ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μέτρα αυτοπροστασίας στις διαδικτυακές επικοινωνίες

Δρ. Βασίλειος Σταθόπουλος

Ε.Ε.Π./Α.Δ.Α.Ε.

Ηράκλειο, 1 Νοεμβρίου 2008

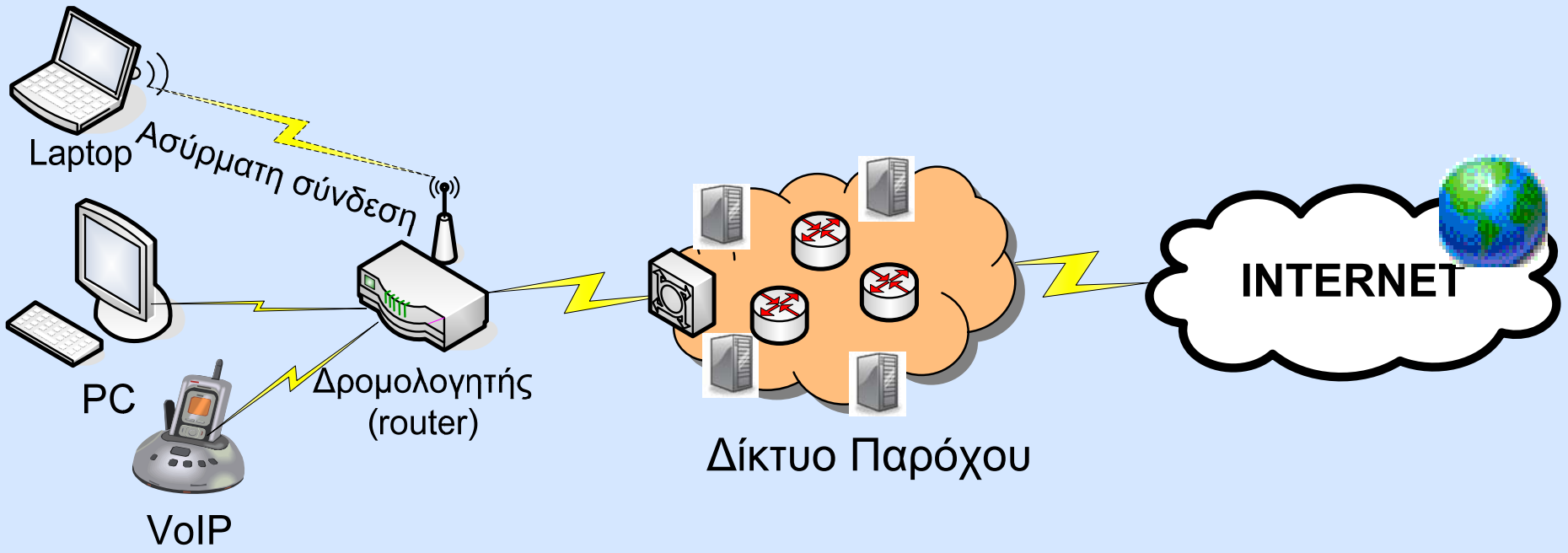
επιμέλεια κειμένου
Π. Κοτζανικολάου, Β. Σταθόπουλος

Περιεχόμενα

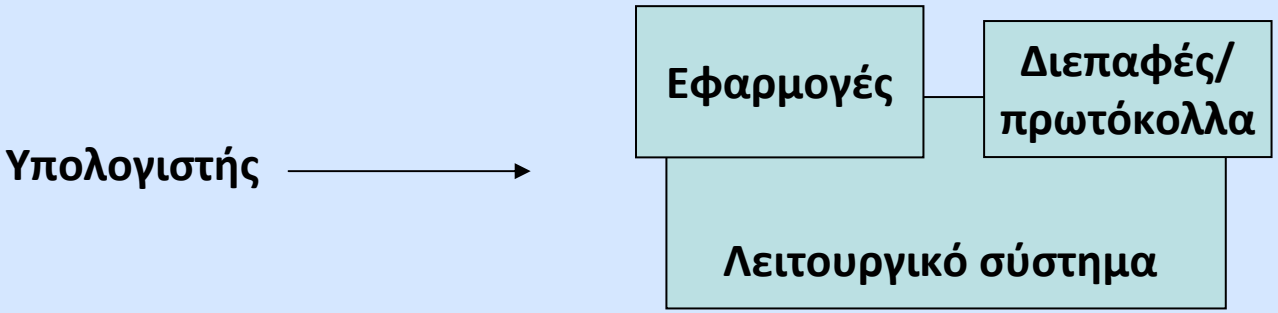
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Υπηρεσίες επικοινωνιών μέσω του διαδικτύου
- Κίνδυνοι και επιθέσεις ασφάλειας
- Μέθοδοι παραβίασης απορρήτου επικοινωνίας
- Μέτρα αυτοπροστασίας

Τυπική διάταξη διαδικτυακής πρόσβασης



Βασικές λειτουργικές οντότητες Υπολογιστή



Υπηρεσίες διαδικτυακών επικοινωνιών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Ηλεκτρονικό ταχυδρομείο (e-mail)
- Πλοήγηση στο διαδίκτυο (web surfing)
- Ηλεκτρονικές συναλλαγές – αγορές (e-commerce)
- Τηλεφωνία μέσω διαδικτύου (Voice over IP)
- Ανταλλαγή μηνυμάτων (instant messengers, chatting)
- Κοινωνικά δίκτυα (social networks)
- …

Ηλεκτρονικό ταχυδρομείο (e-mail)

