EUROBANK

Συνήθεις μορφές ηλεκτρονικής απάτης σε πληρωμές επιχειρήσεων

Κύρια σημάδια εντοπισμού & αντιμετώπιση

11 Νοεμβρίου, 2025

Η κυβερνοαπάτη αυξάνεται δραματικά και αποτελεί κομμάτι του Οργανωμένου Εγκλήματος

EUROBANK

*"Cyber-enabled fraud is a major **transnational organised crime** that has **grown exponentially** in recent years, both in volume of frauds reported and their global spread"*

- Financial Action Task Force (FATF)

*"We are facing an **epidemic in the growth of financial fraud**, leading to individuals, often vulnerable people, and companies being defrauded **on a massive and global scale**"*

- **Jürgen Stock,** *INTERPOL Secretary General*

*"Cyber crime **through a platform** has become so easy that even a criminal **with limited technical skills** manages to come through. **98%-99%** of online fraudsters are **social engineers, not hackers**"*

- **Brett Johnson,** Former Fraudster, US Most Wanted Cybercriminal

Τι είναι το BEC;

Το **Business Email Compromise** (BEC) αποτελεί μια κατηγορία κυβερνοεγκλήματος όπου κακόβουλοι τρίτοι προσποιούνται μέσω email ότι είναι αξιόπιστες επαγγελματικές επαφές του θύματος (συνήθως προμηθευτές του), προσπαθώντας έτσι να το ξεγελάσουν ώστε να προχωρήσει σε πληρωμές από την εταιρεία ή τον οργανισμό στον οποίο εργάζεται προς λογαριασμούς που ελέγχονται από τους κακόβουλους τρίτους

Το BEC έχει γίνει ένα από τα πιο οικονομικά καταστροφικά κυβερνοεγκλήματα παγκοσμίως με απώλειες

$55B+

σε παγκόσμιο επίπεδο την περίοδο 2013 – 2024.

Οι πλέον διαδεδομένες τυπολογίες του BEC είναι οι:

Invoice Scam: Οι κακόβουλοι τρίτοι υποδύονται τον προμηθευτή της εταιρείας/ οργανισμού. Στέλνουν ένα email ζητώντας αλλαγή του λογαριασμού πληρωμής κατευθύνοντάς την σε έναν λογαριασμό που ελέγχουν. Συχνά, μάλιστα, για να γίνουν πιο πιστευτοί περιμένουν μέχρι να πλησιάσει η λήξη μια τακτικής πληρωμής και μόνο τότε στέλνουν το email που ζητούν την αλλαγή του λογαριασμού πληρωμής.

CEO Fraud: Οι επιτήδειοι προσποιούνται ότι είναι ανώτερο στέλεχος της εταιρείας—συνήθως ο CEO— και μέσω πλαστών και παραπλανητικών email ζητούν από τον υπάλληλό τους να μεταφέρει **άμεσα** χρήματα σε λογαριασμό που τους υποδεικνύουν. Στόχος τους είναι να εκμεταλλευτούν την εξουσία και την αίσθηση του κατεπείγοντος για να παρακάμψουν τις συνήθεις διαδικασίες ελέγχου.

Το 2022 οι απώλειες από αυτή την μορφή της απάτης ήταν 80-φορές μεγαλύτερες από αυτές του Ransomware

Πηγή: FBI IC3 report

Ορισμένα επιπλέον στατιστικά που αναδεικνύουν την έκταση του προβλήματος

EUROBANK

$ 2,8B

Απώλειες στις ΗΠΑ το 2024

£ 54,5M

Απώλειες στο Ηνωμένο Βασίλειο το 2024

€ 3,4M

Απώλειες στην Ελλάδα το 2024

$ 125K

η μέση ζημία στις ΗΠΑ το 2024

£ 21K

η μέση ζημία στο Ηνωμένο Βασίλειο το 2024

€ 42K

η μέση ζημία στην Ελλάδα το 2024

Παραδείγματα Επιθέσεων BEC με μεγάλες απώλειες

EUROBANK

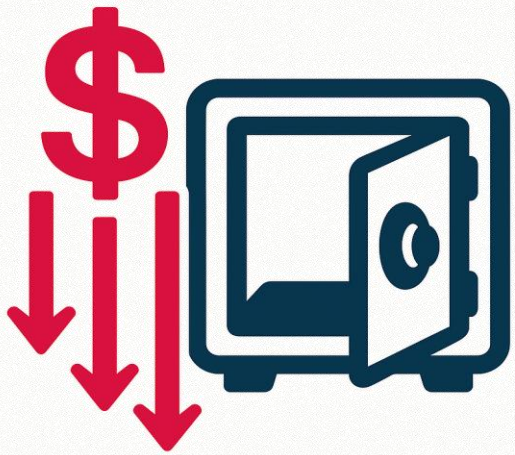
1. **Google & Facebook (2013–2015)**: Λιθουανός, παρίστανε προμηθευτή εξαρτημάτων υπολογιστών και εξαπάτησε τους δύο τεχνολογικούς κολοσσούς, αποσπώντας τους πάνω από $120 εκατ. μέσω πλαστών τιμολογίων και ψεύτικης εταιρείας. Καταδικάστηκε σε 5 χρόνια φυλάκιση.

