Business Email Compromise (BEC)

Προστασία επιχειρήσεων από απάτες μέσω επιχειρησιακού email

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Τι είναι το Business Email Compromise (BEC);

Ορισμός

Το BEC είναι μία από τις πιο επικίνδυνες και οικονομικά καταστροφικές μορφές ηλεκτρονικής απάτης στον κόσμο των επιχειρήσεων. Οι επιτιθέμενοι δεν χρησιμοποιούν τεχνικές εκμεταλλεύσεις — χρησιμοποιούν **εμπιστοσύνη**.

Προσποιούνται στελέχη, συνεργάτες ή αξιόπιστους προμηθευτές για να εξαπατήσουν εργαζόμενους.

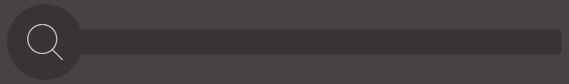
Οι στόχοι της επίθεσης

- Πραγματοποίηση αδικαιολόγητων χρηματικών μεταφορών
- Αποκάλυψη ευαίσθητων εταιρικών δεδομένων
- Αλλαγή στοιχείων τραπεζικών λογαριασμών
- Υποκλοπή κωδικών πρόσβασης

⚠ Το FBI κατατάσσει το BEC ως την #1 οικονομική απειλή για επιχειρήσεις παγκοσμίως.

Πώς εξελίσσεται μια επίθεση BEC;

Οι επιθέσεις BEC ακολουθούν μια συγκεκριμένη αλυσίδα βημάτων — κατανοώντας κάθε στάδιο μπορούμε να εντοπίσουμε και να σταματήσουμε την επίθεση εγκαίρως.



1. Συλλογή πληροφοριών

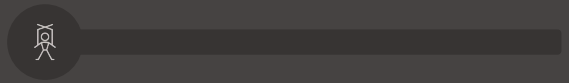
Αναγνώριση της εταιρείας, των εργαζομένων και των προμηθευτών της.

2. Παραβίαση / Πλαστογράφηση

Παραβίαση ή πλαστογράφηση εταιρικού λογαριασμού email.

3. Αποστολή μηνύματος

Σύνταξη και αποστολή πειστικού, παραπλανητικού μηνύματος.



4. Κοινωνική μηχανική

Πίεση του θύματος μέσω τεχνικών χειραγώγησης και επείγοντος.

5. Οικονομική απώλεια

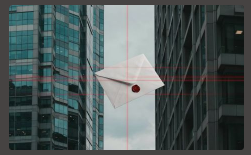
Οικονομική ζημία ή διαρροή ευαίσθητων δεδομένων.

Συνηθισμένα σενάρια BEC

Οι επιτιθέμενοι χρησιμοποιούν διαφορετικές τακτικές ανάλογα με τον στόχο τους. Αναγνωρίστε τα πιο κοινά σενάρια:

CEO fraud

Ο επιτιθέμενος μιμείται τον CEO ή ανώτερο στέλεχος και ζητά επείγουσα μεταφορά κεφαλαίων.



Vendor email compromise

Πλαστογράφηση email προμηθευτή για αλλαγή τραπεζικών στοιχείων την τελευταία στιγμή.

Invoice fraud

Αποστολή ψεύτικου τιμολογίου με νέο IBAN για επερχόμενη πληρωμή.

Credential theft

Ψεύτικο email ζητά στοιχεία σύνδεσης ή ανακατευθύνει σε σελίδα phishing.

Ενδείξεις ύποπτου email

Τα παρακάτω σήματα κινδύνου πρέπει να σας θέσουν σε άμεση επαγρύπνηση. Κανένα μεμονωμένο στοιχείο δεν αρκεί — συνδυάστε τα.

⚠️ Αίσθηση επείγοντος

Πίεση για άμεση δράση χωρίς χρόνο επαλήθευσης — «Πρέπει να γίνει ΤΩΡΑ!»

🔒 Αίτημα εμπιστευτικότητας

«Μην το αναφέρεις σε κανέναν» — κλασική τακτική απομόνωσης του θύματος.

🏦 Αλλαγή τραπεζικών στοιχείων

Αίτημα τελευταίας στιγμής για αλλαγή IBAN πριν από πληρωμή.

📧 Ύποπτο domain

Μικρές διαφορές: **company@acme-corp.com** αντί **acme.com** — πανομοιότυπο οπτικά, διαφορετικό τεχνικά.

📎 Απρόσμενα αρχεία

Συνημμένα ή σύνδεσμοι που δεν αναμένονταν, ακόμα και από γνωστές διευθύνσεις.

Πραγματικά παραδείγματα επιθέσεων

Τα παρακάτω μηνύματα αντιπροσωπεύουν τυπικές φόρμουλες που χρησιμοποιούν οι επιτιθέμενοι. Μοιάζουν αθώα — αλλά κρύβουν μεγάλο κίνδυνο.

