

ΑΠΑΤΗ ΤΟΥ CEO / ΑΠΑΤΗ ΜΕ ΤΟ ΕΤΑΙΡΙΚΟ E-MAIL

Η απάτη του CEO / απάτη με το εταιρικό e-mail λαμβάνει χώρα όταν ένας εξουσιοδοτημένος να πραγματοποιεί πληρωμές υπάλληλος της εταιρείας εξαπατάται προκειμένου να πληρώσει ένα πλαστό τιμολόγιο ή να διενεργήσει μια μη εγκεκριμένη μεταφορά πίστωσης από τον εταιρικό λογαριασμό της επιχείρησης.

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ;

Ο απατεώνας καλεί ή στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου υποδυόμενος υψηλόβαθμο στέλεχος της επιχείρησης (π.χ. Γενικός Διευθυντής ή Οικονομικός Διευθυντής).

Γνωρίζουν επαρκώς την εσωτερική διάρθρωση και οργάνωση της επιχείρησης.

Απαιτούν τη διενέργεια μιας επείγουσας πληρωμής.

Χρησιμοποιούν όρους και εκφράσεις, όπως: "εχεμύθεια/εμπιστευτικότητα", "η επιχείρηση σε εμπιστεύεται", "δεν είμαι αυτή τη στιγμή διαθέσιμος".



Συχνά το αίτημα αφορά τη διενέργεια διασυννοριακών πληρωμών σε τράπεζες εγκατεστημένες εκτός Ευρώπης.

Ο υπάλληλος μεταφέρει τα χρήματα σε λογαριασμό που τηρεί ο απατεώνας.

Οδηγίες για την διαδικασία μπορεί να δοθούν αργότερα, μέσω τρίτου προσώπου ή μηνύματος ηλεκτρονικού ταχυδρομείου.

Απαιτούν από τον υπάλληλο της επιχείρησης να μην ακολουθήσει τις συνήθεις διαδικασίες λήψης έγκρισης για την πληρωμή.

Αναφέρονται σε μια "ευαίσθητη" για την επιχείρηση κατάσταση (π.χ. φορολογικός έλεγχος, συγχώνευση, εξαγορά).

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΕΝΔΕΙΞΕΙΣ;

- Αιφνιδιαστική / Απροειδοποίητη τηλεφωνική κλήση ή e-mail
- Απευθείας επικοινωνία με ανώτερο στέλεχος της επιχείρησης με το οποίο συνήθως δεν επικοινωνεί
- Αίτημα για απόλυτη εχεμύθεια
- Άσκηση πίεσης για το κατεπείγον του αιτήματος
- Ασύνηθες αίτημα αντίθετο με τις εσωτερικές διαδικασίες έγκρισης
- Απειλές ή ασυνήθιστη κολακεία / υποσχέσεις ανταμοιβής

ΤΙ ΜΠΟΡΕΙΤΕ ΝΑ ΚΑΝΕΤΕ;

Ως επιχείρηση

Να γνωρίζετε τους κινδύνους και να διασφαλίζετε ότι και οι υπάλληλοί σας είναι επίσης ενημερωμένοι.

Να ενθαρρύνετε το προσωπικό σας να προσεγγίζει τα αιτήματα για τη διενέργεια πληρωμών με προσοχή.

Εφαρμόστε εσωτερικές διαδικασίες σχετικά με τη διενέργεια πληρωμών.

Εφαρμόστε διαδικασία για την επαλήθευση της νομιμότητας αιτημάτων διενέργειας πληρωμών που λαμβάνονται μέσω e-mail.

Καθιερώστε διαδικασίες υποβολής αναφορών για τη διαχείριση περιστατικών απάτης.

Ελέγξτε τις πληροφορίες που αναρτώνται στην ιστοσελίδα της επιχείρησής σας, περιορίστε τις πληροφορίες και επιδείξτε ιδιαίτερη προσοχή σε σχέση με τα κοινωνικά μέσα δικτύωσης.

Να αναβαθμίζετε και να ενημερώνετε το λογισμικό τεχνικής ασφαλείας.

! Να επικοινωνείτε πάντα με την αστυνομία σε περιπτώσεις απόπειρας απάτης, ακόμα και αν δεν είστε θύμα αυτής.

Ως εργαζόμενος

Να εφαρμόζετε αυστηρά τις υφιστάμενες διαδικασίες ασφαλείας σε σχέση με τη διενέργεια πληρωμών και καταβολής προμηθειών. Μην παραλείπετε κανένα βήμα και μην υποκύψετε σε πιέσεις.

Να ελέγχετε πάντα με προσοχή τις διευθύνσεις ηλεκτρονικού ταχυδρομείου όταν διαχειρίζεστε ευαίσθητες πληροφορίες / πραγματοποιείτε μεταφορές χρημάτων.

Σε περίπτωση αμφιβολίας για εντολή πληρωμής, συμβουλευθείτε έναν αρμόδιο συνάδελφό σας.

Μην ανοίγετε ποτέ ύποπτους ηλεκτρονικούς συνδέσμους (links) ή ύποπτα επισυναπτόμενα αρχεία που λαμβάνετε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Να είστε εξαιρετικά προσεκτικοί όταν ελέγχετε το προσωπικό σας e-mail στους υπολογιστές της επιχείρησης στην οποία εργάζεστε.

Περιορίστε τις πληροφορίες και επιδείξτε προσοχή σε σχέση με τα μέσα κοινωνικής δικτύωσης.

Αποφεύγετε την κοινοποίηση πληροφοριών σχετικά με την ιεραρχία, την ασφάλεια και τις ακολουθούμενες διαδικασίες της επιχείρησης στην οποία εργάζεστε.

! Αν λάβετε ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ύποπτη τηλεφωνική κλήση, να ενημερώνετε πάντοτε τη διεύθυνση μηχανογραφικής υποστήριξης.