ΣΧΟΛΕΙΟ: ΓΥΜΝΑΣΙΟ- ΓΕ.Λ. ΧΡΥΣΟΒΙΤΣΑΣ

Μάθημα: Ερευνητική Εργασία

Θέμα: Διαδικτυακές Αγορές και Ασφάλεια

Τάξη: Β’ Γενικού Λυκείου.
Έτος:2017-2018

Επιβλέπουσα καθηγήτρια: Γκορόγια Θεοδώρα ΠΕ86

Περιεχόμενα

Κεφάλαιο 1ο: Τα υπέρ των αγορών στο διαδίκτυο

Ενότητα 1:Από τη μεριά της ηλεκτρονικού εμπόρου

1)Μείωση του λειτουργικού κόστους: Ένα ηλεκτρονικό κατάστημα για να λειτουργήσει χρειάζεται πολύ μικρότερο κόστος σε σχέση με ένα συμβατικό. Ενοίκιο, λογαριασμοί κοινής ωφέλειας, μισθοδοσία προσωπικού, κόστος συστημάτων ασφάλειας, αποτελούν διαχρονικά σημαντικές επιβαρύνσεις για την λειτουργία μιας επιχείρησης. Τα ηλεκτρονικά καταστήματα μπορούν να έχουν πολύ χαμηλότερα κόστη λειτουργίας και συντήρησης.
2)Καλύτερη διαχείριση αποθεμάτων & διευκόλυνση προγραμματισμού: Η διατήρηση αποθεμάτων είναι ένα θέμα για όλες τις επιχειρήσεις καθώς απαιτεί την δέσμευση ενός κεφαλαίου. Με την χρήση του e-commerce, το απόθεμα αυτό ελαχιστοποιείται και συνεπακόλουθα μειώνεται και το κεφάλαιο που πρέπει να δεσμεύσει ο επιχειρηματίας.
3)Διεύρυνση της πελατειακής βάσης: Σε ένα δικτυακό κατάστημα δυνητικά μπορούν να έχουν πρόσβαση πελάτες από όλα τα σημεία του πλανήτη.
4)Μειωμένο κόστος marketing: Οι συμβατικοί τρόποι προώθησης ενός προϊόντος είναι συνήθως πιο ακριβοί σε σχέση με τους ηλεκτρονικούς. Ένα ηλεκτρονικό κατάστημα λειτουργεί και αυτοτελώς ως μέσο διαφήμισης. Πόσο μάλλον, όταν συνδυαστεί με άλλα εργαλεία ηλεκτρονικής διαφήμισης (χρήση social networks, Google AdWords και άλλα)
5)Αποτελεσματικότερο marketing: Το marketing με την χρήση των δικτυακών εργαλείων μπορεί εκτός από φτηνότερο να είναι και αποτελεσματικότερο, με αποτελέσματα απόλυτα μετρήσιμα. Το Διαδίκτυο είναι αμφίδρομο μέσο και έτσι μπορούν να αντλούνται χρήσιμες πληροφορίες για το προφίλ των καταναλωτών, κάτι που μπορεί να κατευθύνει καλύτερα τους υπεύθυνους marketing αλλά και τους επιχειρηματίες για την προσέλκυση υποψήφιων πελατών.

Ενότητα 2: Από τη μεριά του καταναλωτή

1) Βρίσκουμε αυτό που θέλουμε, όποτε θέλουμε, ακόμα κι αυτά που δεν ξέρουμε ότι θέλουμε με μερικά κλικ. Ούτε ατέλειωτες βόλτες σε αγορές, πολυκαταστήματα και μαγαζιά, ούτε χάσιμο χρόνου
2) Βρίσκουμε πράγματα που δεν θα τα δούμε στα ράφια και στις βιτρίνες καταστημάτων στην χώρα μας, ούτε που θα διαφημιστούν.
3) Βρίσκουμε λεπτομέρειες/χαρακτηριστικά και πληροφορίες του προϊόντος που ενδιαφερόμαστε, ώστε να μπορούμε να κάνουμε σύγκριση με άλλα ίδια ή αντίστοιχα που πρόκειται να ψωνίσουμε.
Με λίγα λόγια, μέσα σε μερικά λεπτά, με τον πιο εύκολο τρόπο, κάνουμε μια ολοκληρωμένη έρευνα αγοράς και αποφασίζουμε αποτελεσματικά τι θα ψωνίσουμε.

4) Παίρνουμε αυτό που πραγματικά πληρώνουμε, κι όχι αυτό που θα μας πλασάρει ο καθένας που έχει ένα κατάστημα, ως "μάρκα" ή ως "εξαιρετικό" προϊόν..."Made in China".
5) Βρίσκουμε ποικιλίες για πάρα πολλά προϊόντα, σε διάφορες τιμές και ποιότητες online.

Κεφάλαιο 2ο: Κίνδυνοι κατά τη διαδικασία online αγορών

Η διακίνηση προϊόντων και οι μεταφορές χρηματικών ποσών στο διαδίκτυο προσελκύουν σχεδόν πάντα το ενδιαφέρον **hackers** και **«διαδικτυακών απατεώνων»**, οι οποίοι προσπαθούν να αποκομίσουν παράνομα οφέλη με πολλούς και συχνά **ευρηματικούς τρόπους**.

