

# Ασφάλεια στο διαδίκτυο.

Σε αυτή την ενότητα θα μάθετε πώς να χρησιμοποιείτε το διαδίκτυο με μεγαλύτερη ασφάλεια. Θα δείτε πώς να αναγνωρίζετε ύποπτα μηνύματα και απάτες, να προστατεύετε τα προσωπικά σας στοιχεία και να δημιουργείτε ασφαλείς κωδικούς πρόσβασης.

Βρείτε εκπαιδευτικό  
βίντεο στην  
ιστοσελίδα μας:



Ασφάλεια στο διαδίκτυο.

## **Αναγνώριση ψεύτικων μηνυμάτων Τράπεζας ή ΓεΣΥ.**

Τον τελευταίο καιρό, πολλοί άνθρωποι στην Κύπρο λαμβάνουν μηνύματα (SMS) που φαίνονται να προέρχονται από την τράπεζά τους ή από το ΓεΣΥ, αλλά στην πραγματικότητα είναι απάτη. Σκοπός τους είναι να σας κάνουν να πατήσετε έναν σύνδεσμο και να δώσετε τους κωδικούς ή τα στοιχεία της κάρτας σας.

## Αναγνώριση ψεύτικων μηνυμάτων Τράπεζας ή ΓεΣΥ.

Ακολουθούν τρόποι για να τα αναγνωρίζετε:

1

### Μηνύματα που σας βιάζουν

Λένε ότι κάτι «έχει πρόβλημα» ή «πρέπει να διορθωθεί αμέσως», για να σας κάνουν να ενεργήσετε χωρίς να σκεφτείτε.

2

### Σύνδεσμοι (links) μέσα στο μήνυμα

Ένα γνήσιο μήνυμα από τράπεζα ή το ΓεΣΥ δεν θα σας ζητήσει ποτέ να πατήσετε σε σύνδεσμο για να δώσετε τους κωδικούς σας.

3

### Αίτημα για προσωπικά στοιχεία

Ο Οργανισμός Ασφάλισης Υγείας (ΟΑΥ) και οι τράπεζες δεν ζητούν ποτέ κωδικούς πρόσβασης, στοιχεία κάρτας ή κωδικό μιας χρήσης (OTP) μέσω SMS ή email.

4

### Ορθογραφικά λάθη ή περίεργη διατύπωση

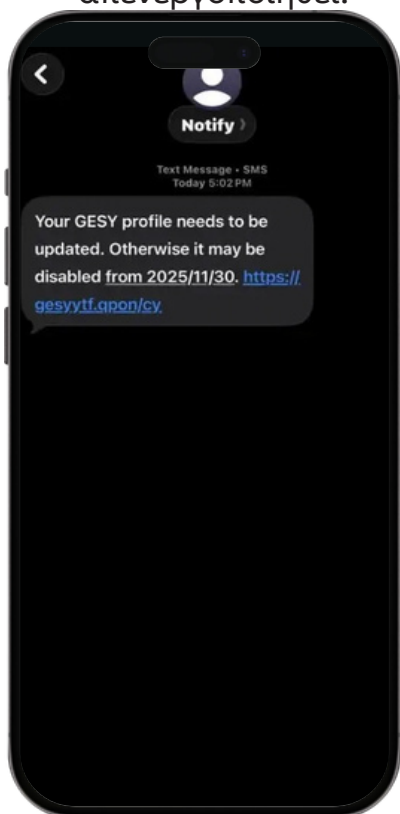
Τα ψεύτικα μηνύματα συχνά έχουν ορθογραφικά λάθη, περίεργη διατύπωση ή δεν απευθύνονται σε εσάς με το όνομά σας.

Ασφάλεια στο διαδίκτυο.

## Αναγνώριση ψεύτικων μηνυμάτων Τράπεζας ή ΓεΣΥ.

### Παραδείγματα απάτης

Σας ζητά να πατήσετε σε σύνδεσμο που περιλαμβάνεται σε SMS, ισχυριζόμενο ότι το προφίλ σας στο ΓεΣΥ χρειάζεται ενημέρωση και ότι, διαφορετικά, θα απενεργοποιηθεί.



Σας ζητά να καλέσετε έναν αριθμό που αναφέρεται σε SMS, ισχυριζόμενο ότι έγινε ύποπτη συναλλαγή στον τραπεζικό σας λογαριασμό.

