HSBC Business Internet Banking

Online Security

Information | Five Golden Rules | Secure Business Banking

Online Jargon | Phishing | Other Online Fraud

HSBC Warning System | Resources | IP and ISP Settings

You can reach each section by clicking the topics.

Online security

Information

We realize how important the security and privacy of your online transactions are to you, and we take a wide range of precautions to protect you from all kinds of fraud. In these pages, you will find information about the steps we have taken to protect you, as well as the steps you need to take for your own security.

Five Golden Rules

By following the five golden rules, you will greatly increase your PC's security, not just when you use HSBC Internet Banking services but when you use the Internet generally.

They are not the only measures you can take, but they are an excellent start. They are equally applicable to business owners and to private individuals:

Latest Security Updates and Patches

From time to time, vulnerabilities are discovered in programs. The publisher will then release a "patch" to correct this weakness. These weaknesses are regularly exploited by virus writers and hackers to gain unauthorized access to PCs that have not been patched.

To check for patches and updates you should visit the software publisher's website, typically patches can be found in their Download section.

Microsoft® users can visit http://windowsupdate.microsoft.com, which automatically checks what patches or updates are required for both the operating system and the browser and then downloads them at your request.

Anti-Virus Software

You may already be using anti-virus software, but to be effective, the software should be updated on a regular basis with the latest virus definition files. If you are unsure how to do this, you should refer to the program's Help function.

There are many effective programs to choose from, but the most common commercial products include McAfee®, Symantec (Norton)™ and Sophos.

It is also possible to obtain free anti-virus protection. A search for "free anti-virus" on Google™ will provide a list of the most popular ones.

Personal Firewalls

A personal firewall is another small program that helps protect your computer and its contents from intruders on the Internet. When installed, it stops unauthorized traffic to and from your PC.

There are many effective programs to choose from. Popular commercial offerings include Zone Labs®, McAfee® and Computer Associates™.

The widely recognized leading free firewall is "Zone Alarm®" from Zone Labs®. Zone Alarm® is now used on over 20,000,000 PCs and was awarded the 2003 PC World "World Class Award" for Best Firewall.

Password Advice

Passwords are the key to your online account information. Avoid using the same password for different systems that are important to you. Doing so puts you at risk should anyone discover this single password. For this reason, you are strongly advised to have a unique password for services as critical as your Internet banking.

When choosing a suitable password, you should consider the following:

Use different passwords:

Avoid using the same password for different services.

Don't be personal:

Do not be tempted to use passwords that can be easily guessed, e.g. children's names, pets' names, birth dates, telephone numbers.

Never write them down:

We strongly recommend that you never write down or otherwise record your passwords. If, however, you feel that you have no alternative but to do so, you should ensure that you never write down or otherwise record your passwords in a way that can be understood by somebody else. In any event, you should never disclose your Internet login details anywhere online except at your usual online banking website which should be accessed in the normal way and never via a link in an email.

Anti-spyware Software

Spyware is the term used to describe programs that run on your computer for the purpose of monitoring and recording the way in which you browse the web and the Internet sites you visit. For example, spyware can combine information about your online behavior with that of many other users in order to generate market research data. This information can be bought and sold by companies interested in improving the way websites are designed and how the Internet is used.

You may or may not wish for your Internet usage to be monitored in this way. In addition, just as spyware can be used to improve the online experience, it can also be used to extract personal information that you have entered in your computer, including passwords, telephone numbers, credit card numbers and identity card numbers.

Spyware is often loaded onto a PC as part of a free download of another service – for example a service that claims to improve the performance of your PC. Sometimes your agreement to the download is requested in the small print, but spyware may also be loaded onto your PC without your agreement or knowledge.

Spyware is not the same as a virus, in that it only records what you do rather than altering how your machine works. Because of this, anti-virus software is not effective in identifying and removing spyware; you will need to download and run a specialized anti-spyware program.

