



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ  
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Διοίκηση Ασφάλειας Πληροφοριακών  
Συστημάτων**

Αρ. Άσκησης - Τίτλος Άσκησης	<b>Σχεδιασμός μιας Ανθρωποκεντρικής Εκστρατείας Ευαισθητοποίησης για την Κυβερνοασφάλεια (Awareness Campaign)</b>
Όνομα φοιτητή - Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Γιαννίκος Παναγιώτης – ΜΠΚΕΔ24007
	Μπαλτζής Δημήτρης – ΜΠΚΕΔ24026
	Ραυτόπουλος Μάριος – ΜΠΚΕΔ24034
Ημερομηνία παράδοσης	25/02/25



## Εκφώνηση Άσκησης

Εργασία Γ': Σχεδιασμός μιας Ανθρωποκεντρικής Εκστρατείας Ευαισθητοποίησης για την Κυβερνοασφάλεια (Awareness Campaign)

Περιγραφή:

Σε αυτή την ομαδική εργασία, οι φοιτητές σε ομάδες θα σχεδιάσουν μια ολοκληρωμένη εκστρατεία (campaign) ευαισθητοποίησης για την κυβερνοασφάλεια, προσαρμοσμένη σε ένα συγκεκριμένο κοινό-στόχο (π.χ., υπαλλήλους μιας εταιρείας, φοιτητές ενός πανεπιστημίου ή το ευρύ κοινό). Η εκστρατεία θα πρέπει να επικεντρώνεται στην αντιμετώπιση των ανθρώπινων ευπαθειών στην κυβερνοασφάλεια, όπως οι επιθέσεις phishing, η διαχείριση κωδικών πρόσβασης, η κοινωνική μηχανική και οι ασφαλείς διαδικτυακές συμπεριφορές.

Η εργασία θα απαιτεί:

1. Ταυτοποίηση του κοινού: Ανάλυση των κοινών προκλήσεων και συμπεριφορών του επιλεγμένου κοινού σε θέματα κυβερνοασφάλειας.
2. Ανάπτυξη περιεχομένου: Δημιουργία εκπαιδευτικού υλικού όπως αφίσες, βίντεο ή διαδραστικό περιεχόμενο που καλύπτουν τις ανάγκες του κοινού, προωθώντας παράλληλα βέλτιστες πρακτικές.
3. Συμπεριφορικές εκτιμήσεις: Εφαρμογή αρχών από την ψυχολογία της συμπεριφοράς και τους ανθρώπινους παράγοντες, ώστε η εκστρατεία να επηρεάζει αποτελεσματικά τις στάσεις και τις δράσεις.
4. Σχέδιο αξιολόγησης: Πρόταση μιας μεθόδου για την αξιολόγηση του αντίκτυπου της εκστρατείας, όπως μέσω ερευνών πριν και μετά ή μέσω προσομοιωμένων δοκιμών κυβερνοασφάλειας.

Τελικό παρουσίαση:

Θα είναι μια αναφορά που συνοψίζει το σχέδιο της εκστρατείας, τη λογική πίσω από αυτό, καθώς και μια παρουσίαση που θα αναδεικνύει το υλικό και τη στρατηγική. Στόχος είναι η ανάπτυξη πρακτικών, ανθρωποκεντρικών λύσεων για την ενίσχυση της ευαισθητοποίησης και της ανθεκτικότητας στην κυβερνοασφάλεια.

Υπάρχει η επιλογή να την κάνετε στα Αγγλικά ή στα Ελληνικά. Θα πρέπει να ανεβάσετε την PowerPoint παρουσίαση σας.



