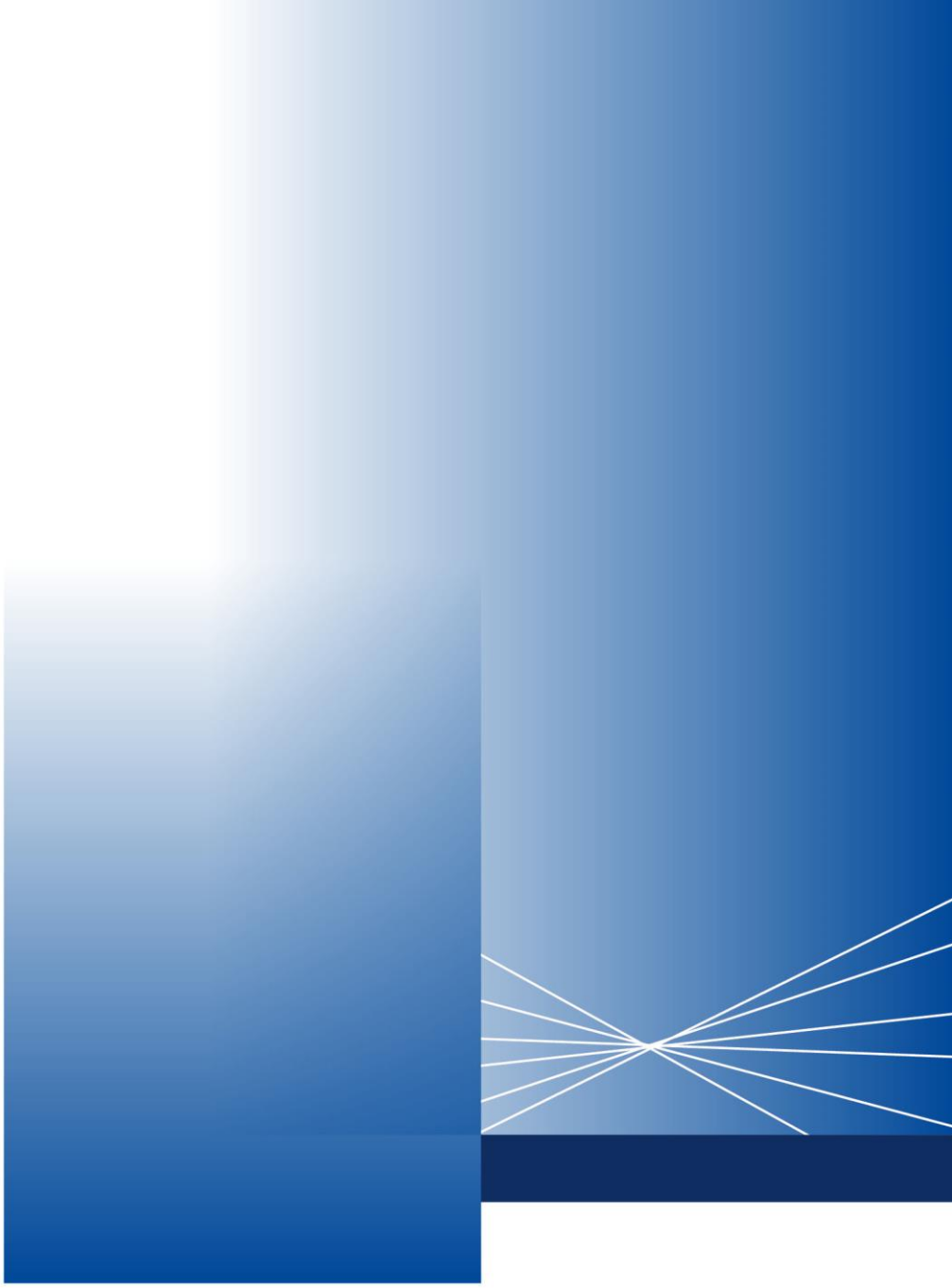
ΑΑΔΕ
Ανεξάρτητη Αρχή Δημοσίων Εσόδων

ΥΠΗΡΕΤΟΥΜΕ ΠΙΣΤΑ
ΔΗΜΟΣΙΟ ΣΥΜΦΕΡΟΝ
ΚΟΙΝΩΝΙΚΟ ΣΥΝΟΛΟ



Οδηγός προστασίας πολιτών από επιθέσεις με παραπλανητικά μηνύματα SMS για την υποκλοπή προσωπικών στοιχείων (SMISHING)