Κίνδυνοι παραβίασης απορρήτου και μέτρα αυτοπροστασίας

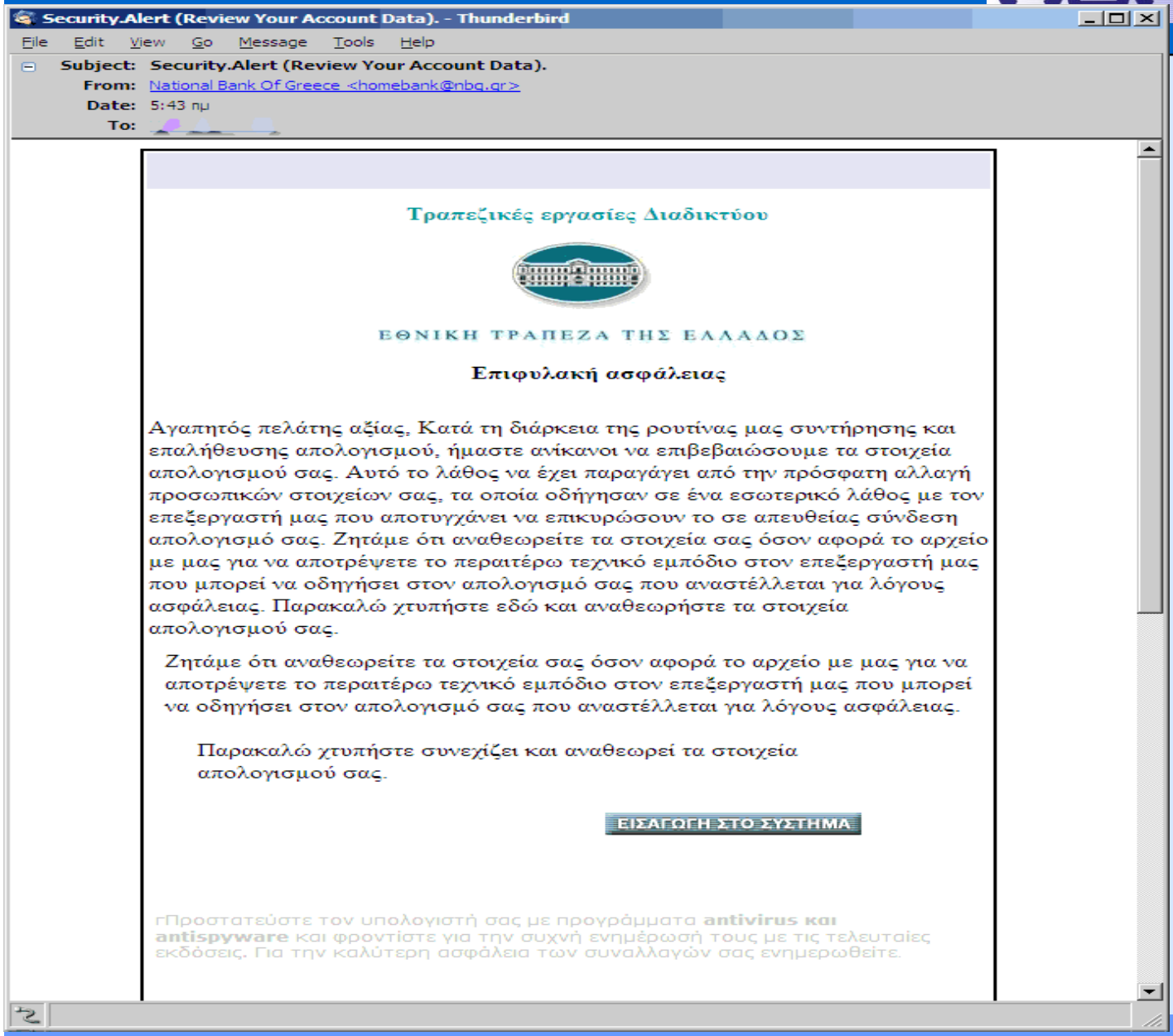
Επιθέσεις Phishing

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Παράφραση fishing (= ψαρεύω)
- Αποστολή **παραπλανητικών μηνυμάτων**, με σκοπό να πείσουν / δελεάσουν τον χρήστη να αποκαλύψει ευαίσθητες πληροφορίες
- **Αποστέλλονται μαζικά**, σε χιλιάδες ή ακόμα και σε εκατομμύρια παραλήπτες
- Εκμεταλλεύονται το **πλήθος** των πιθανών παραληπτών
- Υπόθεση:
  - Πολύ υψηλό επίπεδο ενημέρωσης χρηστών (99%)
  - 1.000 τυχαίοι παραλήπτες
  - 1.000 – (99 % * 1.000) = 10 υποψήφια «θύματα»
- Πραγματικότητα:
  - το επίπεδο γνώσης / ενημέρωσης των χρηστών **δεν είναι υψηλό**
  - ο αριθμός των παραληπτών μπορεί να ανέρχεται σε **εκατοντάδες χιλιάδες** …

Παραδείγματα επιθέσεων phishing

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ



1. Το email αποστέλλεται
α) **χωρίς να παραβιάζεται** η υπηρεσία κατά την μεταφορά και
β) **χωρίς** να μεταφέρει **κακόβουλο λογισμικό**
γ) μεταφέρει **παραπλανητικό κείμενο**

2. Το phishing στηρίζεται
α) στην **άγνοια** του πελάτη **και**
β) στην **αλλοιωμένη πληροφορία** στοιχείων αποστολέα “From”

3. Απαιτείται **e-mail spoofing** για την αλλοίωση της πληροφορίας **“From”.**

Παραδείγματα επιθέσεων phishing

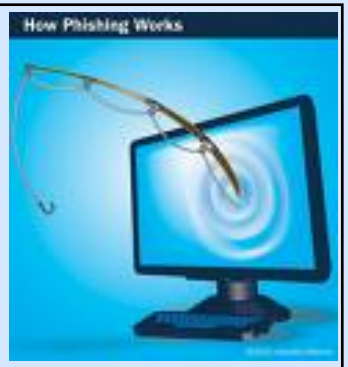
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

From: VISA Service [mailto:VisaService@visa.com]

Sent: Thursday, February 23, 2006 10:23 AM

To: ……

Subject: Attention! Several VISA Credit Card bases have been LOST



Good afternoon, unfortunately some processings have been cracked by hackers, so a new secure code to protect your data has been introduced by Visa. You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank. If you don't see any suspicious transactions, it doesn't mean that the card is not lost and cannot be used. Probably, your card issuers have not updated information yet. That is why we strongly recommend you to visit our website and update your profile, otherwise we cannot guarantee stolen money repayment. Thank you for your attention. Click **here** and update your profile.

Εξελιγμένες επιθέσεις Phishing

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Vishing (= voice + phishing)
  - Ο επιτιθέμενος γνωρίζει:
    - την ηλεκτρονική διεύθυνση και
    - τον αριθμό τηλεφώνου του χρήστη.
  - Αρχικά στέλνεται το παραπλανητικό μήνυμα, περιγράφοντας στο χρήστη κάποιο «πρόβλημα» στον λογαριασμό του.
  - Το παραπλανητικό email συνοδεύεται από τηλεφωνική επικοινωνία (πολλές φορές κάνοντας χρήση του “caller ID spoofing”

Κίνδυνοι από συνημμένα αρχεία

- ηλεκτρονικά μηνύματα που περιλαμβάνουν συνημμένα αρχεία (attachments)
- Οι ενεργοί σύνδεσμοι (links) εντός του κειμένου των e-mails ενδέχεται επίσης να μεταφέρουν κακόβουλο λογισμικό

Κακόβουλο λογισμικό

- Ιοί (Computer viruses) – worms - Trojan horses – Adware – Spyware

- Ιοί (Computer viruses)
  - Ο ιός είναι ένα κομμάτι κώδικα που προσθέτει τον εαυτό του σε άλλα προγράμματα ή αρχεία λειτουργικών συστημάτων και εκτελεί τη ζημιά
  - Δεν μπορεί να εκτελεστεί από μόνος του αλλά χρησιμοποιεί το “host” πρόγραμμα.
  - Οπότε η ενεργοποίηση του ιού γίνεται αν ο κάτοχος ενεργοποιήσει το “host” πρόγραμμα
  - Παράδειγμα: μπορούν να σβήσουν αρχεία υπολογιστή ή να κλειδώσουν το σύστημα ενός υπολογιστή
  - Υπάρχει πλήρης αναλογία με το βιολογικό ιό.

Κακόβουλο λογισμικό

- Internet Worm
  - Το Worm είναι πρόγραμμα όπου μπορεί **να εκτελεστεί από μόνο του** (separate entity)
  - **Διαδίδει τον εαυτό του** σε πλήρως εκτελέσιμη έκδοση και σε άλλες μηχανές **από μόνο του**
  - Τρόποι μετάδοσης
    - Computer worms εξαπλώνονται με το να **εκμεταλλεύονται τις αδυναμίες των network services** (π.χ. SQL Slammer and Blaster: tunnel into your system and allow malicious users to control your computer remotely**)**
    - Computer worms που **εξαπλώνονται ως Trojan horses**
  - Παράδειγμα: internet worms που ενσωματώνουν SMTP engines δηλαδή το απαραίτητο κώδικα email και επικοινωνίας ώστε να παρακάμπτουν τα έτοιμα προγράμματα email ολοκληρωτικά.
  - Επομένως ο χρήστης του μολυσμένου υπολογιστή δεν αντιλαμβάνεται τίποτα μόνο σε περίπτωση load
  - Η εξάπλωση είναι ραγδαία και διεθνώς κάνουν την μεγαλύτερη ζημιά

