμπτουσία· Ορθοδοξία-Πολιτισμός-Επιστήμες





Κατά το παρελθόν έτος, επιχειρήσεις σε όλο τον κόσμο κατέγραψαν τεράστιες απώλειες ως αποτέλεσμα των πολλαπλών τύπων απάτης γνωστών ως Business Email Compromise (BEC), αποφέροντας στους scammers κέρδη κοντά στα 215 εκατομμύρια δολάρια σε ένα έτος.

Η έκθεση προέρχεται από μια ανακοίνωση δημόσιων υπηρεσιών που εκδίδεται από το *Internet Crime Complaint Center (IC3)*, μια συνεργασία μεταξύ του *FBI* και του *National White Collar Crime Center.*

Σύμφωνα με την έκθεση, τα περισσότερα από τα θύματα είναι από τις ΗΠΑ, οι οποίοι υπέστησαν το μεγαλύτερο μέρος των οικονομικών απωλειών, αλλά επιχειρήσεις σε 45 άλλες χώρες σε όλο τον κόσμο εξαπατήθηκαν επίσης.

Το IC3 αναφέρει ότι μεταξύ 10 Οκτωβρίου 2013 και 1 Δεκεμβρίου 2014, συνολικά 2.126 θύματα έπεσαν θύμα απάτης τύπου BEC, με 1.198 από τα θύματα να είναι από τις Ηνωμένες Πολιτείες, ενώ 928 να είναι από άλλες χώρες.

Ωστόσο, η κατάσταση είναι ολέθρια για τις επιχειρήσεις στις ΗΠΑ, καθώς αποτελούν στόχο πιο συχνά και κατά την περίοδο ανάλυσης, κατέγραψαν συνολικά 180 εκατομμύρια δολλάρια σε οικονομικές απώλειες.
Σε μεγαλύτερη κλίμακα, οι απάτες τύπου BEC έχουν ως στόχο μεγάλες εταιρείες που είτε αγοράζουν πλασματικά αγαθά ή παραδίδουν τα προϊόντα τους στους scammers, αφού οδηγούνται σε συμφωνία για καθυστερημένη πληρωμή.
Αυτό επιτυγχάνεται μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή φαξ με τον scammer να παρουσιάζεται ως μακροχρόνιος συνεργάτης των στοχευμένων επιχειρήσεων. Το μήνυμα που λαμβάνει το θύμα τους ζητά να αποσταλούν τα αγαθά ή τα χρήματα σε έναν διαφορετικό λογαριασμό ή σε άλλη τράπεζα από τη συνηθισμένη.
Δεδομένου ότι υπάρχει μια σταθερή σχέση μεταξύ των συνεργαζόμενων μερών, το

θύμα συμφωνεί με το αίτημα και οι scammers τελικά παραλαμβάνουν το εμπόρευμα ή τα κεφάλαια. Το καθεστώς είναι πολύπλοκο, δεδομένου ότι περιλαμβάνει επίσης πλαστά έγγραφα.

Μια παραλλαγή της απάτης συνιστάται στην ανάληψη του ελέγχου του λογαριασμού e-mail ενός υψηλόβαθμου στελέχους από τους scamers, τον οποίο χρησιμοποιούν για να στείλουν ένα αίτημα εμβάσματος προς τον υπεύθυνο της επιχείρησης αυτής.

Εναλλακτικά, οι κυβερνοεγκληματίες αποκτούν πρόσβαση στο email ενός εργαζομένου και το χρησιμοποιούν για την αποστολή αιτήσεων πληρωμής τιμολογίου στους επιχειρηματικούς εταίρους που προσδιορίζονται από τη λίστα των επαφών.

Σε άλλες απάτες ηλεκτρονικού ταχυδρομείου (εργασία από το σπίτι, λαχειοφόρο αγορά κλπ), τα θύματα πολλές φορές παρασύρονται ώστε να δεχθούν μια γενναιόδωρη προσφορά εργασίας για να χρησιμοποιηθούν τελικά ως «μεταφορείς» χρημάτων.

Συγκεκριμένα λαμβάνουν στον προσωπικό τραπεζικό τους λογαριασμό χρήματα που λαμβάνονται παράνομα από τον απατεώνα και καλούνται να παραδώσουν ορισμένα από αυτά μέσω τραπεζικού εμβάσματος σε τραπεζικό λογαριασμό που ανήκουν στον απατεώνα.

Το IC3 αναφέρει ότι τα θύματα μερικές φορές παρασύρονται σε άνοιγμα λογαριασμών για ψεύτικες εταιρείες στο δικό τους όνομα. Έτσι, όταν η απάτη αποκαλυφθεί, όλα δείχνουν ότι το θύμα ήταν υπεύθυνο.

Με βάση την έρευνα του IC3, φαίνεται ότι οι περισσότεροι από αυτούς τους απατεώνες βρίσκονται στην Κίνα, καθώς οι πληρωμές μέσω εμβάσματος έγιναν προς τράπεζες στην Κίνα και το Χονγκ Κονγκ.

Πηγή: Secnews.gr