1. Παραποίηση δεδομένων
2. Κακόβουλα προγράμματα
3. Ψάρεμα (phishing)
4. Άρνηση εξυπηρέτησης
5. Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών (hackin-cracking)
6. Υποκλοπή δεδομένων
7. Απατηλές συναλλαγές

Ενότητα1: Προσοχή στα προσωπικά σας δεδομένα

Η υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών,ης κ.λπ). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα (cracker) να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς, κ.λπ.

Κάποιοι θεωρούν τις Απάτες (Scams) ως ένα είδος υποκλοπής, μόνο που οι Απάτες συνήθως δεν ενδιαφέρονται για τις προσωπικές μας πληροφορίες, αλλά προσπαθούν να προκαλέσουν τον οίκτο μας για τον ανθρώπινο πόνο ώστε να προσφέρουμε λεφτά για να βοηθήσουμε ένα δήθεν καλό σκοπό. Για παράδειγμα, σχεδόν κάθε μεγάλη καταστροφή (σεισμός, πλημμύρες, πείνα, πόλεμος) έχει προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες να προσφέρουν λεφτά για να βοηθήσουν για κάποιο καλό σκοπό. Πολλοί άνθρωποι έχουν χάσει πολλά λεφτά για τέτοιους “καλούς” σκοπούς. Κάποιοι έχουν χάσει ακόμα και τη ζωή τους, καθώς έχουν ταξιδέψει σε άλλες χώρες για να γνωρίσουν αυτούς που επωφελούνταν των προσφορών τους.

<u>Πού μπορεί να συμβεί:</u>
1.Μέσω ηλεκτρονικών μηνυμάτων (e-mail) που ξεγελούν το χρήστη ώστε να οδηγηθεί σε πλαστές ιστοσελίδες.

2.Κατά το φυλλομέτρημα οποιασδήποτε σοβαρής ιστοσελίδας, η οποία έχει μολυνθεί απο ιο.
3.Κατά τη περιήγηση σε ιστοσελίδες με αναληθή προϊόντα και πληροφορίες.
4.Κατά τη χρήση οποιουδήποτε φυλλομετρητή Διαδικτύου, ο οποίος έχει μολυνθεί με πρόγραμμα που καταγράφει προσωπικές και οικονομικές πληροφορίες, τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν.

Ενότητα 2: Κακόβουλα προγράμματα

Υπάρχουν διάφοροι τύποι κακόβουλων προγραμμάτων όπως: ιοί (viruses), δούρειοι ίπποι (Trojan horses), σκουλήκια (worms) κ.α.

➔ Τα προγράμματα αυτά δρουν καταστροφικά στον υπολογιστή μας με διάφορους τρόπους όπως:

α) «Μολύνουν» άλλα προγράμματα του υπολογιστή μας και τα αναγκάζουν να μην λειτουργούν σωστά,

β) Διαγράφουν ή αλλοιώνουν αρχεία στον υπολογιστή μας,

γ)Μεταφέρουν στον υπολογιστή μας άλλα επιβλαβή προγράμματα,

δ) Δίνουν πρόσβαση στον υπολογιστή μας σε άλλους οι οποίοι μπορεί να τον χρησιμοποιήσουν για παράνομες ενέργειες,

ε) Γεμίζουν τον υπολογιστή μας με άχρηστα προγράμματα, τα οποία τον επιβραδύνουν ή σε ορισμένες περιπτώσεις σταματούν εντελώς τη λειτουργία του.

Ενότητα 3: Προσοχή στα Μηνύματα "Phishing"

Το ηλεκτρονικό ψάρεμα (phishing) συνήθως επιχειρείται μέσω μηνυμάτων ηλ. ταχυδρομείου, διαφημίσεων ή ιστοτόπων που μοιάζουν με εκείνους που ήδη χρησιμοποιείτε. Για παράδειγμα, κάποιος που επιχειρεί επίθεση ηλ. ψαρέματος μπορεί να σας στείλει μέσω ηλ. ταχυδρομείου ένα μήνυμα το οποίο μοιάζει να προέρχεται από την τράπεζά σας, ώστε να σας παρασύρει να αποκαλύψετε στοιχεία για τον τραπεζικό σας λογαριασμό.

Μηνύματα ή τοποθεσίες μέσω των οποίων επιχειρείται ηλ. ψάρεμα ενδέχεται να σας ζητήσουν τα εξής:

- Ονόματα χρήσης και κωδικοί πρόσβασης, περιλαμβανομένων αλλαγών στους κωδικούς πρόσβασης
- Αριθμούς κοινωνικής ασφάλισης
- Αριθμούς τραπεζικών λογαριασμών
- Κωδικούς PIN (Αριθμοί προσωπικής ταυτοποίησης)
- Αριθμούς πιστωτικών καρτών
- Το πατρικό της μητέρας σας

- Η ημερομηνία των γενεθλίων σας

Σημαντικό: Δεν θα σας ζητηθεί ποτέ από την Google ή το Gmail να δώσετε τέτοιου είδους πληροφορίες σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου.

Αναφορά μηνυμάτων ηλεκτρονικού ψαρέματος (phishing)

Όταν αναγνωρίσουμε κάποιο μήνυμα ως ύποπτο ή ως απόπειρα ηλ. ψαρέματος, ενδέχεται να σας εμφανίσουμε μια προειδοποίηση ή να μετακινήσουμε το μήνυμα στον φάκελο των Ανεπιθύμητων. Εάν κάποιο μήνυμα δεν έχει επισημανθεί σωστά, ακολουθήστε τα παρακάτω βήματα για να το επισημάνετε ως απόπειρα ηλ. ψαρέματος ή όχι.