## Περιεχόμενα

1. Εισαγωγή .....	4
2. Ταυτοποίηση του κοινού: Ανάλυση των κοινών προκλήσεων και συμπεριφορών του επιλεγμένου κοινού σε θέματα κυβερνοασφάλειας .....	5
3. Ανάπτυξη περιεχομένου: Δημιουργία εκπαιδευτικού υλικού όπως αφίσες, βίντεο ή διαδραστικό περιεχόμενο που καλύπτουν τις ανάγκες του κοινού, προωθώντας παράλληλα βέλτιστες πρακτικές .....	6
3.1 Περιγραφή Εκστρατείας και Χρονοδιάγραμμα .....	6
3.2 Ανάλυση Περιεχομένου του Υλικού .....	6
3.2.1 Εκπαιδευτικό Υλικό (Infographics, Posters): .....	7
3.2.2 Διαδραστικό Υλικό (Quizzes & Phishing Simulations) .....	8
4. Συμπεριφορικές εκτιμήσεις: Εφαρμογή αρχών από την ψυχολογία της συμπεριφοράς και τους ανθρώπινους παράγοντες, ώστε η εκστρατεία να επηρεάζει αποτελεσματικά τις στάσεις και τις δράσεις .....	11
5. Σχέδιο αξιολόγησης: Πρόταση μιας μεθόδου για την αξιολόγηση του αντικτύπου της εκστρατείας, όπως μέσω ερευνών πριν και μετά ή μέσω προσομοιωμένων δοκιμών κυβερνοασφάλειας .....	12
5.1 Αρχική και Τελική Αξιολόγηση Γνώσεων .....	12
5.2 Συνεχής Παρακολούθηση της Εξέλιξης της Εκστρατείας .....	12
6. Επίλογος .....	13



## 1. Εισαγωγή

Στον σύγχρονο ψηφιακό κόσμο, η κυβερνοασφάλεια δεν αφορά μόνο τις τεχνολογικές λύσεις αλλά και τον ανθρώπινο παράγοντα. Έρευνες δείχνουν ότι το 90% των κυβερνοεπιθέσεων ξεκινούν από ανθρώπινα λάθη, όπως η απρόσεκτη διαχείριση κωδικών, η αλληλεπίδραση με phishing emails και η ελλιπής κατανόηση των κινδύνων.

Η παρούσα εκστρατεία ευαισθητοποίησης έχει σχεδιαστεί με στόχο τη μείωση των ανθρώπινων ευπαθειών στην κυβερνοασφάλεια και περιλαμβάνει:

Ταυτοποίηση του κοινού-στόχου – Ανάλυση των αναγκών και των αδυναμιών του κοινού σε θέματα ασφάλειας.

Ανάπτυξη εκπαιδευτικού περιεχομένου – Χρήση αφισών, βίντεο και διαδραστικών εργαλείων για την ενίσχυση της επίγνωσης.

Συμπεριφορικές εκτιμήσεις – Αξιοποίηση αρχών της ψυχολογίας για πιο αποτελεσματική αλλαγή νοοτροπίας και πρακτικών.

Σχέδιο αξιολόγησης – Καθορισμός δεικτών μέτρησης (KPIs) για την αποτίμηση της επιτυχίας της εκστρατείας.

Η εκστρατεία αυτή δεν αποτελεί απλά μια ενημερωτική καμπάνια, αλλά μια συστηματική προσπάθεια αλλαγής συμπεριφοράς που στοχεύει στην καλλιέργεια μιας ισχυρής κουλτούρας κυβερνοασφάλειας.



## 2. Ταυτοποίηση του κοινού: Ανάλυση των κοινών προκλήσεων και συμπεριφορών του επιλεγμένου κοινού σε θέματα κυβερνοασφάλειας

Για τη συγκεκριμένη εκστρατεία, επιλέγουμε ως κοινό-στόχο τους υπαλλήλους μιας ιδιωτικής εταιρείας, όπως μιας τράπεζας, η οποία περιλαμβάνει διαφορετικά τμήματα και ένα ευρύ φάσμα εργαζομένων (π.χ. ανθρώπινο δυναμικό, τραπεζικοί υπάλληλοι, λογιστήριο).

