Windows PC Privacy Guide

Securing Communications

I. Introduction – About Privacy

Privacy indirectly influence our thinking, decisions, and behaviors by;

1. protecting us from abuse or harm, such as from discrimination, retaliation, retribution, reprisal and vengeance of our beliefs and opinions, political afflictions and reputations;
2. from unreasonable government intrusion (meddling) into our personal lives and affairs;
3. by allowing us to form our own opinions, insights, perceptions, to exist independently and different.
4. through the separation of our personal information from public information;
5. by protecting our confidentiality, off the record, in personal matters;
6. by letting us have decency and dignity, such as when visiting the restrooms;
7. and by the respect for trust in our relationships.

Without the right of privacy, there is no real freedom of speech or freedom of opinion, and so there is no actual democracy.

"*Democracy requires opposing voices; it requires a certain level of reasonable political conflict. And it requires that government misdeeds be exposed. That can only be done when whistleblowers and people committing acts of journalism can do so without being spied upon.*" - **Dilma Vana Rousseff democratic President of Brazil**

"*Freedom of expression, in particular, freedom of the press, guarantees popular participation in the decisions and actions of government, and popular participation is the essence of our democracy*." **- Corazón Aquino democratic President of the Philippines**

Government must be answerable to the people. When the functions of government are privatized, all of that breaks down and government becomes answerable to profit. It's time to reestablish the clear dividing lines between government functions and corporate functions, between the public space and the private space.

Privacy is a core principle in any free society.

II. Software Applications – for Privacy

- **Bit Message**
- **DNScrypt**
- **uTorrent**
- **BTsync**
- **TOR**
- **GPG "Gpg4win" and "Gpg4o"**
- **GnuPGP "GoAnywhere OpenPGP Studio"**
- **PGPi and PGP**
- **OpenSSL**
- **S/MIME**
- **Thunderbird**
- **SoftEther VPN**
- **Boxcryptor**
- **HardEncrypt**
- **7z**
- **Wuala**
- **PeerBlock**

Bit Message https://bitmessage.org
Unlike webmail that offers zero privacy, "Bit Message" encrypts your message using AES 256 and delivers it over a decentralized P2P network. Works with the TOR network for increasing your anonymity. It's also built using open source code and offers a portable no install mode and is given away freely at no cost.

DNSCrypt http://dnscrypt.org
Adds elliptic curve cryptography encryption and authentication to your DNS queries. When you type a name in the URL field of a web browser, you expect to go to the appropriate web site. But if something or someone is messing with the DNS query, that may not be the case. For example, instead of going to your bank's website, you may be sent to a very good copy of the actual website specifically to steal your banking credentials.

In addition, interception of your DNS queries reveal every site you visited, geolocation and provides for DNS hijacking, redirection, impersonation, phishing, spoofing and censoring.

uTorrent http://www.utorrent.com or **http://www.bittorrent.com**
uTorrent lets you publish your files or newsletter to lots of other people using the bit torrent protocol. In fact, the more your files are shared, the more copies will seed more downloaders by using their PC's to do it for you. It's a great way to distribute files and aids in both freedom of speech and privacy, given other downloaders distribute your files for you.

Note: v3.1 build 26595 (719 KB) MD5: 07B96DBE4770D3B0B1A50D6C5FF15FC3 is "advertisement free". Newer versions push advertising into the applications.

BTSync http://labs.bittorrent.com/experiments/sync.html
BTSync is a "File Synchronization" application. It provides AES 128 encryption over a P2P decentralized network. It supports "unlimited syncing size", "unlimited syncing devices" and "One-Way Synchronization"

Note: BTSync isn't a cloud storage solution, to sync files the service must be "on" at both ends (PC to PC/PCs).

TOR https://www.torproject.org
Free software using an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy. Basically, TOR makes it harder for government surveillance from learning what sites you visit and your physical location (IP Address).

GPG http://www.gpg4win.org
Gpg4win (GNU Privacy Guard for Windows) is Free Software that lets you encrypt files and messages such as used in email. GPG supports OpenPGP and S/MIME (X.509). The Outlook plugin GPGOL is compatible with Microsoft Outlook 2003, 2007, 2010 and 2013.