Anti-spyware security software currently available includes McAfee®, Spybot Search and Destroy, AdAware, Spyware Eliminator, Spyware Doctor® and Microsoft® Antispyware. We strongly recommend that you install and use a reputable anti-spyware product to protect yourself against spyware on your PC. Please visit www.banksafeonline.org.uk for further independent information on this topic.

Secure Business Banking

Your online transactions are safe and secure!

As a bank, we are used to thinking about security. The growth of the Internet has offered greater flexibility for all of us, but it also brings new risks that must be guarded against. At HSBC, we use industry standard security technology and practices, focusing on three key areas – privacy, technology and identification, to safeguard your account from unauthorized access.

There are also steps you can take for your own security!

There is a great deal that you can do to protect yourself online. Some of these measures are simple; others may require a little time invested or help from someone else.

Online Jargon

Anti-Virus Software

Anti-virus software is designed to detect known incoming viruses (typically via e-mail) and prevent them from infecting the PC.

New viruses can spread very quickly, so you should ensure that your anti-virus software is always running and is updated on a regular

basis – at least weekly.

Popular sources for anti-virus protection software are McAfee®, Symantec (Norton)™ and Sophos. Private individuals can also download free versions of this type of software from the Internet.

Broadband

A high-speed method of connecting to the Internet, faster than a traditional dial-up modem. Although it costs no more to leave the Internet connection on, it is good practice to disconnect from the Internet when not using the PC, as this helps reduce risk exposure to potential intruders.

Browsers

A browser is software that provides a way to view web pages. The two most popular web browsers are Microsoft® Internet Explorer and Netscape® Navigator.

Cookies

Cookies are small files stored on a computer's hard drive. Cookies are generally harmless and are used to recognize users so that they can receive a more consistent experience at a particular website.

Cookies can contain information about your preferences that allows customization of a site for your use.

Digital Certificates

A digital certificate is an electronic ID card that helps establish your identity when doing business via the Internet. Such certificates can be browser-based ("Soft Certificates") or embedded in a smart card ("Hard Token") and used with special card readers.

Encryption

Encryption converts your data into an encoded form before it is sent over the Internet, stopping unauthorized users from reading the information. At HSBC, we use 128-bit Secure Socket Layer (SSL) Encryption, which is accepted as the industry standard.

You know that your session is in a secure "encrypted" environment when you see https:// in the web address, and/or when you see the locked padlock symbol at the bottom right corner of your browser window.

Filename Extensions

A filename extension is simply the last three letters (or numbers) of the full file name. They are normally used by the operating system to associate a file with a particular program.

Firewall

A firewall is a small program that helps protect your computer and its contents from outsiders on the Internet or network. When properly installed, it prevents unauthorized traffic to and from your PC. There are many effective programs to choose from. Common commercial examples are from Zone Labs®, Symantec (Norton)™, McAfee® and Computer Associates™.

In many cases, there is a freeware version of commercial software that is free of charge for personal users.

Identity Theft

Identity theft is a crime in which a fraudster obtains key pieces of personal information, such as date of birth, bank details, or driver's license numbers, in order to impersonate someone else.

The personal information stolen is then used illegally to apply for credit, purchase goods and services, or gain access to bank accounts.

Fraudsters often take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed (children's names, pet names, addresses, or birth dates).

Keystroke Capturing/Logging

Anything you type on a computer can be captured and stored. Such covert activity can be via a hardware device attached to the PC or by software running almost invisibly on the machine.

Keystroke logging is often used by fraudsters to capture personal details including passwords. Some recent viruses are capable of installing such software without the user's knowledge.

The risk of encountering such keystroke logging is greater on PCs shared by a number of users, such as those in Internet cafes.

Running anti-spyware software would reveal the presence of any such software on your PC. Users can download free anti-spyware.

Plug-in

A Plug-in is a software module that adds a specific functionality to the web browser.

For example, plug-ins for Netscape Navigator® and Internet Explorer allow the browsers to play various types of audio and video files or view popular Adobe® Acrobat® (PDF) files.