Επείγουσα πληρωμή

«Παρακαλώ ολοκλήρωσε **άμεσα** αυτή την πληρωμή των €45.000. Είναι εμπιστευτικό, μην το συζητήσεις με κανέναν άλλο. — Διευθύνων Σύμβουλος»

Αλλαγή λογαριασμού

«Σας ενημερώνουμε ότι αλλάξαμε τον τραπεζικό μας λογαριασμό. Παρακαλούμε χρησιμοποιήστε το νέο IBAN για την τρέχουσα πληρωμή σας.»

Υποκλοπή μισθοδοσίας

«Χρειάζομαι επειγόντως τα στοιχεία μισθοδοσίας όλου του προσωπικού για έλεγχο. Στείλε μου τώρα σε αρχείο Excel.»

⊗ Αν λάβετε παρόμοιο μήνυμα: ΜΗΝ απαντήσετε. Επικοινωνήστε με τον αποστολέα μέσω γνωστού τηλεφώνου.

Πώς προστατευόμαστε;

Η προστασία από BEC απαιτεί συνδυασμό τεχνικών μέτρων και ανθρώπινης επαγρύπνησης.

MFA παντού

Ενεργοποιήστε Multi-Factor Authentication σε όλους τους εταιρικούς λογαριασμούς email και συστήματα.

Δεύτερο κανάλι

Επιβεβαιώνετε κάθε αίτημα πληρωμής μέσω τηλεφώνου σε γνωστό αριθμό — ποτέ μέσω reply στο ίδιο email.

Έλεγχος domain

Πάντα ελέγχετε προσεκτικά το domain του αποστολέα — ακόμα και μία παραγεμιστή διαφορά αρκεί.

Εκπαίδευση

Τακτικές ασκήσεις προσομοίωσης phishing και ενημερωτικές συνεδρίες για όλο το προσωπικό.

Εταιρικές διαδικασίες: πριν από κάθε πληρωμή

Εφαρμόστε αυτή την τετραπλή διαδικασία επαλήθευσης χωρίς εξαιρέσεις — ακόμα και για «επείγοντα» αιτήματα.

01

Επιβεβαίωση μέσω τηλεφώνου

Καλέστε τον αιτούντα στον **γνωστό** αριθμό τηλεφώνου της εταιρείας — ποτέ στον αριθμό που αναγράφεται στο email.

02

Four eyes principle

Κάθε πληρωμή πρέπει να εγκρίνεται από **δύο διαφορετικά άτομα** — ανεξάρτητα από το ποσό ή τον βαθμό επείγοντος.

03

Έλεγχος IBAN

Συγκρίνετε τον IBAN με τα καταχωρημένα στοιχεία του συστήματός σας. Οποιαδήποτε αλλαγή απαιτεί αυτόματη επαλήθευση.

04

Επιβεβαίωση αλλαγών

Κάθε αλλαγή τραπεζικού λογαριασμού από προμηθευτή επιβεβαιώνεται **τηλεφωνικά** πριν εφαρμοστεί.

Τι κάνουμε αν υποψιαστούμε BEC;

Άμεσες ενέργειες

- **ΜΗΝ** απαντήσετε στο ύποπτο email
- **ΜΗΝ** ανοίξετε συνδέσμους ή συνημμένα
- Ενημερώστε **άμεσα** το IT ή το SOC της εταιρείας
- Διατηρήστε το μήνυμα ως αποδεικτικό στοιχείο — μην το διαγράψετε

Αν έχει ήδη γίνει πληρωμή

- Επικοινωνήστε **αμέσως** με την τράπεζά σας για παγοποίηση της συναλλαγής
- Ακολουθήστε το εταιρικό σχέδιο αντιμετώπισης περιστατικών (Incident Response Plan)
- Υποβάλετε αναφορά στις αρχές (Δίωξη Ηλεκτρονικού Εγκλήματος)
- Τεκμηριώστε όλα τα γεγονότα με χρονολογική σειρά

⊗ Κάθε λεπτό μετράει — η ταχύτητα αντίδρασης καθορίζει αν τα χρήματα ανακτηθούν.

Checklist προστασίας & συμπεράσματα

Η λίστα ελέγχου σας

- [x] MFA ενεργό σε όλους τους λογαριασμούς
- [x] Έλεγχος domain αποστολέα σε κάθε email
- [x] Επιβεβαίωση πληρωμών μέσω δεύτερου καναλιού
- [x] Χρήση Password manager
- [x] Αναφορά ύποπτων emails στο IT
- [x] Συνεχής εκπαίδευση προσωπικού

Τα 3 κεντρικά μηνύματα

🎯 Ο άνθρωπος είναι ο στόχος

Το BEC βασίζεται στην εξαπάτηση ανθρώπων, όχι συστημάτων.

✅ Η επαλήθευση σώζει

Ένα τηλεφώνημα επαλήθευσης μπορεί να αποτρέψει απώλεια εκατοντάδων χιλιάδων ευρώ.

📚 Εκπαίδευση & Διαδικασίες

Οι σωστές διαδικασίες και η συνεχής εκπαίδευση μειώνουν δραστικά τον κίνδυνο.