Αποφύγετε τις επιθέσεις ηλ. ψαρέματος (phishing)

Να είστε πάντα προσεκτικοί σε περίπτωση μηνυμάτων από ιστοτόπους που ζητούν προσωπικά στοιχεία. Εάν λάβετε μηνύματα του είδους αυτού:

1. Μην κάνετε κλικ σε τυχόν συνδέσμους και μην υποβάλετε οποιαδήποτε προσωπικά στοιχεία, ωσότου βεβαιωθείτε ότι η διεύθυνση ηλ. ταχυδρομείου είναι πραγματική.
2. Αν ο αποστολέας έχει διεύθυνση Gmail, υποβάλετε μια αναφορά κατάχρησης του Gmail στην Google.

Σημείωση: Το Gmail δεν πρόκειται ποτέ να σας ζητήσει προσωπικά στοιχεία, όπως κωδικούς πρόσβασης, μέσω ηλ. ταχυδρομείου.

Όταν λαμβάνετε ένα μήνυμα που σας φαίνεται ύποπτο, να μερικά πράγματα που μπορείτε να προσέξετε:

- Ελέγξτε ότι η διεύθυνση ηλ. ταχυδρομείου και το όνομα του αποστολέα ταιριάζουν.
- Ελέγξτε αν το μήνυμα είναι επικυρωμένο μέσω ελέγχου ταυτότητας.
- Περάστε τον δείκτη του ποντικιού πάνω από οποιουσδήποτε συνδέσμους προτού κάνετε κλικ σε αυτούς. Εάν η διεύθυνση URL του συνδέσμου δεν ταιριάζει με την περιγραφή της σύνδεσης, μπορεί να σας οδηγεί σε μια ιστοσελίδα ηλ. ψαρέματος (phishing).
- Ελέγξτε τις κεφαλίδες του μηνύματος για να βεβαιωθείτε ότι για την κεφαλίδα "από" δεν εμφανίζεται κάποιο εσφαλμένο όνομα.

Κεφάλαιο 3ο: Τρόποι προστασίας

Ενότητα 1: Σιγουρευτείτε ότι το site που επιλέξατε είναι αξιόπιστο

Αναζητήστε πρωτόκολλο SSL στην ιστοσελίδα του e-shop που επιλέξατε.

Τι είναι το πρωτόκολλο ασφαλείας SSL;

Το ακρωνύμιο SSL προκύπτει από τους όρους "Secure Sockets Layer" και πρόκειται για ένα πρωτόκολλο επικοινωνίας με ηλεκτρονικό πιστοποιητικό, το οποίο εγγυάται την ασφαλή μεταφορά δεδομένων μεταξύ ενός server (website) και ενός browser (client). Πιο συγκεκριμένα, το πρωτόκολλο SSL είναι υπεύθυνο για:

- την πιστοποίηση του server από τον browser
- την παροχή ενός ασφαλούς κρυπτογραφημένου περιβάλλοντος για την ανταλλαγή δεδομένων μέσω αυτού.

Επομένως, η επικοινωνία με ένα website το οποίο δεν χρησιμοποιεί πρωτόκολλο SSL μπορεί οποιαδήποτε στιγμή να παραβιαστεί από κάποιον hacker, ο οποίος θα αποκτήσει αυτομάτως πρόσβαση σε όλα τα στοιχεία που μοιράζονται οι δύο πλευρές. Από emails, ονόματα και τηλεφωνικές επαφές μέχρι στοιχεία λογαριασμών και κωδικοί ασφαλείας, όλα μπορεί να γίνουν εύκολη λεία για κάποιον που δεν έχει αγνές προθέσεις.

Αντιθέτως, τα websites που είναι κρυπτογραφημένα με SSL προστατεύουν τους επισκέπτες τους, ώστε κανένας να μην μπορεί να έχει πρόσβαση στην επικοινωνία τους με τον εκάστοτε browser.

Πώς θα καταλάβω αν ένα website έχει SSL;

Είναι πολύ απλό! Θα το αναγνωρίσετε από:

1) Το URL

Το URL θα πρέπει να ξεκινά με “https” και όχι απλώς “http”.

2) Το λουκέτο (όχι δεν είναι διακοσμητικό!)

Το πράσινο λουκέτο που βρίσκεται είτε αριστερά είτε δεξιά από τη μπάρα URL υποδεικνύει ότι ο server είναι πιστοποιημένος και άρα η σύνδεση μαζί του είναι ασφαλής. Με αυτόν τον τρόπο όλα τα δεδομένα που θα μοιραστούν μέσω αυτής της επικοινωνίας θα παραμείνουν μεταξύ τους. Εάν το λουκέτο δεν είναι πράσινο τότε είτε το πιστοποιητικό έχει λήξει και δεν ισχύει πια είτε έχει γίνει ανάκλησή του από τις αρχές που είναι υπεύθυνες για την έκδοση πιστοποιητικών.

Πατώντας επάνω στο εικονίδιο μπορείτε να αντλήσετε περισσότερες πληροφορίες για τον πάροχο του πιστοποιητικού αλλά και το εκάστοτε website.

