

Business Email Compromise

Εντοπίστε άμεσα και προστατευτείτε από την πιο συνηθισμένη απάτη που αφορά Επιχειρήσεις κάθε μεγέθους.



Τι είναι το Business Email **Compromise**;

Το Business Email Compromise είναι μια μορφή απάτης που στοχεύει τις πληρωμές που πραγματοποιούν εταιρίες κάθε μεγέθους και κάθε δραστηριότητας προς προμηθευτές ή συνεργάτες τους.

Επιτήδριοι τρίτοι, υποδυόμενοι κάποιον εργαζόμενο του προμηθευτή, συνήθως γνωστό και έμπιστο πρόσωπο για την εταιρία-στόχο, ζητούν, μέσω email, την αλλαγή του υφιστάμενου λογαριασμού πληρωμής με έναν καινούργιο (ο οποίος στην πραγματικότητα ανήκει στους επιτήδειους).

Το αίτημα αυτό μπορεί να συνοδεύεται με μία επικείμενη πληρωμή ή απλά στοχεύει στην αλλαγή λογαριασμού πληρωμής για όλες τις επόμενες πληρωμές. Αν το αίτημα γίνει αποδεκτό από την εταιρία-στόχο και πραγματοποιηθεί στα συστήματά της η αλλαγή του λογαριασμού πληρωμής, τότε τα χρήματα καταλήγουν στα χέρια των επιτήδειων.

Είμαι επιχειρηματίας, πώς μπορώ να **προστατεύσω** την επιχείρησή μου;

1. Θεσπίζω μια νέα διαδικασία για τις πληρωμές μου, ώστε κάθε φορά που λαμβάνω αίτημα αλλαγής του λογαριασμού πληρωμής, το αίτημα να **επιβεβαιώνεται απευθείας** με τον προμηθευτή.
2. Ζητώ από τους συνεργάτες/προμηθευτές μου να ορίσουν ένα **έμπιστο άτομο** με το οποίο εγώ ή τα στελέχη μου **μπορούμε να επικοινωνούμε** για θέματα λογαριασμών πληρωμής και τιμολογίων. Κρατώ σε κάποιο αρχείο τα στοιχεία επικοινωνίας αυτού του προσώπου και χρησιμοποιώ **πάντα αυτά**.
3. **Εκπαιδεύω τους υπαλλήλους μου**, ιδιαίτερα αυτούς που πραγματοποιούν ή εγκρίνουν πληρωμές να αναγνωρίζουν άμεσα τα σημάδια μίας τέτοιας απάτης.
4. Εφαρμόζω τα **απαραίτητα μέτρα ασφαλείας** στους εταιρικούς servers και υπολογιστές και φροντίζω να ανανεώνονται συνεχώς με τις τελευταίες εκδόσεις.

Πραγματοποιώ πληρωμές για την εταιρία μου.

Ποιες είναι **οι ενέργειες που θα με γλυτώσουν** από μία τέτοια απάτη;

1. Ελέγχω προσεκτικά τη διεύθυνση email: Όταν λαμβάνω ένα email για αλλαγή λογαριασμού πληρωμής ελέγχω πολύ προσεκτικά τη διεύθυνση του αποστολέα και την αντιπαραβάλλω με άλλα παλαιότερα emails του. Δεν μου αρκεί το display name που βλέπω να είναι αυτό που έχω συνηθίσει γιατί οι κακόβουλοι τρίτοι έχουν φροντίσει να είναι ακριβώς ίδιο με αυτό που κανονικά χρησιμοποιείται για/από το συγκεκριμένο πρόσωπο. Ελέγχω τη διεύθυνση γράμμα προς γράμμα, ψάχνω για μικροδιαφορές στην κατάληξη της διεύθυνσης του email - όπως .co αντί για .com - ή για γράμματα που μοιάζουν ίδια αν κάποιος τα «περάσει» γρήγορα. Για παράδειγμα:

- m αντί για n john.smith@arnigo.com αντί για john.smith@amigo.com
- a αντί για a john.smith@amigo.com αντί για john.smith@amigo.com
- l αντί για l john.smith@example.com αντί για john.smith@example.com

2. Πάντα μα πάντα επιβεβαιώνω το αίτημα αλλαγής λογαριασμού πληρωμής με τον προμηθευτή σε απευθείας επικοινωνία μαζί του - κατά προτίμηση με άτομο που γνωρίζουμε καλά - και από κανάλι διαφορετικό από αυτό μου λάβαμε το αίτημα (π.χ. εάν το έχουμε λάβει με email παίρνουμε τηλέφωνο)

3. Δεν κάνω ποτέ χρήση των στοιχείων επικοινωνίας που υπάρχουν στο ύποπτο email: Οι κακόβουλοι τρίτοι γνωρίζοντας ότι το σημείο 2 παραπάνω είναι ένας εύκολος και πολύ αποτελεσματικός έλεγχος που μπορώ να κάνω, προσθέτουν στο email τους, ψεύτικα στοιχεία επικοινωνίας (σταθερό ή κινητό τηλέφωνο) που αν τα χρησιμοποιήσω θα οδηγήσουν σε αυτούς. Πάντα χρησιμοποιώ τα στοιχεία που γνωρίζω ήδη για τον προμηθευτή και μόνον αυτά.