Το κοινό αυτό αποτελείται από άτομα ηλικίας 18 έως 67 ετών, με διαφορετικό επίπεδο εξοικείωσης στις τεχνολογίες και την κυβερνοασφάλεια. Ωστόσο, ως εργαζόμενοι σε έναν υψηλού κινδύνου τομέα, βρίσκονται συχνά στο στόχαστρο κυβερνοεπιθέσεων, όπως:

- **Phishing και κοινωνική μηχανική:** Οι επιτιθέμενοι εκμεταλλεύονται την ανθρώπινη αλληλεπίδραση για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.
- **Χρήση αδύναμων ή επαναλαμβανόμενων κωδικών πρόσβασης,** γεγονός που διευκολύνει επιθέσεις credential stuffing.
- **Απρόσεκτη αλληλεπίδραση με phishing emails και κακόβουλα συνημμένα,** αυξάνοντας την πιθανότητα παραβίασης του συστήματος.
- **Πρόσβαση σε ανασφαλείς ιστοτόπους μέσω επικίνδυνων συνδέσμων,** που μπορεί να οδηγήσει σε malware infections.
- **Ανεπαρκής ενημέρωση και εκπαίδευση σχετικά με τις κυβερνοαπειλές,** με αποτέλεσμα την αυξημένη ευπάθεια σε σύγχρονες τεχνικές επίθεσης.

Η εκστρατεία μας θα επικεντρωθεί στην ενίσχυση της ευαισθητοποίησης και της ανθεκτικότητας του προσωπικού απέναντι σε αυτές τις απειλές, χρησιμοποιώντας πρακτικές προσεγγίσεις που βασίζονται σε εκπαίδευση, διαδραστικότητα και αλλαγή συμπεριφοράς.

### 3. Ανάπτυξη περιεχομένου: Δημιουργία εκπαιδευτικού υλικού όπως αφίσες, βίντεο ή διαδραστικό περιεχόμενο που καλύπτουν τις ανάγκες του κοινού, προωθώντας παράλληλα βέλτιστες πρακτικές

#### 3.1 Περιγραφή Εκστρατείας και Χρονοδιάγραμμα

Η εκστρατεία μας βασίζεται στη διαδραστικότητα και την παιχνιδοποίηση ώστε να προσελκύσει την προσοχή των εργαζομένων και να ενισχύσει τη μάθηση. Μέσω πολλαπλών καναλιών επικοινωνίας (infographics, quizzes, phishing simulations), η εκπαίδευση θα είναι συνεχής, ελκυστική και προσαρμοσμένη στις καθημερινές προκλήσεις που αντιμετωπίζουν οι εργαζόμενοι. Παράλληλα, θα υπάρχει ένα σύστημα επιβράβευσης, το οποίο θα ενισχύει τη συμμετοχή και τη δέσμευση.

##### Χρονοδιάγραμμα Εκστρατείας

- **Ανάλυση κοινού & προετοιμασία υλικού:** 1 μήνας
- **Διάρκεια εκστρατείας:** 3, 6 ή 12 μήνες
  - Ημερήσια βάση: Εκπαίδευση μέσω infographics και posters
  - Εβδομαδιαία βάση: Διαδραστικό περιεχόμενο (Awareness Quizzes, Phishing Simulations)
- **Συστηματική αξιολόγηση:** Συλλογή στατιστικών και ανάλυση προόδου
- **Τελική αξιολόγηση:** Παρουσίαση συνολικών αποτελεσμάτων, 2 εβδομάδες μετά την ολοκλήρωση της εκστρατείας

#### 3.2 Ανάλυση Περιεχομένου του Υλικού

Το περιεχόμενο της εκστρατείας καλύπτει θεμελιώδεις και κρίσιμες πτυχές της κυβερνοασφάλειας που αφορούν το εργασιακό περιβάλλον, όπως:

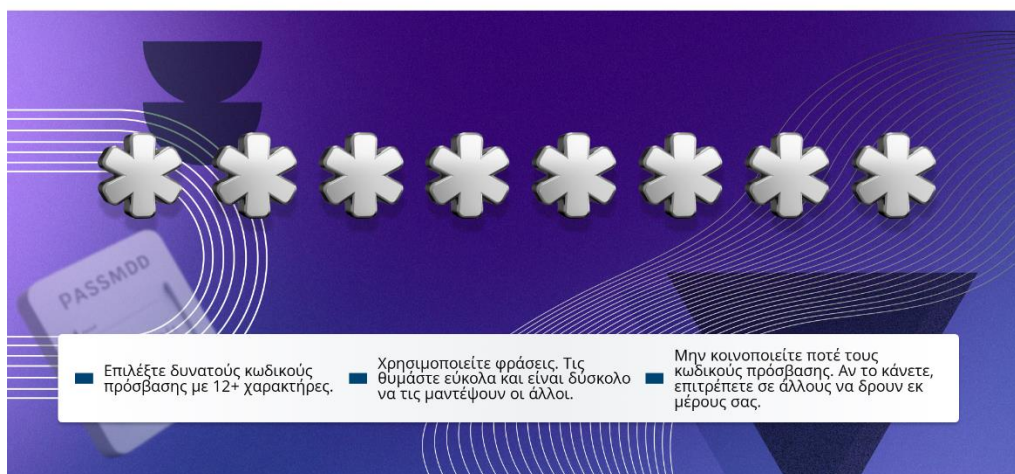
- Διαχείριση κωδικών πρόσβασης – Ενίσχυση της ασφάλειας με MFA & password managers
- Ασφαλής χρήση εξωτερικών συσκευών (USB, Hard Drives, Mobile Devices)
- Εντοπισμός και αντιμετώπιση phishing, smishing & vishing επιθέσεων
- Βέλτιστες πρακτικές backup και προστασία δεδομένων
- Διαχείριση ευαίσθητων δεδομένων στον εργασιακό χώρο
- Σωστή χρήση AI εργαλείων (LLMs) για αποφυγή διαρροής δεδομένων

### 3.2.1 Εκπαιδευτικό Υλικό (Infographics, Posters):

Το εκπαιδευτικό υλικό θα αποδίδεται μέσω:

- Infographics τα οποία θα τοποθετούνται σε monitor που θα βρίσκονται σε στρατηγικά σημεία της εταιρείας όπως (υποδοχή, διάδρομοι, κουζίνα, meeting rooms)
- Posters τα οποία θα τοποθετούνται σε αντίστοιχους χώρους.

#### Κωδικοί πρόσβασης: η πρώτη γραμμή άμυνας ενάντια στους εισβολείς



Εικόνα 1: Παράδειγμα εκπαιδευτικού υλικού με θέμα κωδικούς πρόσβασης

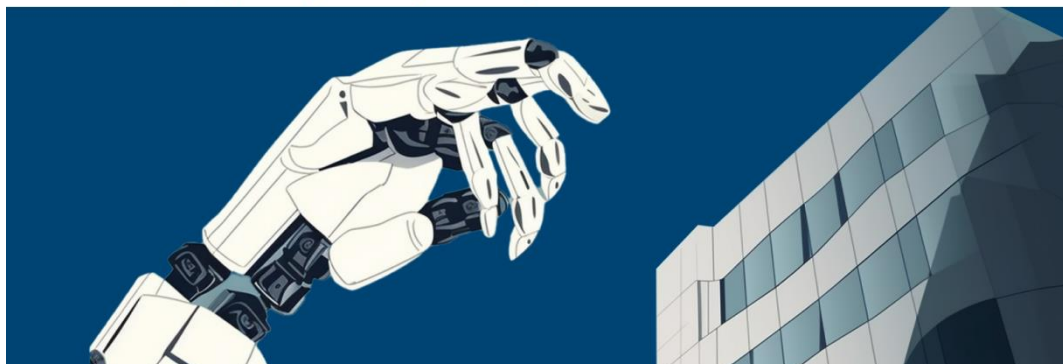
#### USB: κίνδυνος ασφάλειας στη δουλειά



Εικόνα 2: Παράδειγμα εκπαιδευτικού υλικού με θέμα ασφαλούς χρήσης USB



## Η τεχνητή νοημοσύνη (AI) μπορεί να μην καταστρέψει τον κόσμο, αλλά θα μπορούσε να καταστρέψει την εταιρία σας



**Βεβαιωθείτε ότι οι AI εντολές σας δεν περιλαμβάνουν αυτά τα τρία πράγματα:**

■ Προσωπικές πληροφορίες (ονόματα, διευθύνσεις email, ημερομηνίες γέννησης, κτλ.).