2. **Toyota Boshoku (2019)**: Θυγατρική της Toyota έχασε $37 εκατ. όταν απατεώνες προσποιήθηκαν συνεργάτη και έστειλαν ψεύτικες οδηγίες πληρωμής. Η απάτη αποκαλύφθηκε μετά την ολοκλήρωση της μεταφοράς. Σημαντικό ότι ήταν η τρίτη απάτη με την ίδια μέθοδο που στόχευσε την συγκεκριμένη εταιρία μέσα

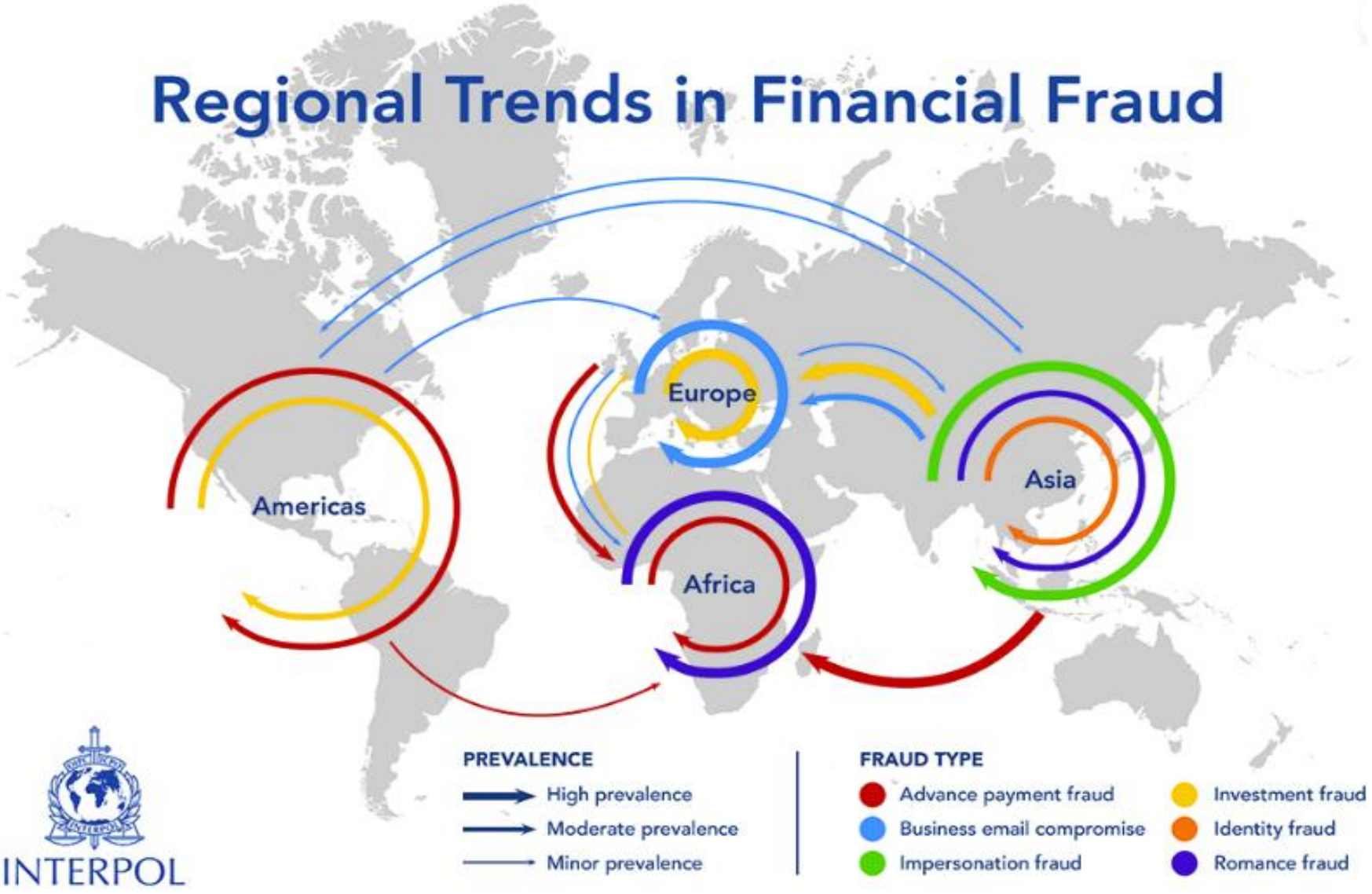
3. **Orion S.A. (2024)**: Βιομηχανία με έδρα το Λουξεμβούργο που δραστηριοποιείται στην παραγωγή Αιθάλης έχασε $60 εκατ. όταν υπάλληλος εξαπατήθηκε και έκανε πολλαπλές μεταφορές χρημάτων για πληρωμές τιμολογίων σε νέο λογαριασμό που του υπέδειξε ο "προμηθευτής" του.