3) Την ημερομηνία λήξης του πιστοποιητικού

Επειδή καμιά φορά τα πράγματα δεν είναι έτσι όπως φαίνονται, θα πρέπει να είστε πολύ προσεκτικοί με τα μηνύματα που σας εμφανίζει ο browser σας σχετικά με το εκάστοτε πιστοποιητικό, γιατί αλλιώς μπορεί να πέσετε θύματα διαδικτυακής κλοπής**.**

Προτιμήστε ιστοσελίδες που γνωρίζετε, με συνέπεια στις υπηρεσίες τους και όσο το δυνατόν περισσότερα reviews από πελάτες

Να ελέγχετε πάντα τις βασικές πληροφορίες που παρέχονται για το ηλεκτρονικό κατάστημα στην ιστοσελίδα του (π.χ. έδρα καταστήματος, ύπαρξη φυσικού καταστήματος, στοιχεία επικοινωνίας, πολιτική επιστροφών, όροι αγορών, πολιτική απορρήτου κ.α.)

Ενότητα 2: Πως μπορείς να προστατευτείς στις on-line αγορές σου

Ελέγξτε τον ιστότοπο της επιχείρησης: Οποιοσδήποτε μπορεί να ανοίξει ένα διαδικτυακό κατάστημα. Γι' αυτό είναι σημαντικό να έχετε κάποια σχετική γνώση για τη φήμη της επιχείρησης που έχετε επιλέξει για να πραγματοποιήσετε τις online αγορές σας. Εξίσου σημαντικό είναι να διαβάζετε τις συστάσεις άλλων πελατών προκειμένου να διαμορφώσετε πλήρη εικόνα για την επιχείρηση.

Προστατεύετε τα προσωπικά σας στοιχεία: Μην αποκαλύπτετε προσωπικά στοιχεία παρά μόνο εάν είστε βέβαιοι για το ποιος τα συλλέγει, το σκοπό για τον οποίο τα ζητάει και τον τρόπο με τον οποίο θα τα χρησιμοποιήσει. Υπάρχουν εταιρείες οι οποίες πουλάνε τα στοιχεία των πελατών τους σε τρίτους. Οι περισσότερες σας δίνουν τη δυνατότητα να αρνηθείτε την κοινοποίηση των προσωπικών σας στοιχείων.

Προσέχετε τις λεπτομέρειες: Ελέγχετε την αναμενόμενη ημερομηνία παραλαβής, το κόστος αποστολής και διεκπεραίωσης της συναλλαγής και αποστολής των προϊόντων, την εγγύηση, την πολιτική επιστροφών, και άλλες σημαντικές λεπτομέρειες. Βεβαιωθείτε ότι υπάρχει διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία μπορείτε να απευθυνθείτε γραπτώς, ή τηλεφωνικός αριθμός επικοινωνίας σε περίπτωση που χρειάζεστε βοήθεια με την παραγγελία ή το προϊόν που αγοράσατε.

Χρησιμοποιείτε έναν ασφαλή browser: Το πρόγραμμα που χρησιμοποιείτε για την περιήγηση σας στο διαδίκτυο θα πρέπει να εγγυάται την ασφάλεια των συναλλαγών σας. Τέτοιες προγράμματα είναι ο Internet Explorer, το Netscape, το AOL, το Opera, το Mozilla Firefox, το Chrome και το Safari.

Διατηρείτε μυστικούς τους κωδικούς εισόδου (passwords): Μην αποκαλύπτετε ποτέ τα passwords που χρησιμοποιείτε και φροντίστε να παραμένουν ασφαλή. Αποφύγετε να χρησιμοποιείτε απλές λέξεις ή την ημερομηνία της γέννησης σας. Φτιάξτε τους κωδικούς ασφαλείας χρησιμοποιώντας συνδυασμούς γραμμάτων και αριθμητικών χαρακτήρων.

Χρησιμοποιείτε μια πιστωτική κάρτα: Η σύμβαση που έχετε υπογράψει με την τράπεζα που εξέδωσε την κάρτα σας εγγυάται ότι έχετε περιορισμένη ευθύνη σε περίπτωση μη εξουσιοδοτημένης χρέωσης. Ασφαλώς, θα πρέπει να ειδοποιείτε αμέσως τον εκδότη της κάρτας σας, σε περίπτωση που πληροφορείστε την πραγματοποίηση κάποιας μη εξουσιοδοτημένης

συναλλαγής με χρέωση του λογαριασμού της κάρτας σας, ή σε περίπτωση απώλειας ή κλοπής της κάρτας σας.

Κρατείστε τις αποδείξεις συναλλαγών και τους λογαριασμούς πληρωμής της κάρτας σας: Πολλές από τις online επιχειρήσεις συνηθίζουν να στέλνουν ένα email όπου επιβεβαιώνεται η παραγγελία σας και συνοψίζεται η ποσότητα και το κόστος της αγοράς. Καλό θα ήταν να κάνετε μια εκτύπωση του email αυτού και να το φυλάξετε για το ενδεχόμενο να σας χρειαστεί στο μέλλον.