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2023

1. Ε **Τι είναι το SMISHING;**

Α Με το όρο **SMISHING** ορίζεται η απόπειρα υποκλοπής προσωπικών στοιχείων, όπως όνομα, ΑΦΜ, ημερομηνία γέννησης, τραπεζικοί λογαριασμοί ή κωδικοί πρόσβασης πολιτών με παραπλανητικά μηνύματα (SMS) σε κινητές συσκευές, από υποτιθέμενες έμπιστες οντότητες (σε αντιστοιχία με το ηλεκτρονικό ψάρεμα «PHISHING», όπου αποστέλλονται παραπλανητικά e-mails αντί SMS). Τα **παραπλανητικά** αυτά μηνύματα συνήθως περιέχουν κάποιο **link** προς έναν **πλαστό** ιστότοπο.

2. Ε **Έχει αναφερθεί κάποια πρόσφατη επίθεση;**

Α **Ναι**, το τελευταίο διάστημα, σε συνεργασία με τις αρμόδιες αρχές, διαπιστώθηκαν κακόβουλες ενέργειες αποστολής παραπλανητικών μηνυμάτων SMS σε κινητές συσκευές (SMISHING), που **αφορούν την ΑΑΔΕ**, και έχουν στόχο την υποκλοπή προσωπικών στοιχείων πολιτών και στοιχείων τραπεζικών καρτών.

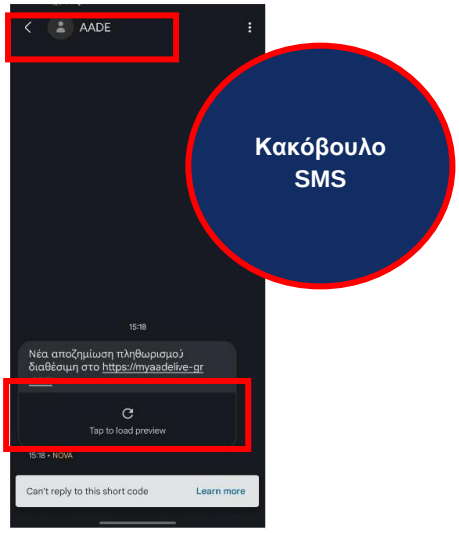
3. Ε **Πώς θα αναγνωρίσω τα κακόβουλα μηνύματα SMS;**

Α Τα κακόβουλα μηνύματα SMS:

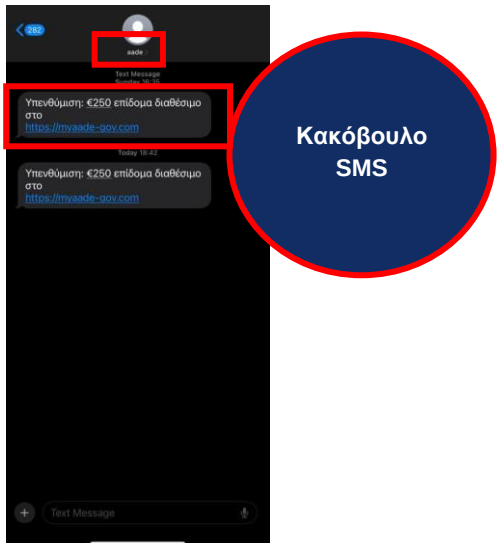
- Φαίνεται σαν να **αποστέλλονται** από την **ΑΑΔΕ** ή κάποια άλλη αξιόπιστη οντότητα
- Παροτρύνουν τους παραλήπτες να **συνδεθούν μέσω link** σε κάποια **πλαστή** ιστοσελίδα

Για παράδειγμα, τα μηνύματα πρόσφατης επίθεσης SMISHING που αφορούν την ΑΑΔΕ:

- Εμφάνιζαν ως αποστολέα την AADE
- Ανέφεραν: **«Νέα αποζημίωση πληθωρισμού διαθέσιμη στο https://myaadelive-gr.com»** ή **«Υπενθύμιση: €250 επίδομα διαθέσιμο στο https://myaade-gov.com»**
- Έμοιαζαν με τα SMS της παρακάτω εικόνας:



Παραπλανητικό SMS 1



Παραπλανητικό SMS 2

4. Ε Α Τι θα συμβεί αν πατήσω το link που αναγράφεται στο κακόβουλο μήνυμα;

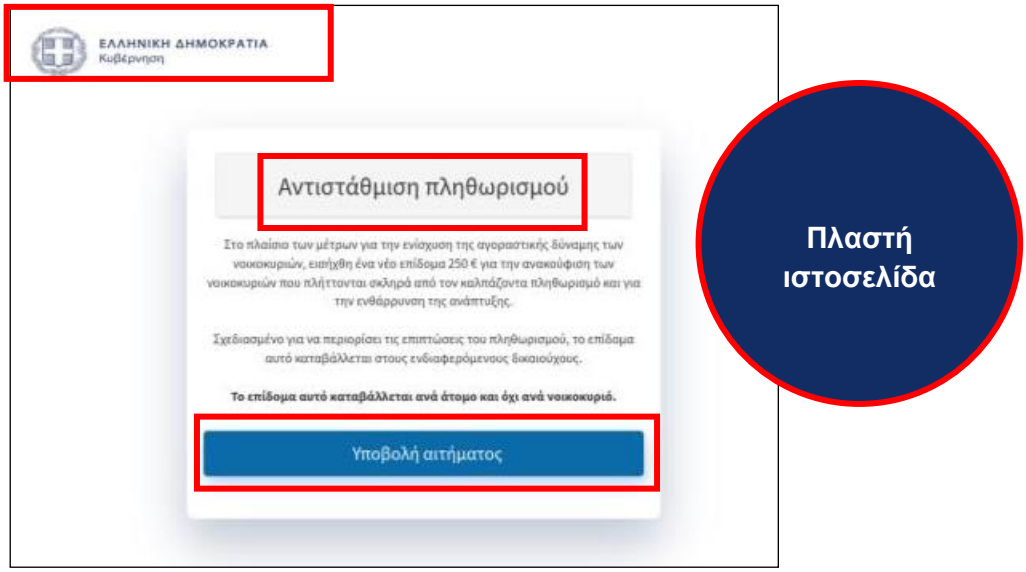
Πατώντας το συγκεκριμένο link του παραπάνω μηνύματος ο πολίτης κατευθύνεται σε **πλαστή** ιστοσελίδα, που τον ενημερώνει πως δικαιούται **επίδομα** και τον προτρέπει να υποβάλει αίτημα, συμπληρώνοντας τα προσωπικά του στοιχεία (Ονοματεπώνυμο, ΑΦΜ, κωδικούς Taxis, Στοιχεία Τραπεζών, κ.λπ.).

Επισημαίνεται ότι η **πλαστή** αυτή ιστοσελίδα:

- Είναι αρκετά αληθοφανής,
- Εμφανίζει το λογότυπο της Ελληνικής Δημοκρατίας και του Gov.gr και
- Κάνει σωστή χρήση της ελληνικής γλώσσας.

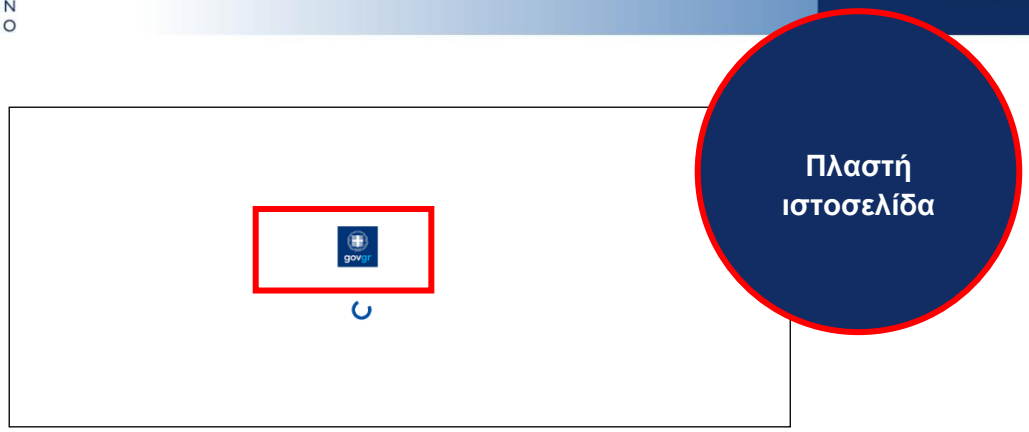
Ακολουθούν φωτογραφίες και σύντομη περιγραφή από τα βήματα της **πλαστής** ιστοσελίδας.