■ Οικονομικές πληροφορίες της εταιρίας, κώδικα πηγής ή οποιαδήποτε εσωτερική επικοινωνία.

■ Οποιοδήποτε περιεχόμενο σχετικό με την στρατηγική της εταιρίας (για παράδειγμα πρακτικά συναντήσεων).

Εικόνα 3: Παράδειγμα εκπαιδευτικού υλικού με θέμα χρήση AI εργαλείων

### 3.2.2 Διαδραστικό Υλικό (Quizzes & Phishing Simulations)

#### 1η Περίπτωση: Awareness Emails/Quizzes

- Οι εργαζόμενοι λαμβάνουν email με μια ερώτηση σχετικά με ένα θέμα κυβερνοασφάλειας (π.χ. "Είναι ασφαλής αυτός ο κωδικός;")
- Μόλις απαντήσουν, μεταφέρονται σε landing page με εξήγηση της σωστής απάντησης και σχετικό εκπαιδευτικό βίντεο

### Συμβουλές ασφάλειας

#### Έλεγχος ταυτότητας πολλών παραγόντων

Στην ψηφιακή εποχή, η μη εξουσιοδοτημένη πρόσβαση στα email, τους τραπεζικούς λογαριασμούς, τα μέσα κοινωνικής δικτύωσης ή τους αποθηκευτικούς χώρους στο cloud ενδέχεται να έχει σοβαρές συνέπειες. Για να περιορίσετε τον κίνδυνο, η χρήση ελέγχου ταυτότητας πολλών παραγόντων (MFA) είναι μια αποτελεσματική και εύκολη λύση. Ακολουθούν μερικές συμβουλές για το πώς να το εφαρμόσετε σωστά:

Συνδεθείτε σε όλους τους σημαντικούς λογαριασμούς σας και βεβαιωθείτε ότι ο έλεγχος ταυτότητας πολλών παραγόντων είναι ενεργοποιημένος παντού (από τις ρυθμίσεις λογαριασμού).

Χρησιμοποιείτε βιομετρικό έλεγχο ταυτότητας ή app ελέγχου ταυτότητας για μέγιστα επίπεδα ασφάλειας σε ευαίσθητους λογαριασμούς (με SMS ή email).

Χρησιμοποιείτε διαφορετικούς τρόπους ελέγχου ταυτότητας (όπως κινητό, διεύθυνση email ή βιομετρικά στοιχεία) για τους λογαριασμούς σας για να περιορίσετε τις επιπτώσεις απώλειας ή κλειδώματος κάποιου τρόπου.



# Ερώτηση κουίζ

Ο έλεγχος ταυτότητας πολλών παραγόντων προστατεύει τον λογαριασμό σας

ΣΩΣΤΟ

ΛΑΘΟΣ

Εικόνα 4: Παράδειγμα Awareness email με quiz

## ΑΚΡΙΒΩΣ!

Η προσθήκη του ελέγχου ταυτότητας πολλών παραγόντων (MFA) στους λογαριασμούς σας είναι ένας απλός και αποτελεσματικός τρόπος να τους προστατεύσετε από μη εξουσιοδοτημένη χρήση. Ακολουθούν μερικές συμβουλές για το πώς να το εφαρμόσετε σωστά:

Συνδεθείτε σε όλους τους σημαντικούς λογαριασμούς σας και βεβαιωθείτε ότι ο έλεγχος ταυτότητας πολλών παραγόντων είναι ενεργοποιημένος παντού (από τις ρυθμίσεις λογαριασμού).

