Τίτλος Δραστηριότητας: Μελέτη περίπτωσης - Κλοπή ψηφιακής ταυτότητας

Στόχος:

Να βοηθήσει τους συμμετέχοντες να κατανοήσουν τις συνέπειες της κλοπής ψηφιακής ταυτότητας, να εντοπίσουν τα λάθη ασφαλείας και να μάθουν τα βήματα για την πρόληψη και την αποκατάσταση.

Διάρκεια:

30 λεπτά

Απαιτούμενα υλικά:

- **Εκτυπωμένα αντίγραφα** ή **ψηφιακή προβολή** του σεναρίου της μελέτης περίπτωσης.
- **Σημειωματάρια και στυλό** για σημειώσεις κατά τη διάρκεια της ομαδικής συζήτησης.

Σενάριο:

Η διαδικτυακή ταυτότητα ενός χρήστη εκλάπη αφού χρησιμοποίησε μια **μη ασφαλή δημόσια σύνδεση Wi-Fi** σε μια καφετέρια για να αποκτήσει πρόσβαση στον τραπεζικό του λογαριασμό. Ένας εισβολέας υπέκλεψε τη σύνδεση και έλαβε τα στοιχεία σύνδεσής τους. Τις επόμενες ημέρες, ο επιτιθέμενος χρησιμοποίησε την ψηφιακή ταυτότητα του ατόμου για να πραγματοποιήσει δόλιες αγορές και να πάρει δάνεια στο όνομα του χρήστη, βλάπτοντας σοβαρά το πιστωτικό του σκορ.

Οδηγίες:

1. **Σχηματισμός ομάδας**:
    - Χωρίστε τους συμμετέχοντες σε **μικρές ομάδες** των 3-5 ατόμων.
2. **Σημεία συζήτησης**:
    - Κάθε ομάδα θα διαβάσει το σενάριο και θα συζητήσει τις ακόλουθες ερωτήσεις:
        - **Ποια λάθη έκανε ο χρήστης που οδήγησαν στην κλοπή της ψηφιακής του ταυτότητας;**
            - Επικεντρωθείτε στη χρήση μη ασφαλούς δημόσιου Wi-Fi για πρόσβαση σε ευαίσθητους λογαριασμούς.

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.

- **Ποια μέτρα θα μπορούσαν να είχαν ληφθεί για να αποφευχθεί αυτό;**
    - Συζητήστε τις βέλτιστες πρακτικές, όπως η χρήση VPN, η ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων και η αποφυγή δημόσιου Wi-Fi για ευαίσθητες συναλλαγές.
- **Πώς μπορούν τα άτομα να ανακάμψουν από την κλοπή ψηφιακής ταυτότητας;**
    - Διερευνήστε βήματα όπως η επικοινωνία με χρηματοπιστωτικά ιδρύματα, το πάγωμα πιστώσεων και η καταγγελία της κλοπής στις αρχές.

3. **Βήματα που πρέπει να ακολουθήσετε στην ομαδική συζήτηση**:
    - **Βήμα 1**: Εντοπισμός των **λαθών ασφαλείας**:
        - Οι ομάδες θα πρέπει να επικεντρωθούν στην κακή απόφαση να χρησιμοποιήσουν μη ασφαλές δημόσιο Wi-Fi και άλλα πιθανά λάθη (π.χ. μη χρήση ελέγχου ταυτότητας δύο παραγόντων).
    - **Βήμα 2**: Καταιγισμός ιδεών **για προληπτικά μέτρα**:
        - Συζητήστε πρακτικούς τρόπους για την πρόληψη της κλοπής ψηφιακής ταυτότητας (π.χ. χρήση VPN, έλεγχος HTTPS, αποφυγή ευαίσθητων συναλλαγών σε δημόσιο Wi-Fi).
    - **Βήμα 3**: Συζητήστε **τα βήματα αποκατάστασης**:
        - Οι ομάδες θα πρέπει να προσδιορίσουν τα βασικά βήματα ανάκαμψης, όπως η επικοινωνία με την τράπεζα, το πάγωμα λογαριασμών και η παρακολούθηση των πιστωτικών αποτελεσμάτων. Μπορούν επίσης να μιλήσουν για τη σημασία της αναφοράς στις νομικές αρχές και της άμεσης αλλαγής των κωδικών πρόσβασης.

Ρόλος συντονιστή:

- Καθοδηγήστε τις ομάδες να επικεντρωθούν **στα λάθη που έγιναν** και στις **προληπτικές λύσεις**.
- Ενθαρρύνετε τους συμμετέχοντες να σκεφτούν κριτικά τα βήματα ανάκτησης και πώς θα μπορούσαν να έχουν προστατεύσει την ψηφιακή τους ταυτότητα.
- Να είστε διαθέσιμοι να απαντήσετε σε ερωτήσεις και να διευκρινίσετε τις βέλτιστες πρακτικές.

Απολογισμός (10 λεπτά):

- Μετά τις ομαδικές συζητήσεις, κάθε ομάδα θα μοιραστεί τα συμπεράσματά της:

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.

- Τα **λάθη** που εντοπίζονται στη συμπεριφορά του χρήστη.
- **Προληπτικά μέτρα που** θα έπρεπε να είχαν ληφθεί για την αποφυγή της ψηφιακής κλοπής ταυτότητας.
- **Βήματα αποκατάστασης** και ενέργειες σε περίπτωση κλοπής ταυτότητας.

- Διευκολύνετε μια **συζήτηση σε ολόκληρη την ομάδα** σχετικά με:
  - **Γιατί το δημόσιο Wi-Fi αποτελεί κίνδυνο;**
  - **Ποιες άλλες κοινές συμπεριφορές μπορούν να θέσουν σε κίνδυνο την ψηφιακή σας ταυτότητα;**
  - **Τι πρέπει να κάνουν τα άτομα μετά την παραβίαση της ψηφιακής τους ταυτότητας;**

Βασικά συμπεράσματα:

- Αποφύγετε την πρόσβαση σε ευαίσθητους λογαριασμούς σε δημόσιο Wi-Fi.
- Χρησιμοποιείτε πάντα ένα **VPN** ή περιμένετε μέχρι να είναι διαθέσιμο ένα **ασφαλές δίκτυο**.
- Προστατεύστε τους λογαριασμούς με **ισχυρούς κωδικούς πρόσβασης** και **έλεγχο ταυτότητας δύο παραγόντων**.
- Εάν συμβεί κλοπή ψηφιακής ταυτότητας, **ενεργήστε γρήγορα** για να ελαχιστοποιήσετε τη ζημιά, επικοινωνώντας με τα σχετικά ιδρύματα και δεσμεύοντας λογαριασμούς.

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.