Όπως επισημαίνει η Διευθύντρια του Ευρωπαϊκού Κέντρου Καταναλωτή κ. Αθηνά Κοντογιάννη*: «Οι πολύ μεγάλες ευκαιρίες μπορεί να κρύβουν παγίδες. Δεν είναι όλα τα ηλεκτρονικά καταστήματα αξιόπιστα ούτε όλες οι διαφημιστικές καταχωρήσεις αληθινές. Το Δίκτυο των Ευρωπαϊκών Κέντρων Καταναλωτή, προκειμένου να βοηθήσει τους καταναλωτές να αποφύγουν τις παγίδες και να μην παραπλανηθούν, δίνει 11 απλές συμβουλές και τους καλεί να τις μελετήσουν, πριν αγοράσουν μέσω διαδικτύου».*

11 τρόποι να εντοπίσετε προϊόντα απομίμησης στο Διαδίκτυο:

1. Δίνουμε προσοχή στις περιγραφές που αναγράφονται κάτω από την ηλεκτρονική διεύθυνση της εταιρείας στα αποτελέσματα της εκάστοτε μηχανής αναζήτησης: Όταν περιλαμβάνονται φράσεις όπως “πάμφθηνο” ή “απόκτησε δωρεάν”, πρόκειται, κάποιες φορές, για ιστοσελίδες με αυξημένο κίνδυνο απάτης.
2. Επαληθεύουμε την ταυτότητα και τα στοιχεία επικοινωνίας του πωλητή που βρίσκονται συνήθως κάτω από τους “όρους χρήσης” της ιστοσελίδας και τα συγκρίνουμε με τα στοιχεία της ιστοσελίδας της επιχείρησης στον επίσημο καταχωρητή εκχώρησης ονομάτων χώρου (Domain Names) με κατάληξη .gr, ο οποίος έχει αδειοδοτηθεί από την ΕΕΤΤ, και ειδικότερα με το πεδίο ‘Ποιος είναι ο ιδιοκτήτης’. Είναι επίσης σημαντικό, να υπάρχουν πλήρη στοιχεία επικοινωνίας με την εταιρεία (επωνυμία, διεύθυνση, ηλεκτρονικό ταχυδρομείο, τηλέφωνο), αριθμός καταχώρησης στο ΓΕΜΗ, ΑΦΜ ή άλλα αντίστοιχα αν πρόκειται για ηλεκτρονικό κατάστημα που εδρεύει σε άλλο κράτος μέλος.
3. Διαβάζουμε τυχόν κριτικές και σχόλια των καταναλωτών για τον συγκεκριμένο προμηθευτή, με τις οποίες μεταφέρουν την εμπειρία τους από τη μεταξύ τους συναλλαγή, πολύ περισσότερο αν πρόκειται για άγνωστο κατάστημα.
4. Επαληθεύουμε την αυθεντικότητα του σήματος αξιοπιστίας της ιστοσελίδας, αν υπάρχει τέτοιο.
5. Ελέγχουμε αν η συγκεκριμένη επώνυμη μάρκα διαθέτει λίστα επίσημων συνεργατών για την πώληση των προϊόντων της ή αν έχει καταγγείλει ιστοσελίδες που πωλούν προϊόντα απομίμησης.
6. Συγκρίνουμε τις τιμές με αυτές του επίσημου καταστήματος. Δεν εμπιστευόμαστε ιστοσελίδες που προσφέρουν ύποπτα ελκυστικές προσφορές στο διαδίκτυο ή στα μέσα κοινωνικής δικτύωσης.

7. Αντιπαραβάλλουμε το επίσημο λογότυπο της μάρκας με αυτό που εμφανίζεται στην αμφισβητούμενη ιστοσελίδα ή πάνω στο προς πώληση προϊόν.
8. Συμβουλευόμαστε τους γενικούς όρους και προϋποθέσεις χρήσης της ιστοσελίδας και αγοράς από αυτή και βεβαιωνόμαστε ότι τηρεί τους κανονισμούς για τα δικαιώματα του καταναλωτή.
9. Είμαστε επιφυλακτικοί με τις κακοσχεδιασμένες ιστοσελίδες, με όσες δεν χρησιμοποιούν σωστά την ελληνική γλώσσα ή διαθέτουν εικόνες ύποπτα κακής ποιότητας.
10. Διασφαλίζουμε την πληρωμή μας. Προτιμάμε πάντοτε μεθόδους πληρωμής που μπορούν να ανακληθούν, μέσω αμφισβήτησης συναλλαγής με την τράπεζά μας (ιδίως χρεωστική ή πιστωτική κάρτα, κατά προτίμηση προπληρωμένη για ακόμη μεγαλύτερη ασφάλεια). Αποφεύγουμε τις μεταφορές χρημάτων με εντολή πληρωμής, με μεταφορά μετρητών ή, ακόμη, και με τραπεζικό έμβασμα, πολύ περισσότερο όταν δεν υπάρχουν στην ιστοσελίδα πλήρη στοιχεία επικοινωνίας με την εταιρεία.
11. Διασταυρώνουμε αν το ηλεκτρονικό κατάστημα αποδέχεται την εξωδικαστική επίλυση οικονομικών διαφορών που ενδέχεται να προκύψουν με τη διαμεσολάβηση του Ευρωπαϊκού Κέντρου Καταναλωτή Ελλάδας, αν είναι διασυνοριακές εντός Ε.Ε. (συμπεριλαμβανομένων της Νορβηγίας και της Ισλανδίας), ή από τον Συνήγορο του Καταναλωτή ή άλλο φορέα που είναι καταχωρημένος στο οικείο Μητρώο της Γενικής Γραμματείας Εμπορίου και Προστασίας Καταναλωτή. Σε κάθε περίπτωση αναζητούμε αν υπάρχει στην ιστοσελίδα του η παραπομπή στην πλατφόρμα της ηλεκτρονικής επίλυσης των διαφορών (πλατφόρμα ΗΕΔ) της Ευρωπαϊκής Ένωσης, όπως οφείλει σύμφωνα με την ενωσιακή νομοθεσία.

Κεφάλαιο 4ο: Ενδεικτικοί τρόποι πληρωμής

Ενότητα 1: Πληρωμή με κάρτα. Τι πρέπει να προσέχετε?