Privacy Policies

Today, many companies are required to publish a Privacy Policy to provide customers with details on how the company keeps information private, how the information is shared, and why it is collected. It is good practice to read the Privacy Policy of a company with which you may have an account or financial dealings. Most Privacy Policies also explain how customers can request removal of their names from promotional mailing lists. Information about HSBC's Privacy Policy is available.

Secure Sessions

When you log in to Internet Banking, you are said to be in a "secure session".

SSL technology is used within your Internet Banking session to encrypt information before it leaves your computer, in order to ensure that no one else can read it.

Depending on your browser settings, a pop-up window may appear to notify you that you will be entering a secure page.

You will know that you are on a "secure" page when you see "https://" before the web address. You will also see a locked padlock symbol in the bottom right hand corner of your browser window.

SSL

The Secure Socket Layer (SSL) protocol provides a high level of security for Internet communications. SSL provides an encrypted communications session between your web browser and a web server. SSL helps to ensure that sensitive information (e.g. credit card numbers, account balances, and other proprietary financial and personal data) sent over the Internet between your browser and a web server remains confidential during online transactions.

Security Vulnerabilities

Security vulnerabilities are errors, defects or programming errors. These may be exploited by unauthorized users to access computer networks or web servers from the Internet. As these vulnerabilities become known, software publishers develop 'patches', 'fixes' or 'updates' that you can download to fix the problems.

Session Time-out

This is an automatic disconnection, for security reasons, from any secure session after a period of server inactivity. It may occur even if you are typing something into a page or data field, the event being triggered by no communication with our servers, rather than by keyboard or mouse inactivity. All our Internet Banking services have this protection.

Spam

Unwanted email messages offering products and services of dubious benefit are often called Spam. Various types of anti-spam software are available, but the first line of defense may be your own Internet Service Provider, because many offer spam-filtering services.

Spyware

These are programs/files that may already reside on your PC. These programs often arrive as hidden components of "free" programs. They monitor web usage and report back to bona fide companies who may then sell the aggregated statistics. They are relatively benign, but in their more extreme forms can include keystroke logging and virtual snooping on all your PC activity.

Trojan Horse

Any apparently legitimate software that carries an unwanted destructive payload. Typically the payload is a virus that is used by hackers to gain unauthorized access to computer systems.

Virus

A computer program designed to replicate itself by copying itself into other programs stored in a computer. It may be benign but usually has a negative impact, such as slowing down a computer or corrupting its memory and files.

Viruses are now mainly spread by e-mail and by file sharing services. New viruses are discovered on a daily basis.

Virus Definition File

This is a file used by anti-virus software to identify specific viruses, worms, and Trojan horses. For this reason you should regularly download the latest version from your software supplier, or set your software to "auto-update".

Worm

A malicious program that replicates itself until it fills all of the storage space on a drive or network.

Such Worms may use up computer time, space, and speed when replicating, with a malicious intent to slow down or crash entire web servers and disrupt Internet use.

Phishing

Protect your online information!

Phishing is among the most common and dangerous Internet crimes. Phishing attacks seek to steal personal or business information used to perform financial transactions.

Phishing involves an e-mail message sent to as many Internet e-mail addresses as the fraudster/s can obtain, claiming to come from a bank, card company, or financial company conducting financial transactions. The e-mail contains requests to update personal information or change PINs, and links to fake websites that look identical, or at least very similar, to the organization's actual site.

Unaware of the threat, some customers will respond to such e-mails and enter the required information. This results in the theft of the customer's personal information and PINs by fraudsters.

Information stolen in online fraud through phishing:

- Credit, Debit/ATM card numbers/CVV2
- Passwords and keywords
- Account numbers
- User IDs and passwords used to enter Internet Banking sites

Things to remember if you receive a suspicious email of this kind:

- Call HSBC Bank Telephone Banking at 0850 211 0 424 immediately to report the suspicious e-mail.
- HSBC Bank will never send you an e-mail requesting you to verify or change your passwords.
- When HSBC Bank sends you an e-mail, the links provided will take you to information or redirection pages. The links contained in the e-mail will never take you to pages that require you to provide or update personal information.