Κακόβουλο λογισμικό

- Δούρειοι Ίπποι (*Trojan horse, also known as a Trojan*)
  - Προγράμματα που εμφανίζονται να εκτελούν μία επιθυμητή λειτουργία αλλά στην πραγματικότητα εκτελούν μη-εμφανείς κακόβουλες ενέργειες.
  - Παραδείγματα: 'waterfalls.scr.exe‘ or 'preetygirls.exe‘. Πολύ σημαντικό το extension του αρχείου .exe, .com, .scr, .bat, or .pif.
- Προγράμματα παρακολούθησης (spyware)
  - καταγράφουν τις ενέργειες του χρήστη (π.χ. Internet surfing habit, πληκτρολόγηση) συνήθως με στόχο τις στοχευόμενες διαφημίσεις
  - παρεμβαίνουν στον έλεγχο του χρήστη, (π.χ. installing additional software, redirecting Web Browser activity, accessing websites blindly that will cause more harmful viruses.
  - Ακόμα, αλλάζουν τα computer settings, με αποτέλεσμα αργές ταχύτητες σύνδεσης, διαφορετικές home pages)
  - Μεταφέρονται με την μέθοδο π.χ. των Δουρείων Ίππων
- What about Adware
  - μηχανισμοί που έχουν στόχο εμφάνιση διαφημίσεων και μεταφέρονται στα προγράμματα freeware που εγκαθιστά ο χρήστης.

Κίνδυνοι από κακόβουλο λογισμικό

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

1. Παρακολούθηση της ηλεκτρονικής αλληλογραφίας
   - Ονόματα και ηλεκτρονικές διευθύνσεις παραληπτών / αποστολέων
   - Θέμα και περιεχόμενο μηνυμάτων
   - Ημερομηνία και ώρα αποστολής / λήψης μηνυμάτων
2. Διαγραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου (Denial-of-Service attack)
3. Αποστολή μηνυμάτων χωρίς τη γνώση του χρήστη (spamming)

E-mail: Μέτρα αυτοπροστασίας

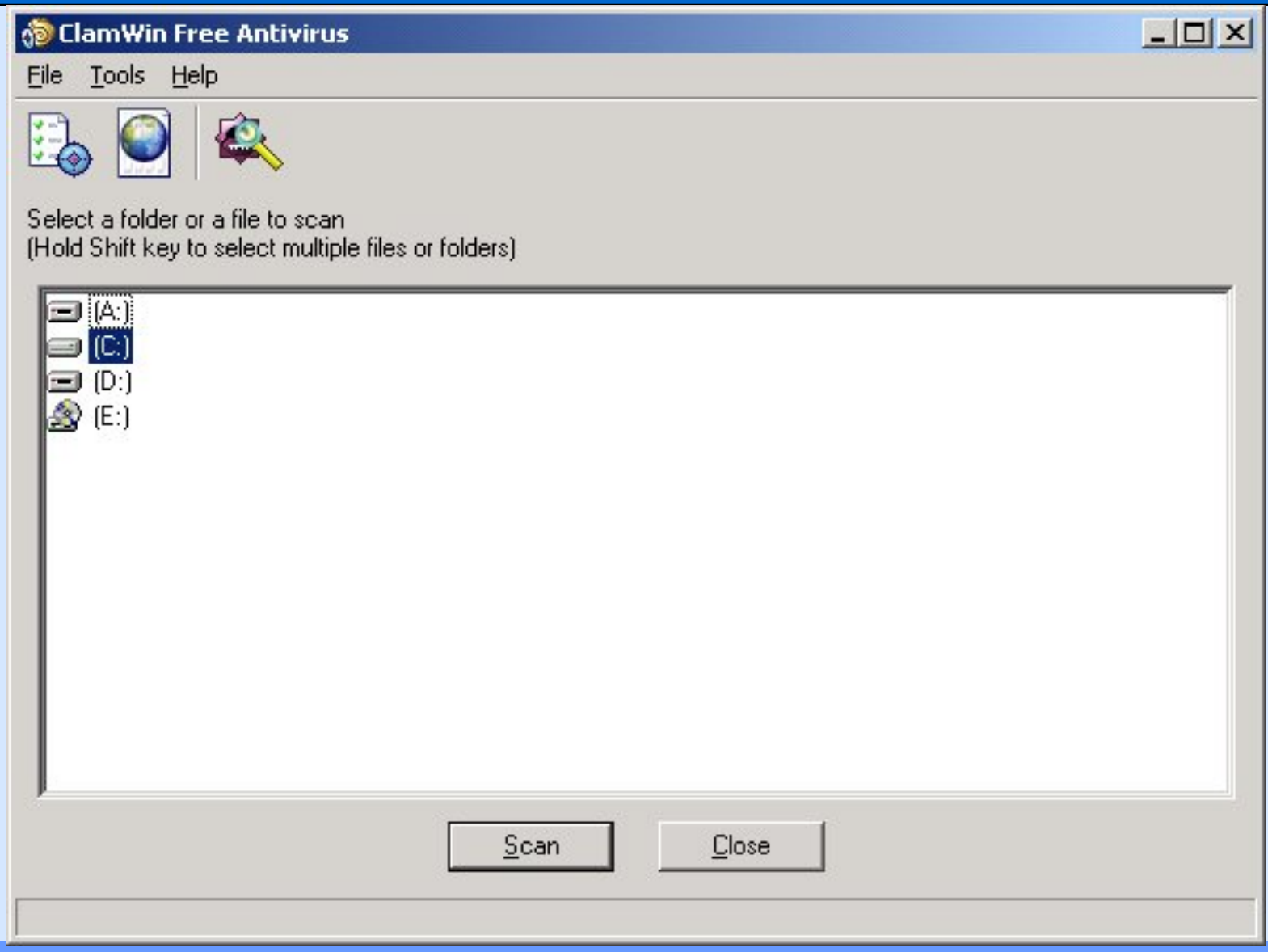
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

1. **Εγκαταστήστε πρόγραμμα προστασίας ιών (antivirus – antispyware) που ελέγχει τα συνημμένα αρχεία σε πραγματικό χρόνο (real-time scan).**
   - **Δωρεάν εκδόσεις**
     - **AVAST, http://www.avast.com/**
     - **AVG, http://free.grisoft.com/**
     - **BitDefender, http://www.bitdefender.com/**
     - **ClamAV, http://www.clamav.com**
     - **ClamWin, http://www.clamwin.com**