1. Πατώντας το link του μηνύματος ο χρήστης κατευθύνεται σε **πλαστή** ιστοσελίδα της **ΑΑΔΕ** όπου ενημερώνεται πως δικαιούται επίδομα 250 € και προτρέπεται να υποβάλει αντίστοιχο αίτημα.



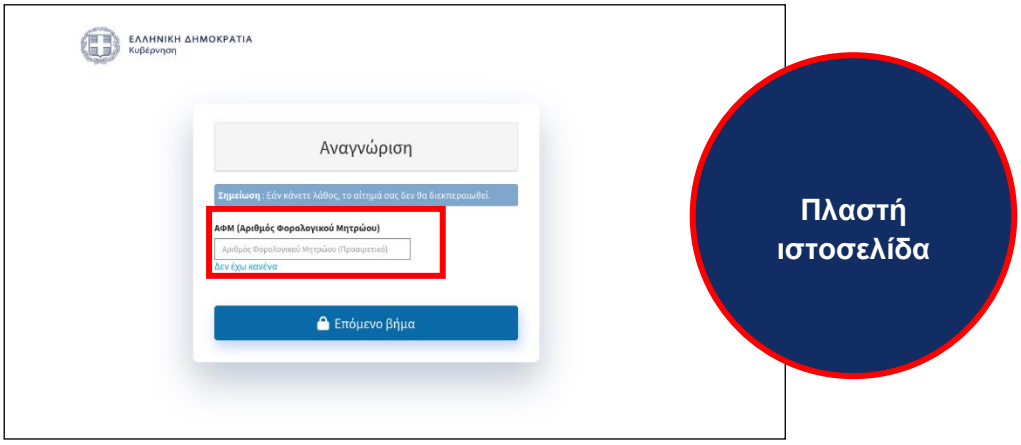
Πλαστή ιστοσελίδα 1 – Αρχική Σελίδα

2. Πατώντας **«Υποβολή αιτήματος»** εμφανίζεται η φόρμα εισαγωγής προσωπικών στοιχείων του πολίτη. Στην φόρμα απεικονίζεται το λογότυπο του gov.gr.



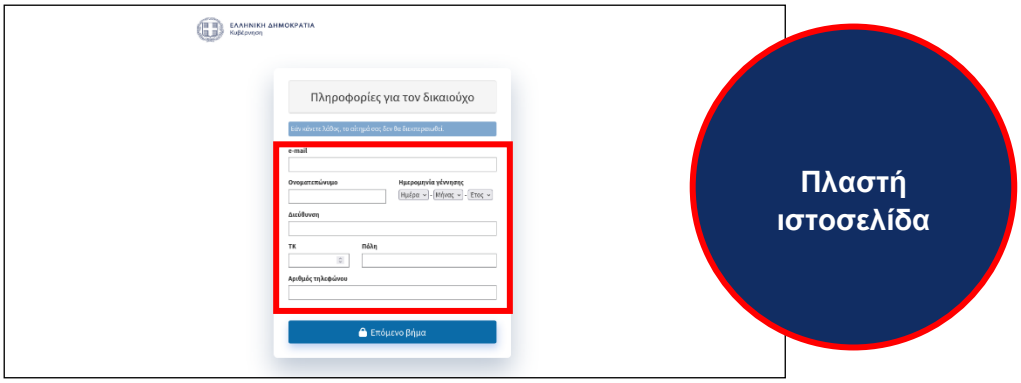
Πλαστή ιστοσελίδα 2 - Λογότυπο Gov.gr

3. Αρχικά ζητείται από τον πολίτη να εισάγει τον **Αριθμό του Φορολογικού του Μητρώου** (ΑΦΜ).



