Τίτλος Δραστηριότητας: Παιχνίδι ρόλων - Αντιμετώπιση μιας ψηφιακής απειλής

Στόχος:

Να βοηθήσει τους συμμετέχοντες να αναγνωρίσουν μια απόπειρα phishing, να κατανοήσουν γιατί είναι επικίνδυνη και να επιδείξουν την κατάλληλη αντίδραση.

Διάρκεια:

15-20 λεπτά

Απαιτούμενα υλικά:

- **Εκτυπωμένα αντίγραφα** ή **ψηφιακή απεικόνιση** του σεναρίου του ηλεκτρονικού μηνύματος ηλεκτρονικού "ψαρέματος" για κάθε ομάδα.
- **Σημειωματάρια και στυλό** (προαιρετικά) για να κρατάτε σημειώσεις κατά τη διάρκεια της συζήτησης.

Οδηγίες:

1. **Σχηματισμός ομάδας**:
    - Χωρίστε τους συμμετέχοντες σε **ζευγάρια**.
2. **Σενάριο**:
    - Λαμβάνετε ένα email που μοιάζει 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: Επαλήθευση των στοιχείων του λογαριασμού σας"**
    - **Μήνυμα**:

      "Παρατηρήσαμε ασυνήθιστη δραστηριότητα στον τραπεζικό σας λογαριασμό. Για την προστασία του λογαριασμού σας, πρέπει να επαληθεύσετε τα στοιχεία σας.
      Παρακαλούμε κάντε κλικ στον παρακάτω σύνδεσμο και συνδεθείτε στο λογαριασμό σας.
      [Σύνδεσμος σύνδεσης FakeBank.com]
      Σας ευχαριστούμε για τις τραπεζικές σας συναλλαγές μαζί μας.
      Με τους καλύτερους χαιρετισμούς,
      Ομάδα υποστήριξης πελατών"

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.

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

---

4. **Εργασία**:
    - **Ο συμμετέχων 1** θα πρέπει να εξηγήσει πώς θα αντιδρούσε αρχικά στο μήνυμα ηλεκτρονικού ταχυδρομείου, εξετάζοντας αν υποψιάζεται ότι πρόκειται για απόπειρα ηλεκτρονικού "ψαρέματος" ή όχι.
    - **Ο συμμετέχων 2** θα παράσχει συμβουλές εμπειρογνωμόνων σχετικά με:
        - Γιατί το μήνυμα ηλεκτρονικού ταχυδρομείου είναι πιθανότατα απόπειρα ηλεκτρονικού "ψαρέματος".
        - Οι συγκεκριμένες **κόκκινες σημαίες** (π.χ. ασυνήθιστη γλώσσα, επείγοντα αιτήματα, ύποπτος σύνδεσμος).
        - Τα σωστά βήματα που πρέπει να ακολουθήσετε (π.χ. να μην κάνετε κλικ στον σύνδεσμο, να επικοινωνήσετε απευθείας με την τράπεζα).

Βήματα που πρέπει να ακολουθήσετε στο παιχνίδι ρόλων:

1. **Προσδιορίστε την ψηφιακή απειλή**:
    - Συζητήστε γιατί το μήνυμα ηλεκτρονικού ταχυδρομείου είναι επικίνδυνο:
        - Ύποπτος σύνδεσμος (π.χ., αιωρώντας το ποντίκι πάνω από το σύνδεσμο για να ελέγξετε την πραγματική διεύθυνση URL).
        - Επείγουσα γλώσσα που αποσκοπεί στην πρόκληση πανικού.
        - Έλλειψη προσωπικών στοιχείων (δεν αναφέρεται το πραγματικό όνομα του χρήστη).
2. **Στρατηγική αντίδρασης**:
    - Ο συμμετέχων 2 θα πρέπει να καθοδηγήσει τον συμμετέχοντα 1 στα εξής:
        - **Μην κάνετε κλικ σε συνδέσμους** και μην κατεβάζετε συνημμένα αρχεία.
        - **Αναφέρετε το μήνυμα ηλεκτρονικού ταχυδρομείου** ως phishing στον πάροχο ηλεκτρονικού ταχυδρομείου.
        - **Επικοινωνήστε απευθείας με την τράπεζα** χρησιμοποιώντας τα επίσημα κανάλια επικοινωνίας για να εξακριβώσετε αν το αίτημα είναι νόμιμο.
        - **Διαγράψτε το μήνυμα ηλεκτρονικού ταχυδρομείου** αφού το αναφέρετε.

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.

Ενημέρωση:

- Μετά την ολοκλήρωση του παιχνιδιού ρόλων, κάθε ζεύγος θα πρέπει να παρουσιάσει εν συντομία:
    - Οι **κόκκινες σημαίες** που εντόπισαν στο phishing email.
    - Τα **μέτρα** που έλαβαν για να χειριστούν την κατάσταση και να προστατεύσουν την ψηφιακή τους ταυτότητα.
- Διευκόλυνση μιας **ομαδικής συζήτησης** σχετικά με:
    - **Τι κάνει τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing αποτελεσματικά;**
    - **Ποια είναι άλλα παραδείγματα προσπαθειών phishing** που έχουν αντιμετωπίσει οι συμμετέχοντες;

Ρόλος συντονιστή:

- Βεβαιωθείτε ότι οι συμμετέχοντες κατανοούν τον σκοπό της άσκησης.
- Ενθαρρύνετε τον "ειδικό" σε θέματα κυβερνοασφάλειας να εξηγεί με σαφήνεια πώς να αναγνωρίζει τις απόπειρες ηλεκτρονικού "ψαρέματος" και να καθοδηγεί τον χρήστη.
- Ολοκληρώστε ενισχύοντας τις βέλτιστες πρακτικές για την **ψηφιακή ασφάλεια** και **τον τρόπο αντίδρασης σε απειλές phishing**.

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.