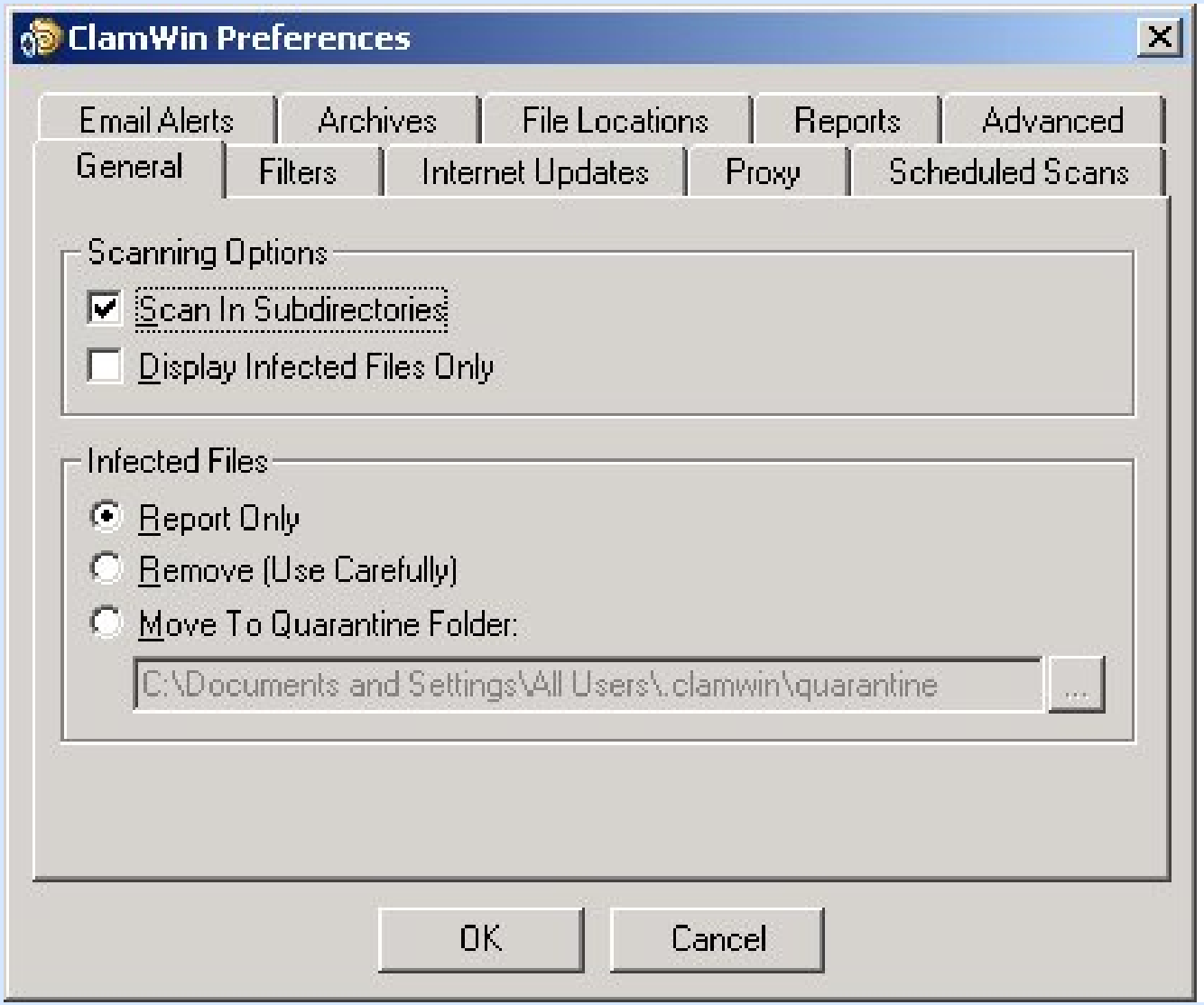
2. **Να είστε ιδιαίτερα επιφυλακτικοί όταν λαμβάνεται μηνύματα που σας ζητούν προσωπικά στοιχεία**

3. **Να θυμάστε ότι το e-mail είναι ένα μη ασφαλές μέσο. Ποτέ μην στέλνετε μέσω e-mail εμπιστευτικές πληροφορίες όπως:**
   - **αρ. λογαριασμού τράπεζας,**
   - **πιστωτική κάρτα,**
   - **κωδικούς πρόσβασης (password) κτλ**

Παράδειγμα δωρεάν λογισμικού antivirus



Παράδειγμα δωρεάν λογισμικού antivirus



E-mail: Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

4. **Σε περίπτωση που λαμβάνετε μηνύματα από άγνωστους αποστολείς:**
   - Να αποφεύγετε να απαντάτε
   - Μην ανοίγετε συνημμένα αρχεία
   - Μην πατάτε σε ενεργούς συνδέσμους (links)

5. **Μην χρησιμοποιείτε τη βασική σας διεύθυνση e-mail για:**
   - ηλεκτρονικές αγορές,
   - chat rooms,
   - εγγραφή σε sites κτλ

Χρησιμοποιείστε κάποια διεύθυνση email που μπορείτε να καταργήσετε ανά πάσα στιγμή, χωρίς άλλο κόστος.

Πλοήγηση στο διαδίκτυο (web surfing)

Κίνδυνοι παραβίασης απορρήτου και μέτρα αυτοπροστασίας

Κίνδυνοι παραβίασης απορρήτου στο διαδίκτυο

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- **Το πρόγραμμα πλοήγησης (web browser) διατηρεί ευαίσθητες πληροφορίες**
  - **Ιστορικό των ιστοσελίδων (browsing history)**
  - **Αποθηκευμένους κωδικούς ασφαλείας (passwords)**

- **Οι πληροφορίες αυτές θα μπορούσαν να αποκαλυφθούν σε τρίτους με διάφορους τρόπους**
  - **Κακόβουλο λογισμικό Trojan, spyware, κτλ**
  - **Κενό ασφάλειας στο πρόγραμμα πλοήγησης**
  - **Οικειοθελώς! (social engineering)**

- **Pharming: αντίστοιχη επίθεση με το phishing με τη διαφορά ότι αφορά ιστοσελίδες με παραπλανητικό όνομα, παραπλήσιο με κάποιο γνωστό site.**
  - **www.ebay.gr www.eebay.gr**
  - **www.microsoft.com www.micros0ft.com**

Μεταφορά πληροφοριών στο διαδίκτυο

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

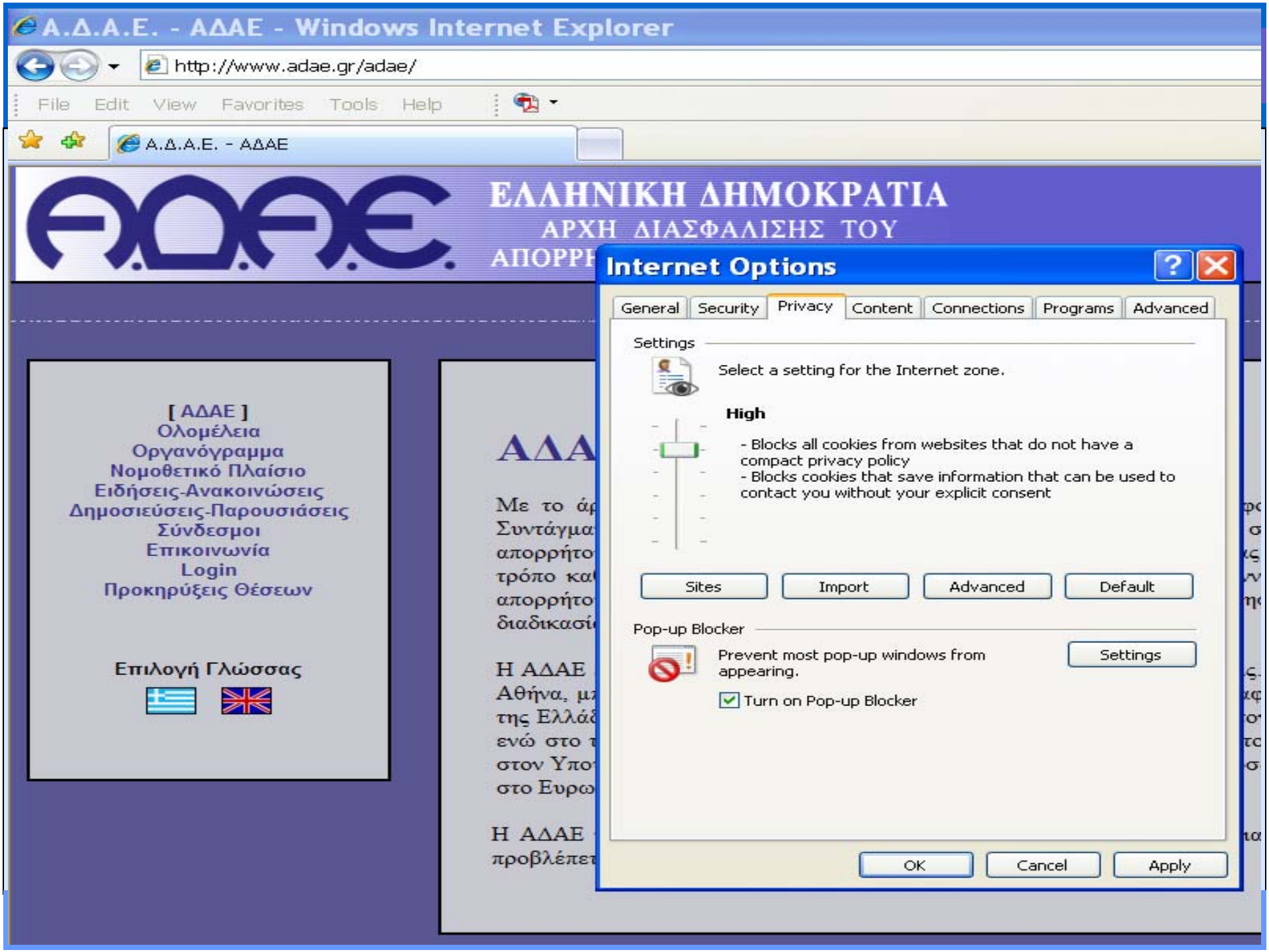
- **Σε πολλές περιπτώσεις ένας χρήστης μπορεί να αποστέλλει πληροφορίες σε δικτυακούς τόπους. Π.χ.:**
  - **Ηλεκτρονικές αγορές (e-commerce)**
    - **Αποστολή στοιχείων πιστωτικής κάρτας**
  - **Εγγραφή σε δικτυακό τόπο**
    - **Προσωπικά στοιχεία**
  - **Κοινωνικά δίκτυα (social networks)**
    - **Προσωπικά στοιχεία, ενδιαφέροντα κτλ.**
  - **Δίκτυα ανταλλαγής αρχείων (file sharing)**
    - **Αρχεία, μουσική κτλ**
  - **Μηχανές αναζήτησης (search engines)**
    - **Στοιχεία αναζητήσεων**
- **Κίνδυνος αποκάλυψης πληροφοριών σε μη έμπιστες οντότητες**
- **Κίνδυνος υποκλοπής από τρίτους κατά τη μεταφορά των πληροφοριών**