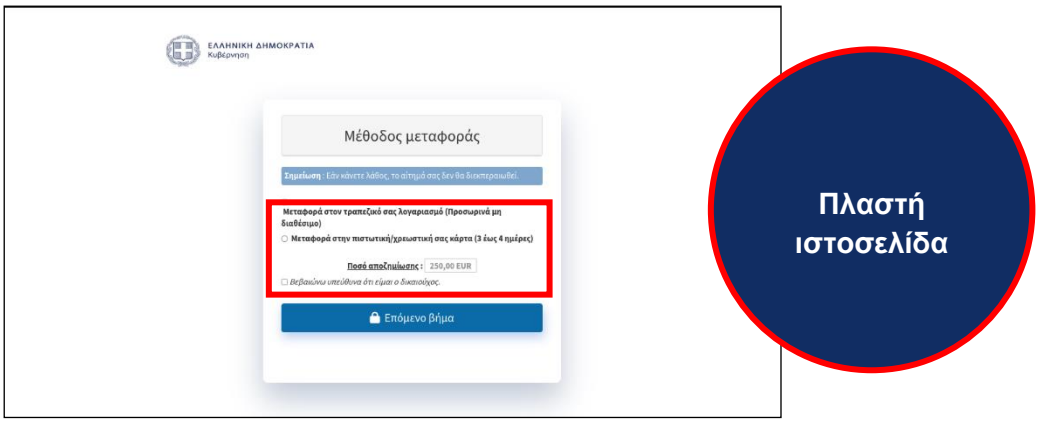
Πλαστή ιστοσελίδα 3 – Εισαγωγή ΑΦΜ

4. Στην συνέχεια ζητούνται τα προσωπικά στοιχεία του χρήστη: email, ονοματεπώνυμο, ημερομηνία γέννησης, διεύθυνση, ΤΚ, πόλη και αριθμός τηλεφώνου.



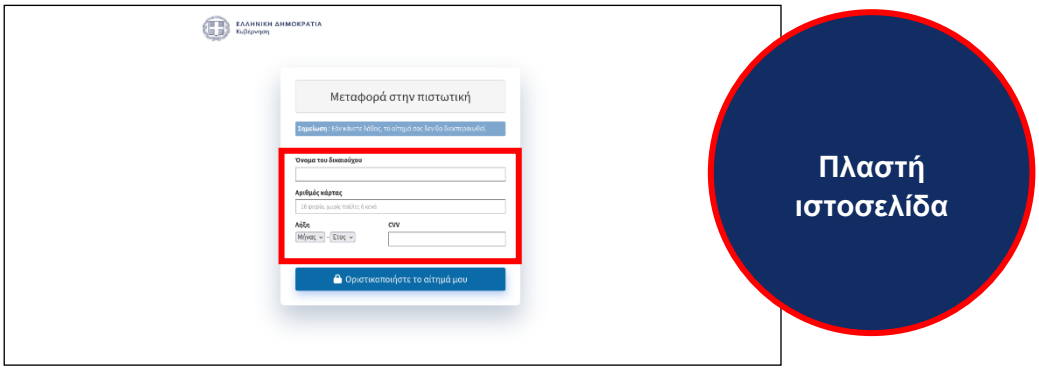
Πλαστή ιστοσελίδα 4 – Εισαγωγή προσωπικών στοιχείων

5. Έπειτα δίνεται η δυνατότητα επιλογής του τρόπου μεταφοράς του επιδόματος, είτε σε τραπεζικό λογαριασμό (που όμως η επιλογή αυτή αναφέρεται ως προσωρινά μη διαθέσιμη) είτε σε πιστωτική κάρτα.