Χρησιμοποιείτε βιομετρικό έλεγχο ταυτότητας ή app ελέγχου ταυτότητας για μέγιστα επίπεδα ασφάλειας σε ευαίσθητους λογαριασμούς (με SMS ή email).

Εικόνα 5: Παράδειγμα landing page με σωστή απάντηση στο quiz

## ΜΠΟΡΕΙΤΕ ΝΑ ΤΑ ΠΑΤΕ ΚΑΛΥΤΕΡΑ ΤΗΝ ΕΠΟΜΕΝΗ ΦΟΡΑ...

Η προσθήκη του ελέγχου ταυτότητας πολλών παραγόντων (MFA) στους λογαριασμούς σας είναι ένας απλός και αποτελεσματικός τρόπος να τους προστατεύσετε από μη εξουσιοδοτημένη χρήση. Ακολουθούν μερικές συμβουλές για το πώς να το εφαρμόσετε σωστά:

Συνδεθείτε σε όλους τους σημαντικούς λογαριασμούς σας και βεβαιωθείτε ότι ο έλεγχος ταυτότητας πολλών παραγόντων είναι ενεργοποιημένος παντού (από τις ρυθμίσεις λογαριασμού).

Χρησιμοποιείτε βιομετρικό έλεγχο ταυτότητας ή app ελέγχου ταυτότητας για μέγιστα επίπεδα ασφάλειας σε ευαίσθητους λογαριασμούς (με SMS ή email).

Χρησιμοποιείτε διαφορετικούς τρόπους ελέγχου ταυτότητας (όπως κινητό, διεύθυνση email ή βιομετρικά στοιχεία) για τους λογαριασμούς σας για να περιορίσετε τις επιπτώσεις απώλειας ή κλειδώματος κάποιου τρόπου.

Σε σημαντικούς λογαριασμούς, ρυθμίστε εναλλακτικό τρόπο ελέγχου ταυτότητας σε περίπτωση που ο αρχικός τρόπος δεν σας παρέχει πρόσβαση ή έχει χαθεί.

Εικόνα 6: Παράδειγμα landing page με λάθος απάντηση στο quiz

## 2η Περίπτωση: Phishing Simulations

- Οι εργαζόμενοι λαμβάνουν ρεαλιστικά phishing emails
- Αν κάνουν κλικ σε σύνδεσμο ή ανοίξουν επισυναπτόμενο αρχείο, μεταφέρονται σε landing page που αναλύει τα ύποπτα σημεία του email και προβάλλει εκπαιδευτικό βίντεο