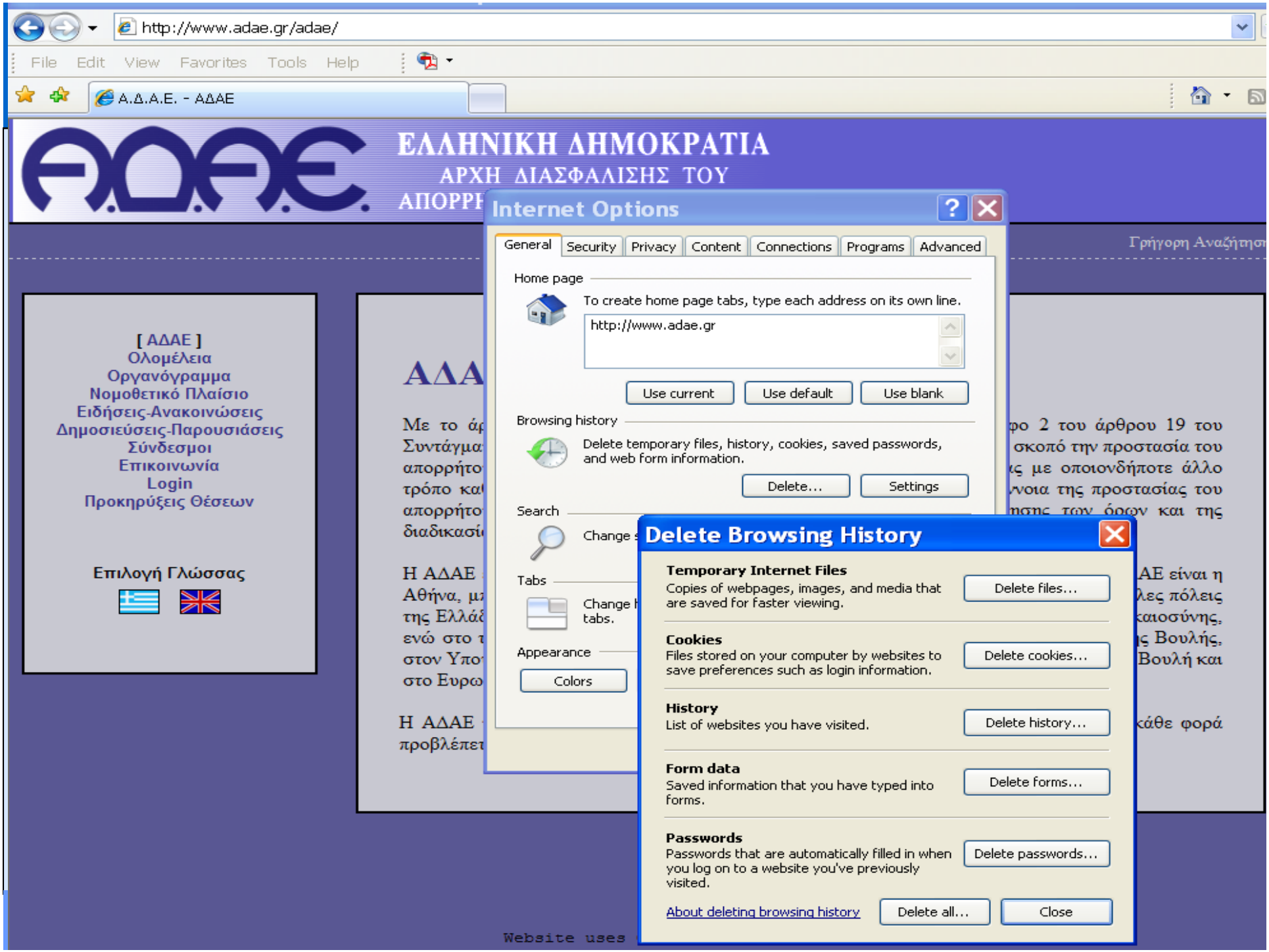
www: Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

6. **Να επιβεβαιώνετε ότι οι ρυθμίσεις ασφάλειας του προγράμματος πλοήγησης (web browser) είναι επαρκώς υψηλές**

- **Ενεργοποιήστε τη διαγραφή ιστορικού ιστοσελίδων από το πρόγραμμα πλοήγησης (browsing history)**
- **Ενεργοποιείστε το κατάλληλο επίπεδο προστασίας απορρήτου (privacy settings)**
- **Αποφεύγετε να αποθηκεύετε τους κωδικούς (passwords) στο πρόγραμμα πλοήγησης**