Ελέγχετε το λογαριασμό της πιστωτικής σας ανά διαστήματα για να διαπιστώσετε αν υπάρχουν «λάθος» χρεώσεις.

Ελέγχετε οπωσδήποτε πριν από την πληρωμή ότι ο ιστότοπος είναι ασφαλής.

Ποτέ μην αποθηκεύετε τα στοιχεία της κάρτας σας στο **site** που χρησιμοποιείτε.

Ποτέ μη δίνετε τα στοιχεία της πιστωτικής σας μέσω **email** ή μέσω τηλεφώνου.

Ποτέ μη πληρώνετε με μεταφορά χρημάτων σε λογαριασμό.

Το πλαστικό χρήμα έχει μπει δυναμικά στη ζωή μας και με τις νέες ρυθμίσεις που επιβάλλονται θα πρέπει υποχρεωτικά να πληρώνεις με κάρτα για να εξασφαλίσεις φοροελαφρύνσεις.
Επειδή ακριβώς θα χρειαστεί κάποιες στιγμές να πληρώσεις με την χρεωστική ή πιστωτική σου κάρτα σε μικρότερα μαγαζιά, ή ακόμα και σε ελεύθερους επαγγελματίες και όχι μόνο στα μεγάλα πολυκαταστήματα όπως συνηθίζονταν μέχρι τώρα σίγουρα θα πρέπει να είσαι επιφυλακτικός.

Υπάρχουν κάποια σημεία στα τερματικά μηχανάκια που πρέπει να προσέχεις όταν πληρώνεις με κάρτα, γιατί υπάρχει περίπτωση κάποιος να έχει τοποθετήσει έναν ανιχνευτή πάνω στο μηχάνημα με σκοπό να αποθηκεύσει τα στοιχεία της κάρτας σου να και σου αποσπάσει χρήματα. Αν προσέξεις αυτές τις λεπτομέρειες όμως θα είσαι σίγουρα ασφαλής.

Ενότητα 2: Πληρωμή με Paypal

Το PayPal, είναι:

1. Μια ηλεκτρονική «τράπεζα».
2. Μία πύλη πληρωμών.

Μπορεί να χρησιμοποιηθεί με δύο τρόπους:

1. Για να πληρώσουμε άλλους.
2. Για να πληρωθούμε εμείς.

Στην ουσία είναι μια online υπηρεσία μεταφοράς χρημάτων. Είναι ασφαλές και εύχρηστο, και γι' αυτό τον λόγο τον χρησιμοποιούν πολλά ηλεκτρονικά καταστήματα, αν όχι σχεδόν όλα. Η εταιρία που το λειτουργεί ήταν έως πρότινος η ίδια που έχει το eBay και γι' αυτό οι περισσότερες αγοραπωλησίες στο eBay εξοφλούνται μέσω PayPal.

<u>Τι μπορεί να κάνει κάποιος στο PayPal:</u>

- Να κάνει αγορές μέσω Internet.
- Να στείλει χρήματα σε κάποιον φίλο ή επαγγελματία που έχει λογαριασμό σε αυτό. (χωρίς απαραιτήτως ο αποστολέας να έχει λογαριασμό, μια πιστωτική/χρεωστική κάρτα αρκεί).

- Να λάβει χρήματα από κάποιον άλλο με αποστολή στον τραπεζικό λογαριασμό του (απαραίτητος ο λογαριασμός PayPal και καλύτερα ρωτήστε την τράπεζά σας αν το υποστηρίζει πρώτα).

Πως λειτουργεί το PayPal

Ακριβώς όπως ένας απλός τραπεζικός λογαριασμός. Μπορούμε να βάλουμε σε αυτόν λεφτά απο μία κάρτα (διότι το Διαδίκτυο δεν έχει ταμεία), να δεχτούμε λεφτά από κάποιον άλλο ή και να στείλουμε λεφτά σε άλλον. Εκτος αυτού, αν χρειάζεται να πληρώσουμε κάποιον αλλα δεν θέλουμε να μπούμε στη διαδικασία του λογαριασμού του ζητάμε ενα ειδικό mail με το ποσό που ζητάει και συμπληρώνουμε στην ειδική κρυπτογραφημένη σελίδα του PayPal τα στοιχεία της κάρτας μας. Είναι 100% ασφαλές. Επίσης κάνει μετατροπές απο/σε δολλάρια/ευρώ/λίρες αυτόματα.