Note: GPG4O is the Germany made application, but isn't FREE (proprietary) and funded by BSI. However the creation of Gpg4win was supported by the BSI (Bundesamt für Sicherheit in der Informationstechnik). Which explains why Gpg4o actually works better than Gpg4win.

GnuPGP http://www.goanywheremft.com/products/openpgp-studio
A free GnuPGP application by Linoma Software GoAnywhere OpenPGP Studio is based upon RFC4880 and supports S/MIME. Which is partnered with IBM, Microsoft, VMware, Oracle, Red Hat and Novell and supports the development and promotion of the OpenPGP standard.

OpenPGP http://www.openpgp.org and **http://www.pgpi.org**
The "OpenPGP Alliance" is an open-source version of PGP that has become an IETF-approved standard specification. PGP/MIME is a standard defined in RFC 3156 which allows you to encrypt attachments together with the message body and to encrypt HTML mails.

PGPi http://www.pgpi.org
This is the free international variant of "**PGP**" created by Phil Zimmermann in 1991 and the source code is available for review.

PGP http://www.symantec.com
PGP is the commercialized version (proprietary software) sold for profit by Symantec Corporation.

OpenSSL http://www.openssl.org
An open source free toolkit for SSL/TLS. You can use this application to generate your digital ID's (certificates) for S/MIME X.590 v3 RFC 2634 and SSL v2 and v3, TLS v1 used by websites to secure connections.

S/MIME X.590 v3 RFC 2634
Asymmetric cryptography encrypts and signs messages based upon "exchanging keys".

Meaning the sender must use their private key with the receiver public key to encrypt a message. Of course, the receiver needs their private key and the sender's public key to decrypt the message. Which makes possible the mechanism of sharing of your public keys with everyone without compromising the security of your private key.

Note: OpenSSL lets you generate your own keys; the private "p12" and the public "cer" from a certificate authority as root that includes an intermediate authority certificate just like VeriSign®. However, yours are not already pre-installed or pre-loaded like VeriSign® or Microsoft®, so there is a need to import them and share the public CA and intermediate with your public certificate (digital ID).

Interestingly, S/MIME originated from GCHQ (1973) of the U.K, and somehow another group known as RSA Labs in the U.S. had independently duplicated the same work only a few years later (1976). Maybe they both had read the 1874 book by William Stanley Jevons describing the principles of asymmetric cryptography?

Later RSA Labs renamed this technique as CMS (Cryptographic Message Syntax). As of now the current version of S/MIME is X.690 v3.2 RFC 5751. The main difference between S/MIME and GPG (variants and forks) is through the implementation of keys. S/MIME uses certificate authorities for authentication of certificates. While GPG was setup for individual trust, one on one, not using a certificate authority.

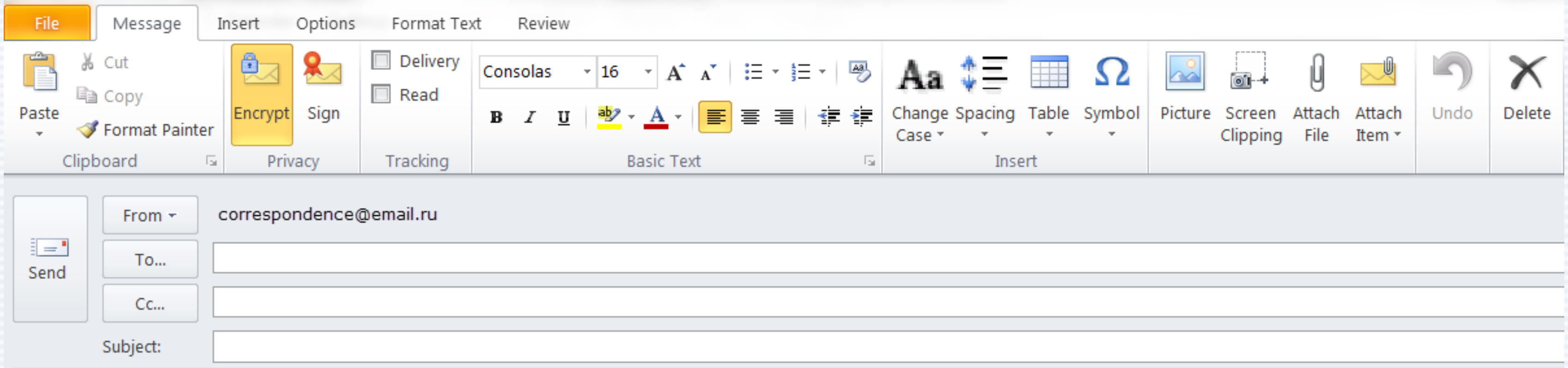
Another distinction between the two methods S/MIME and GPG, is how GPG displays in "**plain text**" the encrypted message inline of the message body. Whereas S/MIME stores the whole HTML message and any attachments into an encrypted "**smime.p7m**" file. So both methods have different advantages and drawbacks depending upon how you use them and what you need to do with them.