Α.Δ.Α.Ε. - ΑΔΑΕ - Windows Internet Explorer
http://www.adae.gr/adae/
File Edit View Favorites Tools Help
Α.Δ.Α.Ε. - ΑΔΑΕ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ
[ΑΔΑΕ]
Ολομέλεια
Οργανόγραμμα
Νομοθετικό Πλαίσιο
Ειδήσεις-Ανακοινώσεις
Δημοσιεύσεις-Παρουσιάσεις
Σύνδεσμοι
Επικοινωνία
Login
Προκηρύξεις Θέσεων
Επιλογή Γλώσσας
Internet Options
General Security Privacy Content Connections Programs Advanced
Settings
Select a setting for the Internet zone.
High
- Blocks all cookies from websites that do not have a compact privacy policy
- Blocks cookies that save information that can be used to contact you without your explicit consent
Sites Import Advanced Default
Pop-up Blocker
Prevent most pop-up windows from appearing.
Settings
Turn on Pop-up Blocker
OK Cancel Apply


http://www.adae.gr/adae/
File Edit View Favorites Tools Help
Α.Δ.Α.Ε. - ΑΔΑΕ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ
[ΑΔΑΕ]
Ολομέλεια
Οργανόγραμμα
Νομοθετικό Πλαίσιο
Ειδήσεις-Ανακοινώσεις
Δημοσιεύσεις-Παρουσιάσεις
Σύνδεσμοι
Επικοινωνία
Login
Προκηρύξεις Θέσεων
Επιλογή Γλώσσας
Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
To create home page tabs, type each address on its own line.
http://www.adae.gr
Use current Use default Use blank
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete... Settings
Search
Tabs
Appearance
Colors
Delete Browsing History
Temporary Internet Files
Copies of webpages, images, and media that are saved for faster viewing.
Delete files...
Cookies
Files stored on your computer by websites to save preferences such as login information.
Delete cookies...
History
List of websites you have visited.
Delete history...
Form data
Saved information that you have typed into forms.
Delete forms...
Passwords
Passwords that are automatically filled in when you log on to a website you've previously visited.
Delete passwords...
About deleting browsing history
Delete all...
Close
Website uses

www: Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

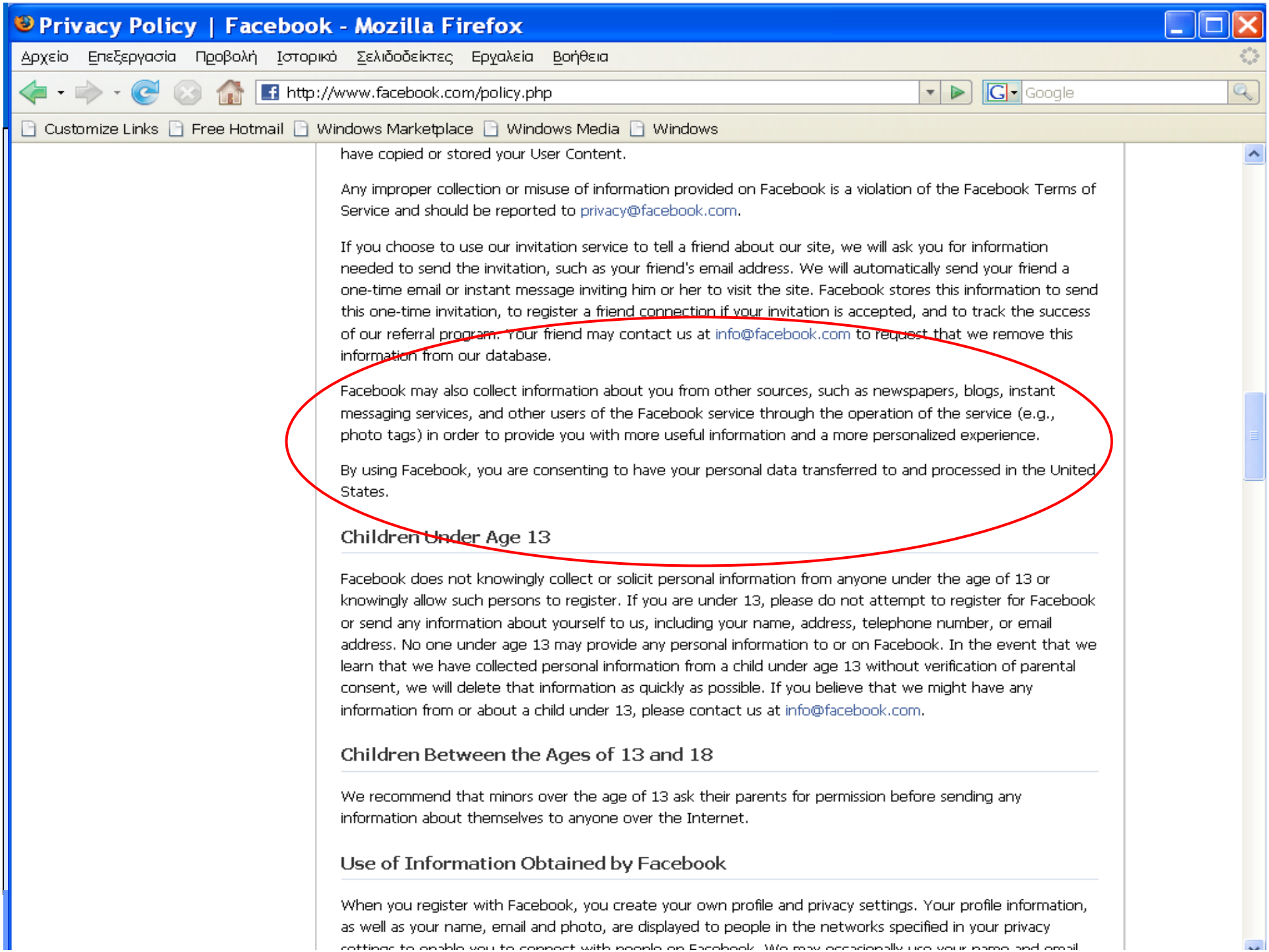
7. **Προτιμήστε κάποιο πρόγραμμα πλοήγησης το οποίο θεωρείται περισσότερο ασφαλές**
   - **Π.χ. Mozilla Firefox (είναι δωρεάν)**

8. **Μην δημοσιεύετε/αποστέλλετε χωρίς δεύτερη σκέψη προσωπικές ή άλλες πληροφορίες, σε δικτυακούς τόπους όπως**
   - **blogs,**
   - **social networks,**
   - **chat rooms,**
   - **instant messengers κτλ**

www: Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

9. **Ελέγξτε την πολιτική απορρήτου (privacy policy) κάθε ιστοσελίδας πριν αποστείλετε οποιαδήποτε πληροφορία ή εγγραφείτε σε κάποια υπηρεσία που παρέχει.**
   - **Πολλές ιστοσελίδες αναφέρουν ρητά ότι συμφωνείτε στην ελεύθερη χρήση πληροφοριών που σας αφορούν.**



have copied or stored your User Content.

Any improper collection or misuse of information provided on Facebook is a violation of the Facebook Terms of Service and should be reported to privacy@facebook.com.

If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will automatically send your friend a one-time email or instant message inviting him or her to visit the site. Facebook stores this information to send this one-time invitation, to register a friend connection if your invitation is accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database.

Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.

By using Facebook, you are consenting to have your personal data transferred to and processed in the United States.

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us at info@facebook.com.

Children Between the Ages of 13 and 18

We recommend that minors over the age of 13 ask their parents for permission before sending any information about themselves to anyone over the Internet.