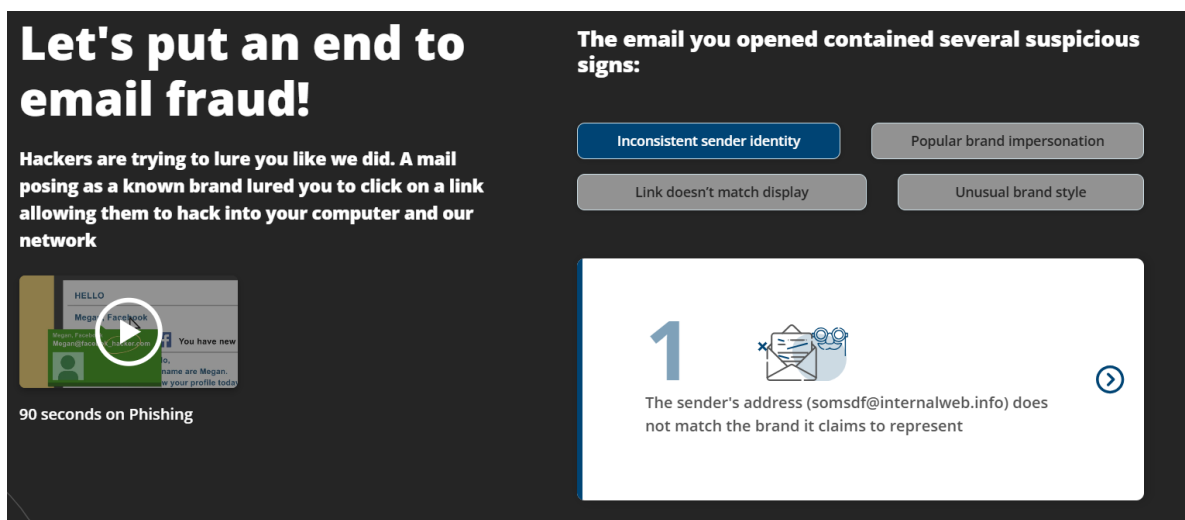
WhatsApp

*We identified an Unusual account activities on your account.*

Please go to your activity page to let us know whether or not this was you  
To help keep you safe, we require an extra security challenge

Review recent activity

Εικόνα 7: Παράδειγμα phishing email



Εικόνα 8: Παράδειγμα landing page μετά το phishing email

Αυτή η πολυεπίπεδη προσέγγιση εξασφαλίζει ότι η εκστρατεία δεν θα είναι παθητική, αλλά θα επιφέρει πραγματική αλλαγή στη συμπεριφορά των εργαζομένων, ενισχύοντας την ανθεκτικότητα της εταιρείας απέναντι στις κυβερνοαπειλές.

#### 4. Συμπεριφορικές εκτιμήσεις: Εφαρμογή αρχών από την ψυχολογία της συμπεριφοράς και τους ανθρώπινους παράγοντες, ώστε η εκστρατεία να επηρεάζει αποτελεσματικά τις στάσεις και τις δράσεις.

Η επιτυχία μιας εκστρατείας ευαισθητοποίησης στην κυβερνοασφάλεια εξαρτάται σε μεγάλο βαθμό από το πώς οι συμμετέχοντες αντιλαμβάνονται, απορροφούν και εφαρμόζουν τις γνώσεις που λαμβάνουν. Για τον λόγο αυτό, εφαρμόζουμε αρχές της ψυχολογίας της συμπεριφοράς και των ανθρώπινων παραγόντων, ώστε να ενισχύσουμε τη διαδραστικότητα και τη συμμετοχή των υπαλλήλων.

Τα βασικά στοιχεία που υιοθετούμε είναι:

- **Gamification (Παιχνιδοποίηση):** Το εκπαιδευτικό και διαδραστικό περιεχόμενο παρουσιάζεται σε μορφή σύντομων, engaging παιχνιδιών με απλά, ελκυστικά γραφικά. Με αυτόν τον τρόπο, το μάθημα γίνεται πιο ενδιαφέρον και αποφεύγεται η κόπωση από τη συμβατική εκπαίδευση.
- **Απλότητα και Καθημερινή Γλώσσα:** Η πληροφορία παρέχεται σε σύντομη και περιεκτική μορφή, αποφεύγοντας εξειδικευμένη ορολογία και τεχνικές λεπτομέρειες που μπορεί να κουράσουν το μη εξοικειωμένο κοινό.
- **Πρόγραμμα Επιβράβευσης:** Οι συμμετέχοντες που πετυχαίνουν υψηλές βαθμολογίες στα κουίζ ή επιδεικνύουν αυξημένη εγρήγορση (π.χ. δεν πέφτουν θύματα phishing simulations) λαμβάνουν ανταμοιβές (π.χ. badges, αναγνώριση από την εταιρεία ή ακόμα και μικρά έπαθλα). Έτσι, ενισχύουμε τη θετική ενίσχυση και διατηρούμε τη δέσμευση των υπαλλήλων με την εκστρατεία.
- **Συνεχόμενη Ενασχόληση μέσω της διαρκούς εκπαίδευσης και ενημέρωσης**

Η ενσωμάτωση αυτών των στοιχείων διασφαλίζει ότι η εκπαίδευση δεν αντιμετωπίζεται ως υποχρέωση αλλά ως μια ενδιαφέρουσα και ωφέλιμη διαδικασία, οδηγώντας σε πραγματική αλλαγή συμπεριφοράς.