Both S/MIME and ALL GPG variants use prime number factorization for obscurity. This method makes computing devices invest " Computational Time" to resolve all the possibilities in obtaining the prime factorization of large numbers. What is the prime factorization of 6497864779319?

Outlook®, Windows® Live Mail (U.S.), Foxmail (Chinese), The Bat (Russian), KDE Kmail, Claws, and many other email clients all support S/MIME.

Note: Outlook® 2007 on XP supports 3DES 168 bit, whereas Outlook® 2010 on W7 supports AES 256 bit.

Outlook® 2010 - Email Client Screen Shot

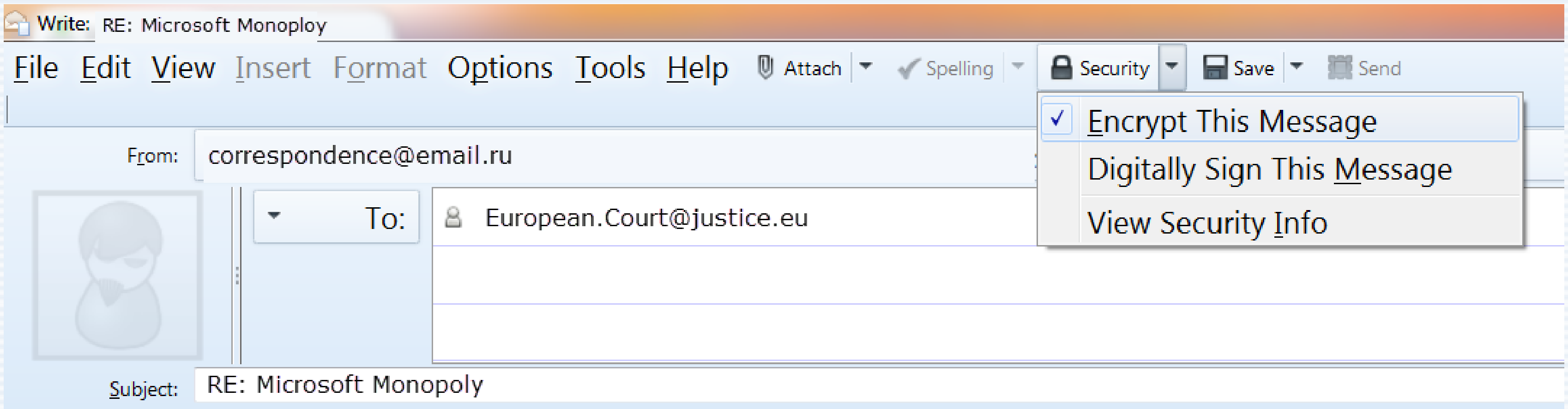


From ▾ correspondence@email.ru

Subject:

Thunderbird www.mozilla.org/thunderbird
An email client that comes with S/MIME support. Unfortunately, it has no option to select the cipher or hash, and the default sending setting is 3DES 168bit, although it can receive AES 256/SHA512.