4. **Crelan Bank (2016)**: Η βελγική τράπεζα έχασε €70 εκατ. από απάτη τύπου “CEO fraud”. Η απάτη εντοπίστηκε κατά την διάρκεια εσωτερικού ελέγχου και οδήγησε σε ενίσχυση των εσωτερικών ελέγχων.

5. **Δημόσιοι & Μη Κερδοσκοπικοί Οργανισμοί**
   - Δήμος Saskatoon (Καναδάς): $1 εκατ. σε ψεύτικο λογαριασμό εργολάβου.
   - Save the Children (2018): $1 εκατ. μέσω παραβιασμένου email.
   - Καθολική ενορία (ΗΠΑ, 2019): $1.7 εκατ. σε απατεώνες.



Η Ροή Χρημάτων από Απάτες BEC Είναι Παγκόσμια



- Στην Ευρώπη, η απάτη BEC είναι η πιο κοινή μορφή ηλεκτρονικής απάτης.
- Οι περισσότερες χρηματικές απώλειες κατευθύνονται σε άλλες χώρες της Ευρώπης.

Πηγή: INTERPOL fraud assessment

Τι πρέπει να κάνω για να προστατευτώ;

EUROBANK

Κάθε φορά που λαμβάνω email με αίτημα από προμηθευτή μου για αλλαγή του συνηθισμένου λογαριασμού πληρωμής του:

Εξετάζω **γράμμα προς γράμμα** το email address από το οποίο έλαβα την επικοινωνία. Κοιτάζω προσεκτικά για **μικρές λεπτομέρειες** που μέσα στην καθημερινότητα μπορεί να ξεφύγουν, όπως:

rn αντί για m	john.smith@arnigo.com αντί για john.smith@amigo.com
ạ αντί για a	john.smith@ạmigo.com αντί για john.smith@amigo.com
1 αντί για l	john.smith@examp1e.com αντί για john.smith@example.com

Τι πρέπει να κάνω για να προστατευτώ;

Ακόμη και αν δεν βρω καμία διαφορά στο email που έλαβα με αυτό που γνωρίζω για τον προμηθευτή μου

Πάντα μα πάντα επιβεβαιώνω το αίτημα αλλαγής λογαριασμού πληρωμής

Επικοινωνώ **απευθείας** με τον προμηθευτή μου και του ζητώ να επιβεβαιώσει την αλλαγή του λογαριασμού

Για την επιβεβαίωση δεν απαντώ **ποτέ** στο email που έχω λάβει, αλλά **καλώ στο τηλέφωνο**

Επιδιώκω να μιλήσω με πρόσωπο το οποίο γνωρίζω και έχω μιλήσει/συνεργαστεί ξανά στο παρελθόν

Τι πρέπει να κάνω για να προστατευτώ;

EUROBANK

Προσέχω πάντα για την τελευταία παγίδα που μπορεί να μου έχουν στήσει:

Δεν χρησιμοποιώ ποτέ τα στοιχεία επικοινωνίας (σταθερό, κινητό) που περιέχονται στην υπογραφή ή στο κείμενο του **email** που μου ζητά την **αλλαγή λογαριασμού πληρωμής**

Για κάθε προμηθευτή/ συνεργάτη προς τον οποίο πραγματοποιώ πληρωμές διατηρώ επίσημο αρχείο με τα ορθά στοιχεία επικοινωνίας του

Επικοινωνώ ή στέλνω μήνυμα μόνο σε τηλέφωνα που έχω χρησιμοποιήσει στο παρελθόν χωρίς πρόβλημα και βρίσκονται στο επίσημο αρχείο της εταιρίας μου