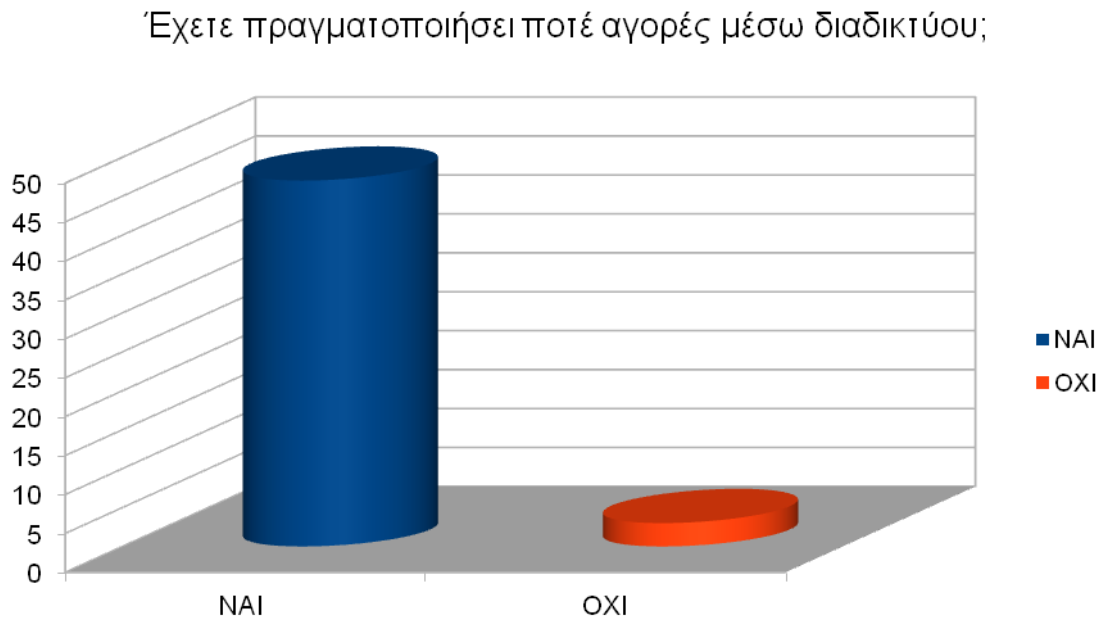
Κεφάλαιο 5ο: Ερωτηματολόγιο

Στα πλαίσια της εργασίας, αποφασίσαμε να διεξάγουμε μία έρευνα σε μορφή ερωτηματολογίου με σκοπό να δημιουργήσουμε μία εικόνα με βάση το πόσο, άτομα διαφόρων ηλικιακών ομάδων γνωρίζουν πως να προστατεύονται στις διαδικτυακές τους συναλλαγές.

Σε δείγμα 50 ατόμων τα αποτελέσματα της έρευνας ήταν τα εξής:

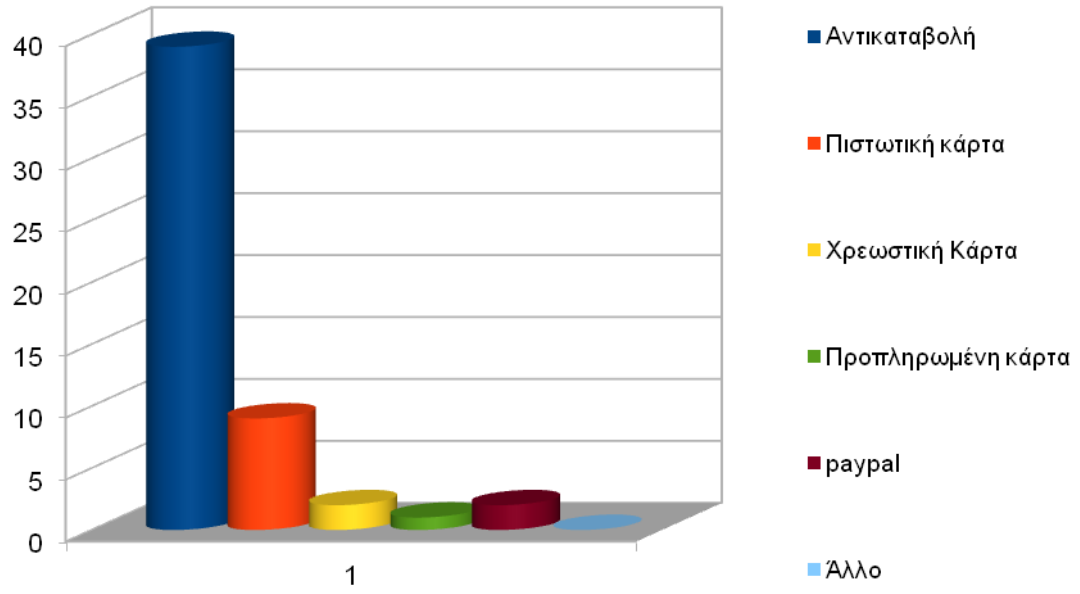
1.

2.



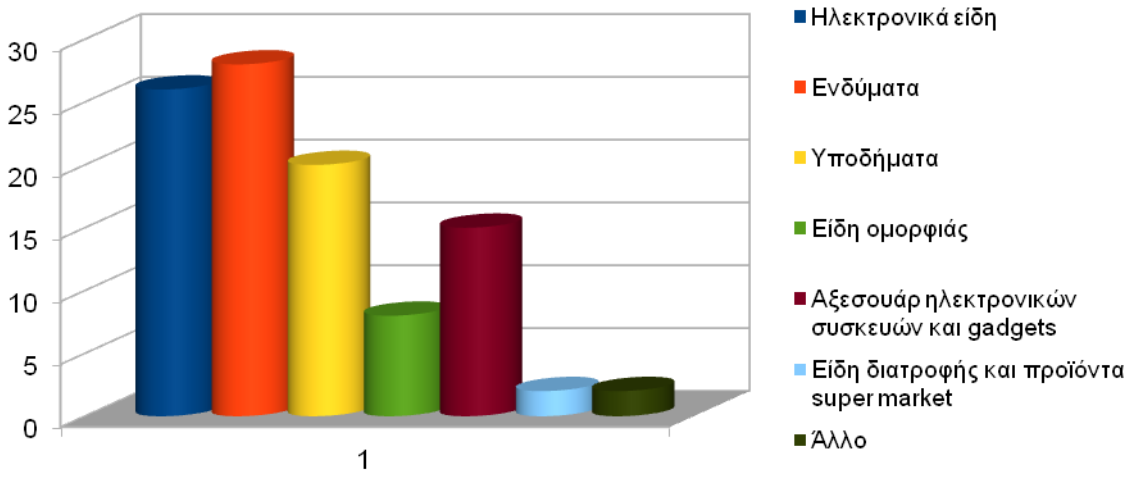
3.