Thunderbird v24 Email Client Screen Shot



Write: RE: Microsoft Monoploy

From: correspondence@email.ru

To: European.Court@justice.eu

Subject: RE: Microsoft Monopoly

✓ Encrypt This Message
Digitally Sign This Message
View Security Info

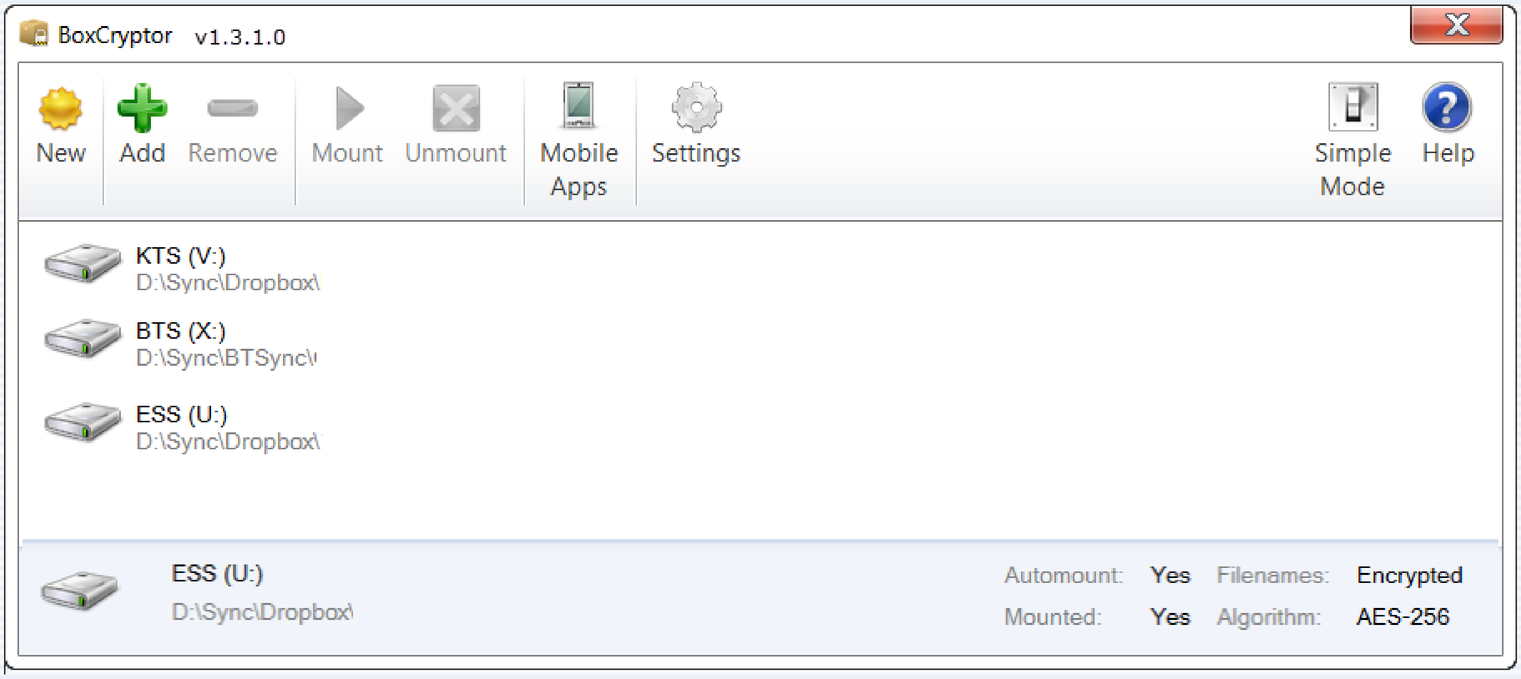
User can add-on support for GnuPGP and Enigmail (an interface for OpenPGP) as an extension. To add GPG to "**Thunderbird Portable**" just download [GPG for Thunderbird Portable 1.4.15 Rev 2] and install it right over your existing installation. Then download the [Enigmail extension] and install it into Thunderbird.

SoftEther VPN http://www.softether.org and Gate Relay Servers!
An open source code child project by the University of Tsukuba Japan. Using VPN allows access to global web services, because government often block foreign competition. You can use SoftEther for any personal or commercial use for free of charge too.

Download the special version of SoftEther VPN Client which has the "VPN Gate Client Plug-in".
http://www.vpngate.net/en/download.aspx

Boxcryptor https://www.boxcryptor.com
Lets you encrypt your data using client side AES 256 bit encryption before synchronize your files to the cloud storage service. Of course, you can use this for any cloud storage service.