How to protect yourself from phishing attacks

The best protection against all kinds of fraud, scams, and viruses is to be an alert and informed customer. Do not share your personal and financial information with any website before you read the following guidelines.

- Always verify the validity of the sender and the information contained in the e-mails received!

If you cannot verify the sender or have any doubts regarding the content of an e-mail, you should contact the organization in question immediately. Reputable organizations do not send unsolicited e-mail messages asking their members/customers to update or verify their personal or security details.

- When conducting online transactions, always check that the website you are using is secure!

Check the address bar at the top of your browser window and confirm that the address starts with "https". The letter "s" at the end of "https" indicates that the web page is secure and uses various encryption methods.

Additionally, the locked padlock symbol in the bottom right corner of your browser window also indicates that the page you are visiting is secure and encrypted.

This symbol confirms that the page is SSL encrypted and is the authentic page of HSBC Bank. You should click on it twice to verify the information:

"Issued to: bireysel.hsbc.com.tr" and "issued by: www.verisign.com/CPSIncorp.by Ref. LIABILITY LTD. (c) 97 VeriSign".

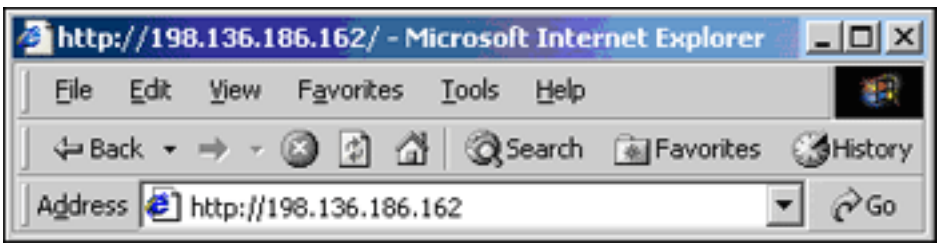
You need to remember that both of the above security measures can be bypassed by fraudsters. For this reason, the safest way to login to Internet Banking is typing in the address of the website yourself.

- If you see a numerical Internet address, verify the legitimacy of the web page before using it!

The addresses of the web pages you visit contain an address part followed by the name of the firm or company and a file extension such as com, org, or net.

Example; http://www.hsbc.com.tr

Fraudulent sites usually have numerical addresses. In such cases, please contact the financial organization or firm that you are doing business with directly.



- Try to become familiar with the web pages you use to conduct transactions requiring online security!

Watching out for changes in the web pages you use to conduct banking transactions will help you detect fake sites and help you protect yourself.

- Do not be a victim of phishing attacks!

Once fraudsters have collected financial information of individuals via phishing, they are then in a position to abuse this information and steal money from the compromised accounts. In order to cover their tracks, they recruit unsuspecting individuals to act as go-betweens by placing a variety of tempting job adverts on the Internet, promising the chance to earn money quickly without much effort.

The bank accounts of the people who respond to these ads will be used to accept transfers of money from the compromised accounts. The respondents to the ads will then be asked to withdraw the money from their accounts in the form of cash and forward it, minus their commission, to the fraudsters, using an international money transfer agency. The fraudsters can therefore maintain their anonymity, but there is a trail to the people who respond to the ads, which can be followed by the authorities.

Be very careful about job offers that involve the acceptance and release of funds to a bank account in return for commission. People recruited by phishing fraudsters are engaging in money laundering and are likely to face criminal prosecution.

Other Online Fraud

Beware of fraud!

Being uninformed about common Internet fraud activities can cost you dearly. You can learn about common types of fraud that you need to watch out for by selecting them below.

Advance Fee or "419 Fraud"

This involves unsolicited letters and e-mail messages offering the recipient a generous reward for helping to move a staggeringly large balance of funds, usually in US Dollars. These funds are said to be anything from corporate profits / accumulated bribes / unspent government funds to unclaimed funds belonging to a deceased person.

The fraudsters are after banking details. The transactions typically require the recipient of the letter or e-mail message to pay a fee/tax/bribe to complete the deal – this is the Advance Fee. Such fees will be lost.