Αν ναι, ποια μέθοδο πληρωμής χρησιμοποιήσατε;

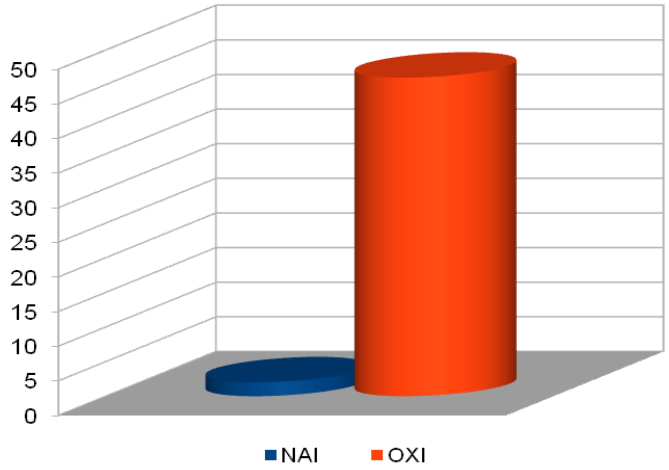


4. Γιατί επιλέξατε το συγκεκριμένο τρόπο πληρωμής;
Στην ερώτηση αυτή, όσοι είχαν απαντήσει με αντικαταβολή στην συντριπτική τους πλειοψηφία απάντησαν ότι νιώθουν περισσότερο ασφαλείς. Όσοι απάντησαν με πιστωτική θεωρούν ότι είναι πιο εύκολο, με χρεωστική γιατι δεν έχει επιπλέον έξοδα και με προπληρωμένη κάρτα ότι νιώθουν μεγαλύτερη σιγουριά.

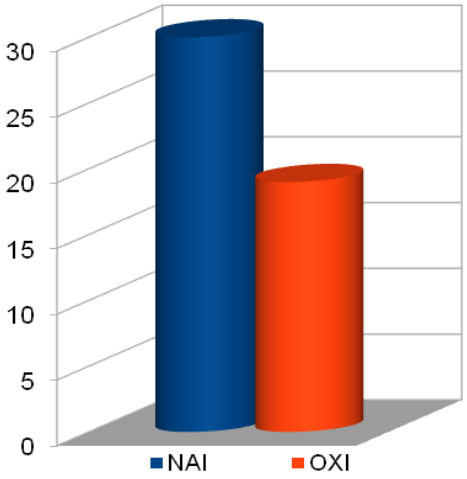
5. Τι είδους αγαθά έχετε αγοράσει διαδικτυακά;



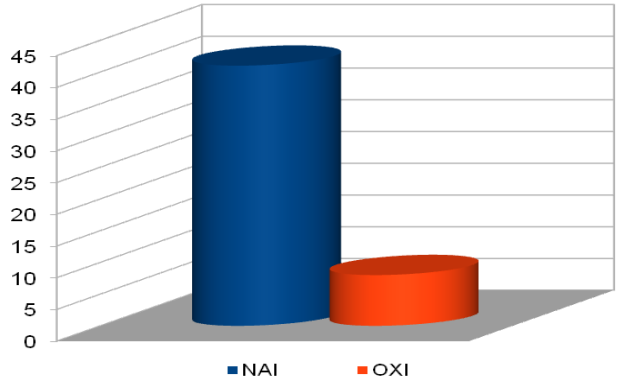
6.Έχετε αντιμετωπίσει ποτέ προβλήματα σχετικά με τον τρόπο πληρωμής που έχετε επιλέξει;



7.Θεωρείτε ότι είστε αρκετά ασφαλείς όταν κάνετε αγορές μέσω διαδικτύου;



8. Γνωρίζετε <u>πώς</u> μπορείτε να κάνετε τις διαδικτυακές αγορές σας με ασφάλεια;



Συμμετέχοντες μαθητές :

Ομάδα 1

Χρηστοβασίλης Χρήστος
Τσιώνης Μιλτιάδης
Παλαιοπάνου Ανδρονίκη

Ομάδα 2

Βλαχιώτης Θεόδωρος
Μπίτος Άγγελος
Παπαχαραλάμπους Χαράλαμπος
Παπανικολάου Ηλίας

Ομάδα 3

Μπακόλα Δήμητρα
Τσαπραλή Δήμητρα
Μούντζια Δήμητρα
Γκοργκόλη Λαμπρινή

ΠΗΓΕΣ:

http://www.excelixi.org/knowledge-base/e-business/ta_5_pleonektimata_tou_ilektronikou_emporiou

http://coolweb.gr/psonia-online-oikonomika/

https://www.huffingtonpost.gr/entry/pos-mporoen-oi-ellenes-katanalotes-na-prostateetoen-apo-apates-kata-tis-online-ayores-toes_gr_5a2530b8e4b03c44072eab1d

https://bit.ly/2kx93ZO

https://bit.ly/2smKwKN

http://www.saferinternet.gr/index.php?parentobjId=Page72&objId=Text452&childobjId=Text452#Text452

Υλικό Παρουσίαση από το saferinternet4kids

https://internetsafety.pi.ac.cy/teenagers-phishing

https://bit.ly/2Jc7rmp