Boxcryptor Application – Screen Shot



BoxCryptor v1.3.1.0

KTS (V:)
D:\Sync\Dropbox\

BTS (X:)
D:\Sync\BTSync\

ESS (U:)
D:\Sync\Dropbox\

ESS (U:)
D:\Sync\Dropbox\

Automount:	Yes	Filenames:	Encrypted
Mounted:	Yes	Algorithm:	AES-256

Boxcryptor Drive – Screen Shot

(U:) ESS

FAT32

67.7 GB free of 80.0 GB

Note: BoxCryptor v1.3.1.0 is FREE and includes "File Name Encryption". Later versions after 1.3.1.0 (05/16/2012) excluded out the file name encryption function by selling it back to YOU.

HardEncrypt http://hcsoftware.sourceforge.net/HardEncrypt/HardEncrypt.html
Uses symmetric encryption (instead of asymmetrical encryption) and source code is available.

7z http://www.7-zip.org
A free file archiver, that lets you encrypt file/s using AES 256 bit by using a password.

Wuala http://www.wuala.com
Cloud storage for backup, file synchronization, file sharing using client side encryption with 5GB storage for free. Note: the dependency of Java is unwelcomed.

Peer Block http://www.peerblock.com
Lets you control who your computer "talks to" on the Internet. By selecting appropriate lists of "known bad" computers, you can block communication with advertising or spyware oriented servers, computers monitoring your p2p activities.

III. TIPS on Privacy Protection

- **Passwords**
- **Javascript™**
- **Adobe® Flash®**
- **Java™**
- **Browser Cookies**
- **Ghostry**
- **MadMACs**
- **Windows® Activation Technology**
- **WSUS**
- **WPA2 AES**

Passwords
Always make passwords long and complex for maximum entropy!

Example

Weak	Strong
myname	Hawaiian.Moon.Rainbows@2014.hi
6 alpha characters lowercase only	30 ASCII Characters (Alpha, Numerical Digits, Symbols) Case Sensitive

JavaScript™

It's time to deprecate JavaScript. This language has no security awareness. It allows for cross site scripting (XSS), script escalation, cross site request forgery (hijacks cookies), JSON hijacking, Javascript and CSS attacks, Sandbox holes, DNS attacks. Recommendation is to disable, turn off and complain to those sites using it as it is very difficult for end user to migrate the risks.

Adobe® Flash®

Both Apple and Microsoft® have said publicly that Flash has issues with reliability, security, and performance. Symantec went on record publically warning wherever possible to disable Adobe® Flash®. So do yourself a favor and disable Adobe Flash until needed. You will be amazed how much faster your web pages load.

Java™

The Department of Homeland Security says despite some fixes to Java (Oracle), it continues to recommend users disable the program in their Web browsers, because it remains vulnerable to attacks that could result in identity theft and other cyber crimes. Software developers can eliminate this security risk altogether just by compiling their code for the intended platform directly rather than for Java. Recommendation, uninstall Java and free yourself of the unnecessary security risk.

Browser Cookies

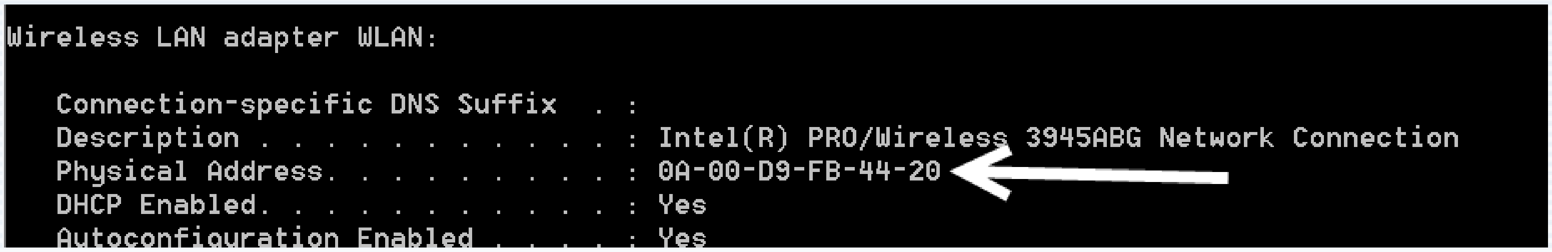
They are intrusive, unnecessary, raise privacy concerns and insecure. Ever wondered why all those ad-servers want to set cookies? Cookies allow sites to track users across sites. Do you want to be tracked and followed everywhere you go? Recommendation, turn them off, and tell your financial banking sites to stop using cookies as it is the wrong method to adapt.