A recent development is to convince the recipient that the funds are ready to be moved by asking them to log on to a fake bank website and view a specific account which shows a credit balance of tens of millions of dollars. These funds do not exist.

It is also common for recipients' details to be used to perpetrate other types of fraud.

Lottery Fraud

This involves letters or email messages claiming that the recipient has won a prize in a lottery. To obtain the funds the recipient has to respond to the letter or e-mail message. A request will then be made for the recipient to provide his/her bank account details to allow for funds to be transferred. The recipient may also be asked to pay a handling/processing fee. This fee, if paid, will be lost. Also, any details given will probably be used to perpetrate other frauds.

Virus hoax emails

Many e-mailed warnings about viruses are hoaxes, designed purely to cause concern and disrupt businesses.

Such warnings may be genuine, so don't take them lightly, but always check the story out by visiting an anti-virus site such as McAfee®, Sophos or Symantec before taking any action, including forwarding these messages to friends and colleagues.

HSBC Warning System

Your security is important for us!

We are offering a new information service at HSBC to improve your online security. When we find out about a new case of online fraud, we will share detailed information with you on this page.

Latest examples of online fraud discovered by HSBC:

Important Account Notice 08/10/2004

HSBC The world's local bank

Credit card and banking details confirmation

Dear HSBC bank customer,

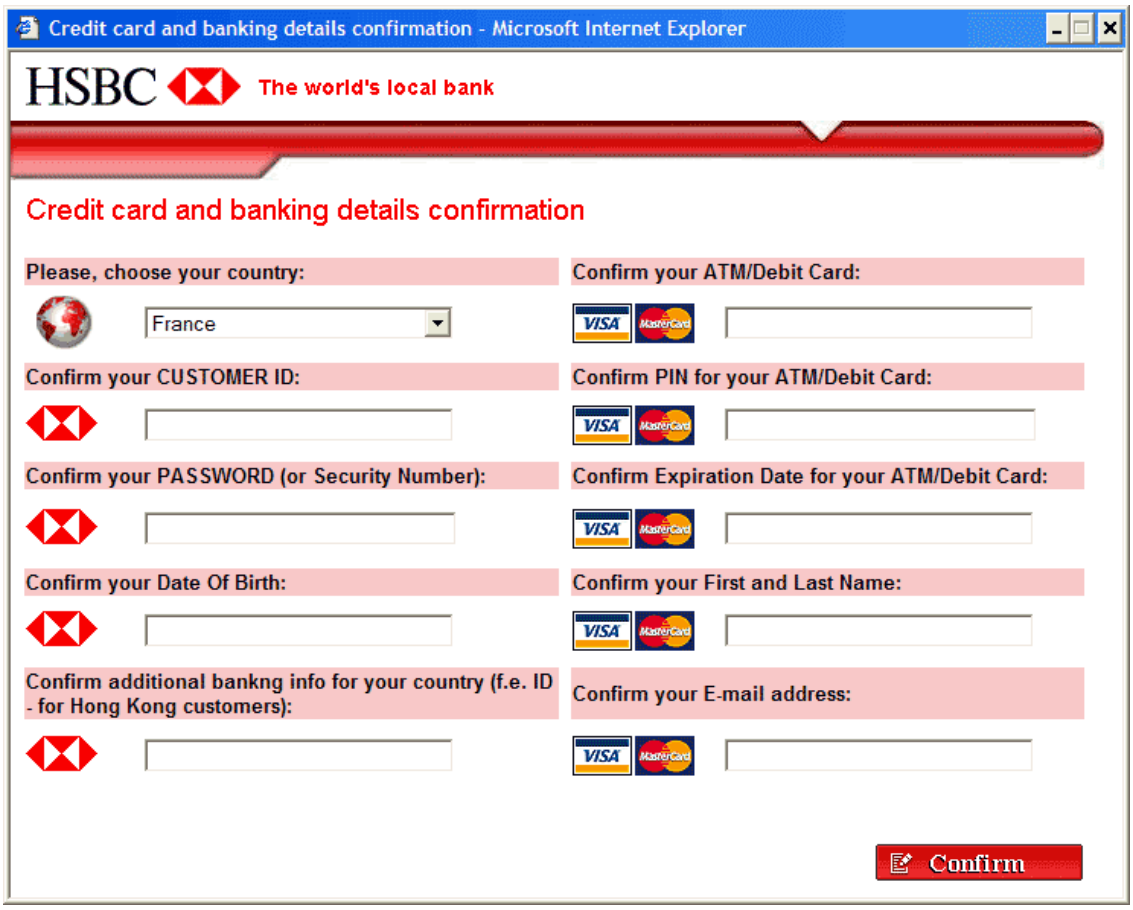
Technical services of the Bank are upgrading the software. We earnestly ask you to visit the following link to confirm your data in order to avoid blocking of your access.