Use of Information Obtained by Facebook

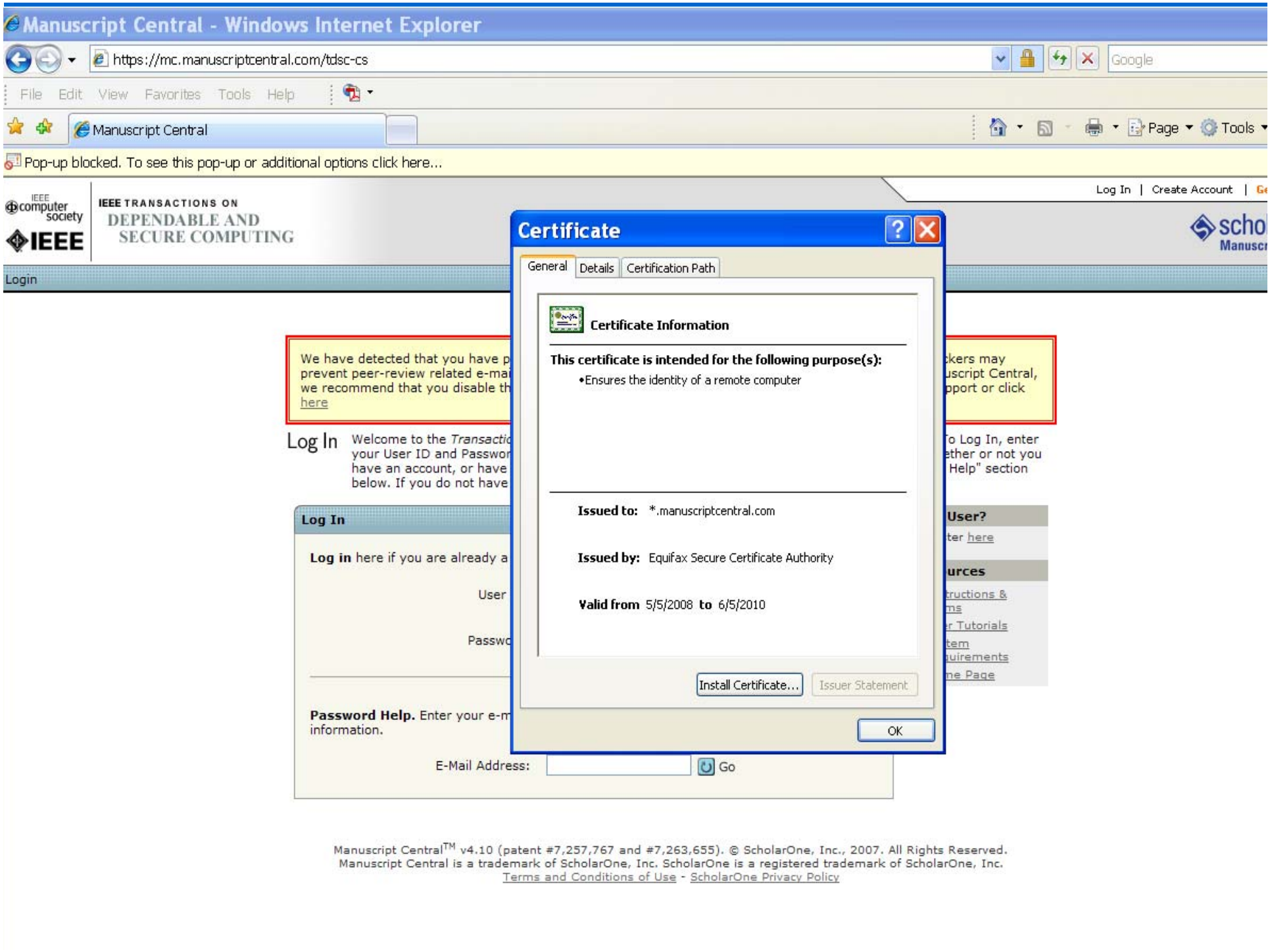
When you register with Facebook, you create your own profile and privacy settings. Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook. We may occasionally use your name and email

www: Μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

10. **Πριν αποστείλετε οποιαδήποτε πληροφορία σε κάποια ιστοσελίδα επιβεβαιώστε ότι :**
    - **Έχει έγκυρο ψηφιακό πιστοποιητικό**
    - **Χρησιμοποιεί κρυπτογράφηση (https:// αντί για http:// και εμφάνιση αντίστοιχης ένδειξης – «κλειδαριάς»)**
    - **Διαβάστε αναλυτικά πιθανά μηνύματα λάθους**

11. **Να είστε πάντα επιφυλακτικοί. Μην θεωρείτε ακριβή και αληθή όσα διαβάζετε στο διαδίκτυο.**


Manuscript Central - Windows Internet Explorer
https://mc.manuscriptcentral.com/tdsc-cs
Google
File Edit View Favorites Tools Help
Manuscript Central
Page Tools
Pop-up blocked. To see this pop-up or additional options click here...
IEEE computer society
IEEE
IEEE TRANSACTIONS ON
DEPENDABLE AND
SECURE COMPUTING
Log In | Create Account
Login
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer
Issued to: *.manuscriptcentral.com
Issued by: Equifax Secure Certificate Authority
Valid from 5/5/2008 to 6/5/2010
Install Certificate...
Issuer Statement
OK
We have detected that you have p
prevent peer-review related e-ma
we recommend that you disable th
here
Log In
Welcome to the Transactio
your User ID and Passwor
have an account, or have
below. If you do not have
Log In
Log in here if you are already a
User
Passwo
Password Help. Enter your e-m
information.
E-Mail Address:
Go
Manuscript Central™ v4.10 (patent #7,257,767 and #7,263,655). © ScholarOne, Inc., 2007. All Rights Reserved.
Manuscript Central is a trademark of ScholarOne, Inc. ScholarOne is a registered trademark of ScholarOne, Inc.
Terms and Conditions of Use - ScholarOne Privacy Policy

Γενικές συμβουλές για ασφαλή πρόσβαση

Μέτρα αυτοπροστασίας

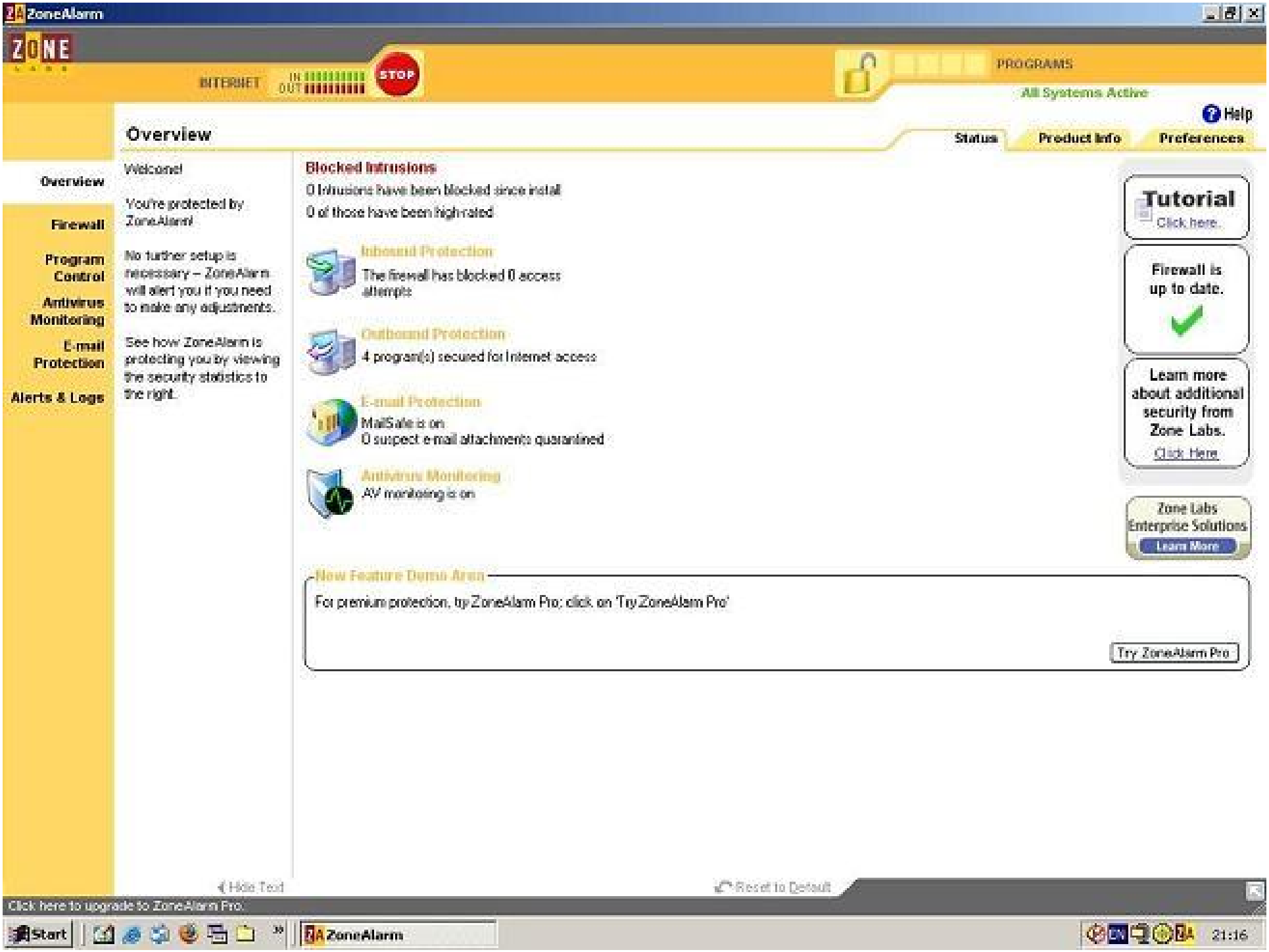
Γενικές συμβουλές και μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