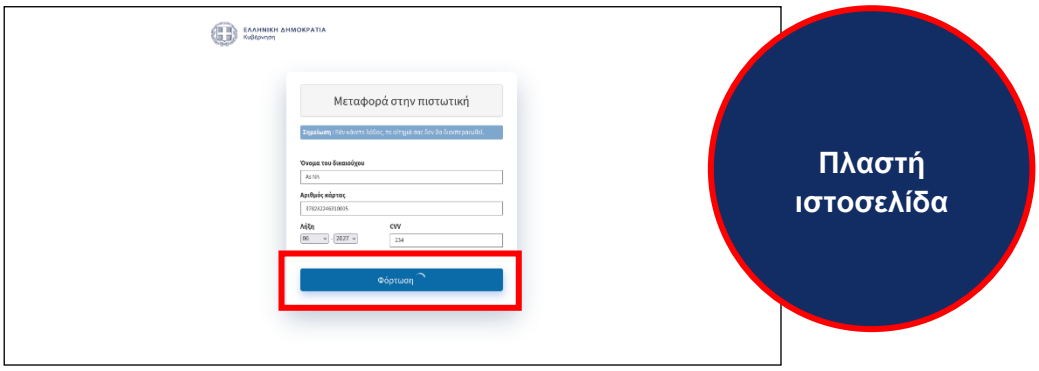
Πλαστή ιστοσελίδα 5 – Επιλογή μεθόδου μεταφοράς

6. Στο επόμενο βήμα ζητούνται τα στοιχεία της τραπεζικής του κάρτας (όνομα δικαιούχου, αριθμός κάρτας, ημ/νία λήξης, CVV)



Πλαστή ιστοσελίδα 6 Εισαγωγή στοιχείων τραπεζικής κάρτας

7. Πατώντας «Οριστικοποιήστε το αίτημά μου» τα στοιχεία αποστέλλονται στην **κακόβουλη ιστοσελίδα** και η διαδικασία σταματάει με την ένδειξη «φόρτωση».



Πλαστή ιστοσελίδα 7 – Τελευταία σελίδα

5. Ε Έλαβα κάποιο μήνυμα που μοιάζει ύποπτο. Τι πρέπει να κάνω;

Α Θα πρέπει να:

1. **ΜΗΝ** επιλέξετε κανένα προτεινόμενο σύνδεσμο (link)

2. **Διαγράψετε ΑΜΕΣΩΣ** το μήνυμα, καθώς είναι παραπλανητικό και οδηγεί σε **πλαστή** ιστοσελίδα της ΑΑΔΕ

3. **Να συνδέεστε** στην ψηφιακή πύλη myAADE μόνο από τη διεύθυνση myaade.gov.gr ή μέσω της επίσημης ιστοσελίδας της Ανεξάρτητης Αρχής Δημοσίων Εσόδων aade.gr.

4. Λάβετε υπ' όψιν ότι η Ανεξάρτητη Αρχή Δημοσίων Εσόδων **δεν θα σας ζητήσει, μέσω μηνύματος SMS ή μηνύματος ηλεκτρονικού ταχυδρομείου και για κανένα λόγο** να αποκαλύψετε προσωπικά σας στοιχεία, όπως όνομα, ΑΦΜ, ημερομηνία γέννησης, τραπεζικούς λογαριασμούς ή κωδικούς πρόσβασης (Username ή Password).

Να θυμάστε ότι ο αποτελεσματικότερος τρόπος προστασίας είναι η **ενημέρωση** ώστε να είστε σε θέση να αναγνωρίζετε πιθανές μορφές μηνυμάτων εξαπάτησης.

Μπορείτε να επισκέπτεστε την σελίδα **Ασφάλεια Ψηφιακών Υπηρεσιών και Συναλλαγών** στο επίσημο site της ΑΑΔΕ, στη διαδρομή *Αρχική σελίδα* > *Εξυπηρέτηση - Ενημέρωση* > *Ασφάλεια Ψηφιακών Δεδομένων* για χρήσιμες συμβουλές προστασίας και πρακτικές ενημέρωσης για τις ψηφιακές σας συναλλαγές.

Επιπλέον, στο θέμα **Απόπειρες υποκλοπής στοιχείων μέσω Μηνυμάτων Εξαπάτησης (Phishing)** στην προαναφερόμενη σελίδα, υπάρχουν πληροφορίες για να εντοπίζετε και να αντιμετωπίζετε και άλλες επιθέσεις ηλεκτρονικού «ψαρέματος».