Ghostry http://www.ghostery.com

Protecting your privacy by blocking over **1,655** trackers and **3,400** tracking patterns from advertising sites!
FREE Firefox Add-on: https://addons.mozilla.org/en-US/firefox/addon/ghostery

MadMACs http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer

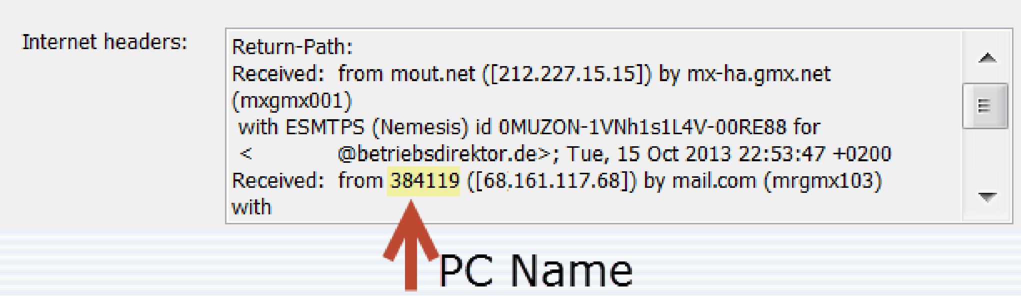
In Windows®, your **MAC Address** (a designation number assigned to your network adapter) exposes your PC identity that obviously can be used for tracking purposes that link back to YOU.



```
Wireless LAN adapter WLAN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Network Connection
   Physical Address. . . . . . . . . : 0A-00-D9-FB-44-20
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

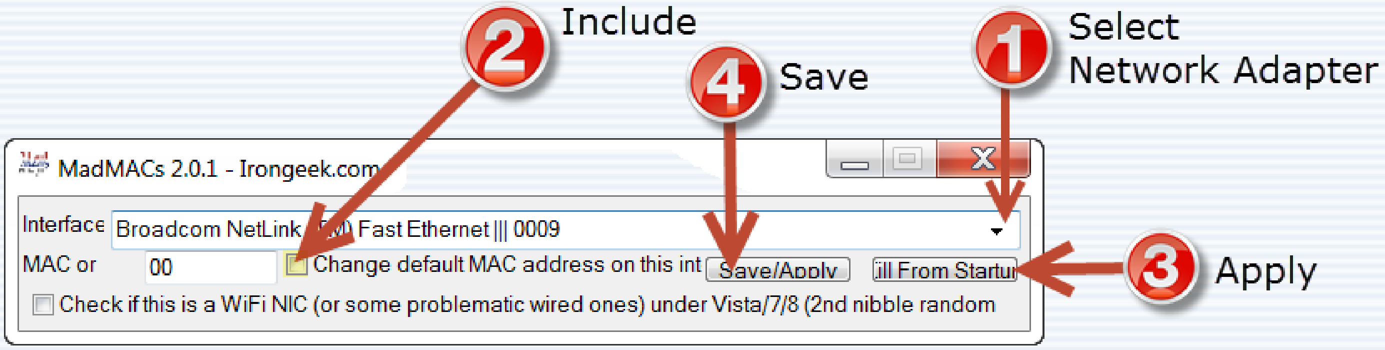
When sending email the Internet header of your message on Windows® PC gives away your "**PC name**" too.



Internet headers:

```
Return-Path:
Received: from mout.net ([212.227.15.15]) by mx-ha.gmx.net
(mxgmx001)
 with ESMTPS (Nemesis) id 0MUZON-1VNh1s1L4V-00RE88 for
 <           @betriebsdirektor.de>; Tue, 15 Oct 2013 22:53:47 +0200
Received: from 384119 ([68.161.117.68]) by mail.com (mrgmx103)
with
```

The PC name obviously can link back to YOU using your computer device.
IronGeek host a free application called “MadMACs” that will randomize both your "Mac Address" and "PC name". Get it here: http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer The source code is included with the download.



MadMACs 2.0.1 - Irongeek.com

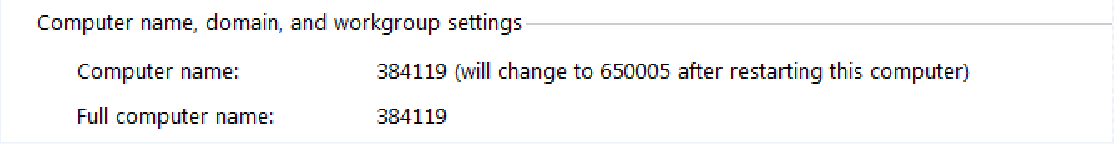
Interface: Broadcom NetLink (TM) Fast Ethernet ||| 0009

MAC or: 00 ☐ Change default MAC address on this int

☐ Check if this is a WiFi NIC (or some problematic wired ones) under Vista/7/8 (2nd nibble random

IronGeek MadMACs application, allows you use a text file named as "dic.txt" to provide your own randomize list of numbers, names as alias. It means, every time your reboot your PC, the computer gets a new randomized name and Mac Address, making it more difficult to link your device and online activities back to you.

Windows® 8.1 – Control Panel\All Control Panel Items**System** "Computer Name"



Computer name, domain, and workgroup settings

Computer name: 384119 (will change to 650005 after restarting this computer)

Full computer name: 384119

Windows® Activation Technology v3
Once the licensing terms are accepted and verified online through "Windows® Activation Technologies", additional on-going **validation submissions** will occur on every visit to the Windows® Update website.

In addition, to every time the PC is booted up and 24 hours later, the following information is collected, encrypted and transmitted back to Microsoft® as follows;

- Computer make and model
- Version information for the operating system and software using Genuine Advantage
- Region and language settings
- A unique number assigned to your computer by the tools (Globally Unique Identifier or GUID)
- Product Key (hashed) and Product ID

- BIOS name, revision number, and revision date
- Hard drive volume serial number (hashed)
- Whether the installation was successful if one was performed
- The result of the validation check, including information about any activation exploits and any related malicious or unauthorized software found, disabled or removed.
- The name and a hash of the contents of the computer's start-up instructions file (commonly called the boot file) to help us discover activation exploits that modify this file.

If your system is identified as non-genuine, the additional information will be sent to Microsoft®.

- Breach identifiers
- The breach's current state, such as cleaned, quarantined, or removed
- The scanning engine version
- Original equipment manufacturer identification
- The breach file name and hash of the file.

Source: Microsoft Genuine Advantage Privacy Statement – December 2008

Note: Microsoft® doesn't respect privacy period. Windows® is proprietary code. The solution here is to dump Windows®, switch over to open source **GNU**/Linux "FREE" code, that everyone loves and gets to review.

WSUS http://www.wsusoffline.net
Using "WSUS Offline Update", you can update any computer running Microsoft® Windows® 32/64 bit and Office® 2007, 2010, 2013 in multiple languages safely, quickly and without an Internet connection.

WPA2 AES
Wireless Protected Access 2 is a security technology commonly used on Wi-Fi wireless networks. If your setting up the wireless router;

1. change the default Gateway Router IP Address of: 192.168.1.1 ,
2. do not broadcast the 32 alphanumeric characters (Case Sensitive) SSID,
   AKXuTSSKzT77VeLwPbVl7FVLcx3nnFA5
3. always use AES instead of TRIP,
4. and use a random hexadecimal 63-character for the WPAS-PSK
   D425F074DD326D430D13930C1B41F2628BCFB4362D326B7D644826E7989BBC20
5. When using public WiFi access use an encrypted VPN connection as an additional layer of security.

http://prism-break.org list alternate applications that support privacy.

IV. Feedback or Suggestion?

What to know more about Privacy?

- ✓ Electronic Frontier Foundation https://www.eff.org/issues/privacy
- ✓ Privacy.org http://privacy.org
- ✓ Privacy International https://www.privacyinternational.org
- ✓ Privacy.net http://privacy.net

Perhaps, you would like to know something important about the economies: www.youtube.com/embed/iFDe5kUUyT0 The Truth About the Economy – Your Prosperity.

If you enjoyed the above here is another concept: http://www.youtube.com/embed/KphWsnhZ4Ag Paradise or Oblivion.

Nina Paley written, directed, produced and animated this free film: http://www.youtube.com/embed/f8LvBnz7oRA Site Sings the Blues.

Dedicated to the war-torn Zamboanga families. http://www.afs.ph