11. **Να εγκαταστήσετε και να χρησιμοποιείτε σύστημα firewall.**
    - Δωρεάν εκδόσεις
      - Ashampoo, http://www2.ashampoo.com/
      - Zonealarm free firewall, http://www.zonealarm.com
      - Agnitum, http://www.agnitum.com/products/outpostfree/
      - COMODO, http://www.personalfirewall.comodo.com/
    - Εμπορικές εκδόσεις

12. **Να ελέγχετε τακτικά για πιθανές ανανεώσεις (updates):**
    1. Το λειτουργικό σύστημα του υπολογιστή
    2. τα προγράμματα πλοήγησης στο διαδίκτυο (web browser)
    3. Το λογισμικό antivirus / anti-spyware
    4. Το σύστημα firewall


Ashampoo FireWall
File Tools Settings Internet Help
Main Menu
Main Menu
Rules
Statistics
Logs
Configuration
Tools
Ashampoo fireWall
Learning Mode
Activated
Learn Mode is activated!
When an application for which no rules have been defined tries to establish a connection a dialog will be displayed . You can then decide whether you want the program to connect.
Block All
This option blocks all connections. This can be useful in some situations - for example if you suspect that a virus or Trojan horse program might be active in your system. Click on the icon on the left to block all connections.
Rules
Defined rules: 9
Edit rules
Connection Statistics
Monitored: 38
Blocked: 0
Allowed: 38
Tasks
Edit rules
View statistics
View logs
Firewall configuration


ZoneAlarm
ZONE
INTERNET
IN
OUT
STOP
PROGRAMS
All Systems Active
Help
Overview
Status
Product Info
Preferences
Overview
Firewall
Program Control
Antivirus Monitoring
E-mail Protection
Alerts & Logs
Welcome!
You're protected by ZoneAlarm!
No further setup is necessary – ZoneAlarm will alert you if you need to make any adjustments.
See how ZoneAlarm is protecting you by viewing the security statistics to the right.
Blocked Intrusions
0 Intrusions have been blocked since install
0 of those have been high-rated
Inbound Protection
The firewall has blocked 0 access attempts
Outbound Protection
4 program(s) secured for Internet access
E-mail Protection
MailSafe is on
0 suspect e-mail attachments quarantined
Antivirus Monitoring
AV monitoring is on
Tutorial
Click here.
Firewall is up to date.
Learn more about additional security from Zone Labs.
Click Here
Zone Labs Enterprise Solutions
Learn More
New Feature Demo Area
For premium protection, try ZoneAlarm Pro; click on 'Try ZoneAlarm Pro'
Try ZoneAlarm Pro
Hide Text
Reset to Default
Click here to upgrade to ZoneAlarm Pro.
Start
ZoneAlarm
21:16

Γενικές συμβουλές και μέτρα αυτοπροστασίας

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

13. **Να χρησιμοποιείτε πάντα κωδικούς ασφάλειας (passwords) για την πρόσβαση στον υπολογιστή σας.**

14. **Οι κωδικοί ασφάλειας πρέπει να ανανεώνονται συχνά και να είναι ισχυροί.**
    - Πάνω από 8 χαρακτήρες
    - Συνδυασμός κεφαλαίων, μικρών, αριθμών, συμβόλων
      - PK123 (χαμηλή ασφάλεια)
      - @dmin1$trat0R
      - #lo$T83+!bot3 (υψηλή ασφάλεια)

15. **Μην αποκαλύπτετε ή μοιράζεστε τους κωδικούς ασφάλειάς σας με κανέναν!**

Προστασία

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

- Συνολικά
  - Πλήρης γνώση για το περιεχόμενο ενός συνημμένου αρχείου
  - Ενημερωμένα λειτουργικά συστήματα και εφαρμογές
  - Να μην χρησιμοποιούνται features στις εφαρμογές όπου αυτοματοποιημένα λαμβάνουν ή εκτελούν αρχεία
  - Δεν πρέπει να ανοίγονται email attachments με file extensions: VBS, SHS, SRC or PIF ή διπλά file extensions: NAME.BMP.EXE or NAME.TXT.VBS
  - Να εμφανίζεται πάντα το file extension στα windows : through Explorer via the Tools menu: Tools/Folder Options/View - and uncheck "Hide file extensions for known file types".
  - Τα file attachments των emails που φέρουν εικόνα μπορεί να είναι επικίνδυνα
  - Τα file attachments των emails που φέρουν κάποιο σεξουαλικό όνομα μπορεί να είναι επικίνδυνα
  - Αποσύνδεση του υπολογιστή από την πρόσβαση στο internet όταν δεν χρησιμοποιείται
  - Αποφυγή σε file downloading από sites που δεν είναι της πλήρης εμπιστοσύνης

Συμβουλές για ασύρματη πρόσβαση στο διαδίκτυο

Μέτρα αυτοπροστασίας

Μέτρα αυτοπροστασίας για ασύρματα δίκτυα

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

16. **Ενεργοποιείστε τους μηχανισμούς κρυπτογράφησης στον ασύρματο δρομολογητή (wireless router)**
    - WPA2 (περισσότερο ασφαλές)
    - WPA-PSK
    - WEP-128
    - WEP-64 (λιγότερο ασφαλές)

17. **Απενεργοποιείτε το μηχανισμό «identifier broadcasting»**

18. **Αλλάξετε τον προσδιοριστή SSID από την τιμή που έχει θέσει ο κατασκευαστής**

19. **Χρησιμοποιείστε ένα ασφαλή κωδικό ασφάλειας για τον Ασύρματο Δρομολογητή, διαφορετικό από την τιμή που έχει θέσει ο κατασκευαστής**

20. **Να ρυθμίσετε το ασύρματο δίκτυο έτσι ώστε να δέχεται συνδέσεις μόνο από συγκεκριμένες ασύρματες κάρτες δικτύου (MAC address)**

Χρήσιμες πηγές ενημέρωσης – πληροφόρησης χρηστών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

1. GRNET-CERT, http://cert.grnet.gr/index.php
2. Greek School Network Emergency Report team http://cert.sch.gr/
3. http://www.dart.gov.gr/
4. http://www.antiphishing.org/
5. http://www.makeitsecure.org
6. http://www.adslgr.com/forum
7. http://www.staysafeonline.org/
8. http://onguardonline.gov/index.html
9. http://www.issa.org/
10. http://www.sans.org/reading_room/whitepapers/awareness/
11. http://www.securityfocus.com/
12. http://www.educause.edu/content.asp?page_id=8762&bhcp=1
13. http://www.itsafe.gov.uk/

Ευχαριστώ για την προσοχή σας

Ερωτήσεις;