

Έχουν κλαπεί τα στοιχεία της πιστωτικής σας κάρτας ή τα τραπεζικά σας στοιχεία;



Κάθε μέρα, όλο και περισσότεροι άνθρωποι απολαμβάνουν την εμπειρία των διαδικτυακών αγορών.

Ωστόσο, οι αγοραστές πρέπει να παραμένουν προσεκτικοί, καθώς οι απατεώνες αναζητούν πάντα τρόπους για να κλέψουν στοιχεία πιστωτικών καρτών ή τραπεζικά στοιχεία!

Χρησιμοποιούν ψεύτικους ιστότοπους, εμφανίζονται ως πωλητές σε ιστότοπους πλειστηριασμών και μπορεί, επίσης, να στέλνουν ψευδή μηνύματα ηλεκτρονικού ταχυδρομείου (phishing), τα οποία υποτίθεται ότι προέρχονται από γνωστούς δικτυακούς τόπους πληρωμών ή λιανικής πώλησης.

Τι πρέπει να κάνετε;

Εάν ο τραπεζικός σας λογαριασμός έχει τεθεί σε κίνδυνο ή παρατηρείτε ασυνήθιστη δραστηριότητα στον λογαριασμό της πιστωτικής σας κάρτας, μπορείτε να λάβετε τα παρακάτω μέτρα:

1. Επικοινωνήστε αμέσως με το χρηματοπιστωτικό σας ίδρυμα για να μπλοκάρετε την πιστωτική/τραπεζική σας κάρτα. Ενδέχεται να μπορείτε να ζητήσετε επιστροφή των χρημάτων σας και να αποτρέψετε περαιτέρω κλοπές.



2. Αλλάξτε τους κωδικούς πρόσβασης. Ο απατεώνας ενδέχεται να έχει τον κωδικό πρόσβασής σας, συνεπώς αντικαταστήστε τον με ισχυρό κωδικό πρόσβασης 15 τουλάχιστον χαρακτήρων, συμπεριλαμβανομένων κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων.

Ενδεχομένως να είναι ευκολότερο να θυμάστε ένα συνθηματικό. Αυτό θα μπορούσε να είναι μια πρόταση που περιλαμβάνει ασυνήθιστες λέξεις, ή λέξεις από διαφορετικές γλώσσες.

Θα πρέπει επίσης να αλλάξετε τα στοιχεία σύνδεσης για κάθε άλλο λογαριασμό σας όπου χρησιμοποιείτε το ίδιο ή παρόμοιο όνομα χρήστη και κωδικό πρόσβασης.

Χρησιμοποιήστε έναν μοναδικό κωδικό πρόσβασης για κάθε λογαριασμό.



3. Ενημερώστε το λογισμικό ανίχνευσης ιών προκειμένου να καταπολεμήσετε νέους ιούς και να προστατεύσετε τη συσκευή σας.



63%

4. Αναφέρετε την απάτη. Οι πληροφορίες σας ενδέχεται να βοηθήσουν στη σύλληψη του απατεώνα και στην πρόληψη περαιτέρω περιστατικών.

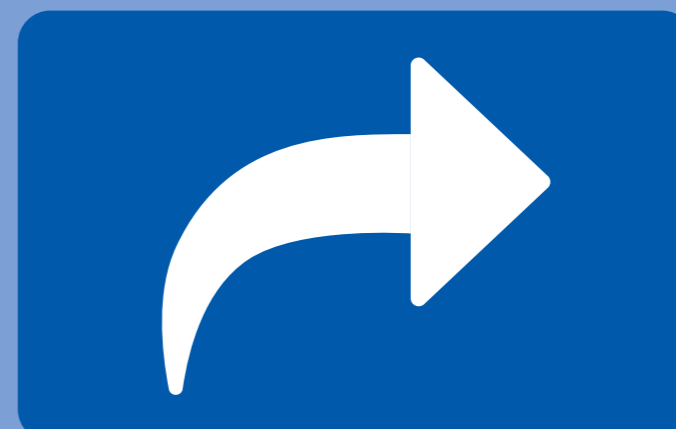
Για να μάθετε πού μπορείτε να λάβετε συμβουλές και να καταγγείλετε την αξιόποινη πράξη στη χώρα σας, επισκεφθείτε την ηλεκτρονική διεύθυνση <https://cybersecuritymonth.eu/cyber-first-aid>



5. Φροντίστε να φυλάξετε όλα τα αποδεικτικά στοιχεία που διαθέτετε για την κλοπή, π.χ. ηλεκτρονικά μηνύματα, τιμολόγια, αποδείξεις, αντίγραφο της διαφήμισης κ.λπ.



6. Μοιραστείτε την εμπειρία σας με την οικογένεια και τους φίλους σας για να συμβάλετε στην προστασία τους.



SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ



#CyberSecMonth

#ThinkB4UClick