## 5. Σχέδιο αξιολόγησης: Πρόταση μιας μεθόδου για την αξιολόγηση του αντικτύπου της εκστρατείας, όπως μέσω ερευνών πριν και μετά ή μέσω προσομοιωμένων δοκιμών κυβερνοασφάλειας.

Η αποτελεσματικότητα της εκστρατείας μας κρίνεται από την ικανότητά της να αλλάξει συμπεριφορές και να βελτιώσει την ευαισθητοποίηση των εργαζομένων σε θέματα κυβερνοασφάλειας. Για να το διασφαλίσουμε, εφαρμόζουμε μεθόδους ποσοτικής και ποιοτικής αξιολόγησης, επιτρέποντας μια αντικειμενική μέτρηση της προόδου.

### 5.1 Αρχική και Τελική Αξιολόγηση Γνώσεων

Πριν από την έναρξη της εκστρατείας, διεξάγεται ένα γενικό τεστ γνώσεων μέσω ερωτηματολογίου. Αυτό μας παρέχει μια αρχική εικόνα του επιπέδου κυβερνοασφάλειας στον οργανισμό.

Μετά την ολοκλήρωση της εκστρατείας, επαναλαμβάνεται η ίδια αξιολόγηση, επιτρέποντάς μας να συγκρίνουμε τα αποτελέσματα και να ποσοτικοποιήσουμε τη βελτίωση.

### 5.2 Συνεχής Παρακολούθηση της Εξέλιξης της Εκστρατείας

Καθ' όλη τη διάρκεια της εκστρατείας, συλλέγουμε δεδομένα σχετικά με τη συμμετοχή και τη δέσμευση των εργαζομένων, χρησιμοποιώντας:

- **Στατιστικά αλληλεπίδρασης με το διαδραστικό περιεχόμενο**
  - Click rates και engagement στα Awareness Quizzes
  - Ανάλυση σωστών/λάθος απαντήσεων
- **Αξιολόγηση Phishing Simulations**
  - Παρακολούθηση των χρηστών που έπεσαν θύματα του simulated phishing
  - Καταγραφή των αναφορών ύποπτων email

Τα παραπάνω δεδομένα μας επιτρέπουν να προσαρμόζουμε την εκστρατεία σε πραγματικό χρόνο, εστιάζοντας σε αδυναμίες που εμφανίζονται στην πορεία.

**Τελικός Στόχος:** Να υπάρχει μια μετρήσιμη βελτίωση στη συμπεριφορά των χρηστών και μια πιο ανθεκτική εταιρική κουλτούρα απέναντι στις κυβερνοαπειλές.



## 6. Επίλογος

Η κυβερνοασφάλεια είναι μια συλλογική ευθύνη και απαιτεί συνεχή εκπαίδευση και επαγρύπνηση. Μέσα από αυτή την εκστρατεία, επιδιώκουμε να κάνουμε την ασφάλεια κομμάτι της καθημερινότητας του κοινού-στόχου, όχι μέσα από τον φόβο, αλλά μέσω της ενημέρωσης και της ενδυνάμωσης.

Με τη χρήση στοχευμένου περιεχομένου, τεχνικών ψυχολογικής επιρροής και εργαλείων αξιολόγησης, η καμπάνια αυτή στοχεύει στην ουσιαστική βελτίωση της ανθεκτικότητας απέναντι στις κυβερνοαπειλές.

Τελικός στόχος δεν είναι απλώς η θεωρητική γνώση, αλλά η πρακτική αλλαγή συμπεριφοράς, που θα προστατεύσει τόσο τα άτομα όσο και τους οργανισμούς από κακόβουλες επιθέσεις.

Αυτή η προσπάθεια δεν σταματά εδώ. Η κυβερνοασφάλεια είναι ένας διαρκής αγώνας και η εκπαίδευση είναι το πιο ισχυρό μας όπλο.