Τίτλος δραστηριότητας: Παιχνίδι ρόλων – Αντιμετώπιση μιας ψηφιακής απειλής

Στόχος:

Να βοηθήσει τους συμμετέχοντες να αναγνωρίσουν μια απόπειρα ηλεκτρονικού ψαρέματος, να κατανοήσουν γιατί είναι επικίνδυνη και να δείξουν τον κατάλληλο τρόπο αντίδρασης.

Διάρκεια

15-20 λεπτά

Απαιτούμενα υλικά:

- **Εκτυπωμένα αντίγραφα** ή **ψηφιακή προβολή** του σεναρίου ηλεκτρονικού ψαρέματος για κάθε ομάδα.
- **Σημειωματάρια και στυλό** (προαιρετικά) για τη λήψη σημειώσεων κατά τη διάρκεια της συζήτησης.

Οδηγίες:

1. **Δημιουργία ομάδων**:
    - Χωρίστε τους συμμετέχοντες σε **ζευγάρια**.
2. **Σενάριο**:
    - Λαμβάνετε ένα email που φαίνεται να προέρχεται από την τράπεζά σας. Το email σας ζητά να επαληθεύσετε τα στοιχεία του λογαριασμού σας κάνοντας κλικ σε έναν σύνδεσμο.
      Παράδειγμα κειμένου email:
    - **Θέμα**: **«Σημαντικό: Επαληθεύστε τα στοιχεία του λογαριασμού σας»**
    - **Μήνυμα**:
      «Αγαπητέ πελάτη,
      Παρατηρήσαμε ασυνήθιστη δραστηριότητα στον τραπεζικό σας λογαριασμό. Για την προστασία του λογαριασμού σας, πρέπει να

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

επαληθεύσετε τα στοιχεία σας.
Κάντε κλικ στον παρακάτω σύνδεσμο και συνδεθείτε στον λογαριασμό σας.
[Σύνδεσμος σύνδεσης FakeBank.com]
Σας ευχαριστούμε που επιλέξατε τις τραπεζικές υπηρεσίες μας.
Με εκτίμηση,
Η ομάδα εξυπηρέτησης πελατών

---

3. **Ανάθεση ρόλων**:
    - **Συμμετέχων 1**: Παίζει το ρόλο του χρήστη που έλαβε το ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος.
    - **Συμμετέχων 2**: Παίζει το ρόλο του ειδικού σε θέματα κυβερνοασφάλειας που συμβουλεύει τον χρήστη για το πώς να χειριστεί την κατάσταση.

---

4. **Εργασία**:
    - **Ο συμμετέχων 1** πρέπει να εξηγήσει πώς θα αντιδρούσε αρχικά στο email, λαμβάνοντας υπόψη αν υποψιάζεται ότι πρόκειται για απόπειρα ηλεκτρονικού ψαρέματος ή όχι.
    - **Ο συμμετέχων 2** θα παρέχει συμβουλές ειδικού σχετικά με:
        - Γιατί το email είναι πιθανότατα μια απόπειρα ηλεκτρονικού ψαρέματος.
        - Τα συγκεκριμένα **προειδοποιητικά σημάδια** (π.χ. ασυνήθιστη γλώσσα, επείγοντα αιτήματα, ύποπτος σύνδεσμος).
        - Τα σωστά μέτρα που πρέπει να ληφθούν (π.χ. να μην κάνει κλικ στον σύνδεσμο, να επικοινωνήσει απευθείας με την τράπεζα).

Βήματα που πρέπει να ακολουθηθούν στο παιχνίδι ρόλων:

1. **Προσδιορίστε την ψηφιακή απειλή**:
    - Συζητήστε γιατί το email είναι επικίνδυνο:

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

- Ύποπτος σύνδεσμος (π.χ. τοποθετήστε τον κέρσορα πάνω από τον σύνδεσμο για να ελέγξετε την πραγματική διεύθυνση URL).
- Γλώσσα που προκαλεί πανικό.
- Έλλειψη προσωπικών στοιχείων (καμία αναφορά στο πραγματικό όνομα του χρήστη).

2. **Στρατηγική αντίδρασης**:
    - Ο συμμετέχων 2 πρέπει να καθοδηγήσει τον συμμετέχοντα 1 ως εξής:
        - **Μην κάνετε κλικ σε κανέναν σύνδεσμο** και μην κατεβάζετε συνημμένα.
        - **Αναφέρετε το email** ως phishing στον πάροχο email.
        - **Επικοινωνήστε απευθείας με την τράπεζα** χρησιμοποιώντας επίσημα κανάλια επικοινωνίας για να επαληθεύσετε εάν το αίτημα είναι νόμιμο.
        - **Διαγράψτε το email** μετά την αναφορά του.

Αναφορά:

- Μετά την ολοκλήρωση του παιχνιδιού ρόλων, κάθε ζευγάρι θα πρέπει να παρουσιάσει συνοπτικά:
    - Τα **προειδοποιητικά σημάδια** που εντόπισαν στο ηλεκτρονικό μήνυμα phishing.
    - Τα **μέτρα** που έλαβαν για να χειριστούν την κατάσταση και να προστατεύσουν την ψηφιακή τους ταυτότητα.
- Διοργανώστε μια **ομαδική συζήτηση** με θέμα:
    - **Τι κάνει τα ηλεκτρονικά μηνύματα phishing αποτελεσματικά;**
    - **Ποια είναι μερικά άλλα παραδείγματα προσπαθειών ηλεκτρονικού ψαρέματος που** έχουν συναντήσει οι συμμετέχοντες;

Ρόλος του συντονιστή:

- Βεβαιωθείτε ότι οι συμμετέχοντες κατανοούν τον σκοπό της άσκησης.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

- Ενθαρρύνετε τον «ειδικό» σε θέματα κυβερνοασφάλειας να εξηγήσει με σαφήνεια πώς να αναγνωρίζουν οι χρήστες τις απόπειρες ηλεκτρονικού ψαρέματος και να τους καθοδηγούν.
- Ολοκληρώστε ενισχύοντας τις βέλτιστες πρακτικές για **την ψηφιακή ασφάλεια** και **τον τρόπο αντιμετώπισης των απειλών ηλεκτρονικού ψαρέματος**.

Co-funded by the European Union

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.