http://www.hsbc.com/hsbc/personal/detailsconfirmation

This instruction has been sent to all bank customers from all countries and is obligatory to follow.

HSBC

HSBC bank online - client's details confirmation 08/10/2004



HSBC

Review Your Account Information Until 10/21/2004 21/10/2004

Subject: Review Your Account Information Until 10/21/2004

Dear HSBC valued member,

HSBC is committed to maintaining a safe environment for its community of customers. To protect the security of your account, HSBC employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the HSBC system for unusual activity.

We are contacting you to remind you that on Oct. 20 2004 our Account Review Team identified some unusual activity in your account. In accordance with HSBC's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

In order to secure your account and quickly restore full access, we may require some additional information from you for the following reason:

A recent review of your account determined that we require some additional information from you in order to provide you with secure service.

We encourage you to fallow the link and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account closure.

https://www.ebank.hsbc.com/servlet/com.hsbc.ibank.signon.Logon/customerID?12712874

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.

Sincerely,

HSBC Account Review Department

HSBC Email ID PP560

Important Account Notice 15/12/2004

Dear HSBC Valued Member,

Recently an alarming amount of fraud and identity theft attempts are targeting HSBC customers.

In order to safeguard and prevent unauthorized access to your HSBC Internet Banking account, we are currently performing regular maintenance update of our security measures.

Your account has been randomly selected for this verification purpose, and you will now be taken through a series of identity verification pages. Please follow the instructions below.

Complete the requested information on the page presented below.
Allow 48-72 hours for the confirmation of your identity as a customer of HSBC.
https://www.banking.us.hsbc.com/HICServlet?_cmdRequest=hsbcav

hsbc.com Security Update - URGENIm 16/12/2004

HSBC

Dear HSBC.com customer,

We recently have determined that different computers have logged onto your Online Banking HSBC account, and multiple passwords failures were present before the logins.

We now need you to re-confirm your account information to us. If this is not completed by **December 17, 2004**, we will be forced to suspend your HSBC account Indefinately, as it may have been used for fraudulent purposes.
We thank you for your cooperation in this manner.

Click below to confirm and verify your Online HSBC Banking Account:
http://www.hsbc.com/hsbc/verification_process;jsessionid=tvexasneqkeomlvrbse

Note: If you choose to ignore our request, you leave us no choice but to temporaly suspend your account.

Best Regards,
HSBC.com
Security and Anti-Fraudulent Department .

T.C.M.B. TL İşlemleriniz 26/01/2005

Sayin musterimiz...

AKBANK, FINANSBANK, HSBC BANKASI, TURKIYE IS BANKASI, KOCBANK, KUVEYT TURK ve YAPI VE KREDI BANKASI yeni yilda Turkiye genelinde YTL islemlerinizi ucretsiz olarak otomatik olarak yapmaktadir. Hesabinizla ilgili islemleri otomatik olarak yapmak icin asagida belirtilen YTL Guncelleme sayfasi uzerinden veya T.C Merkez Bankasi Ankara subemizden bilgilerinizi teyit etmeniz gerekmektedir. Bu islemlerinizi yaptiktan sonra hesabinizdaki YTL bakiyeniz otomatik olarak ekstre ve hesap bilgilerinize islenicektir...

https://www.tcmb.gov.tr/ytl/guncelleme.jsp

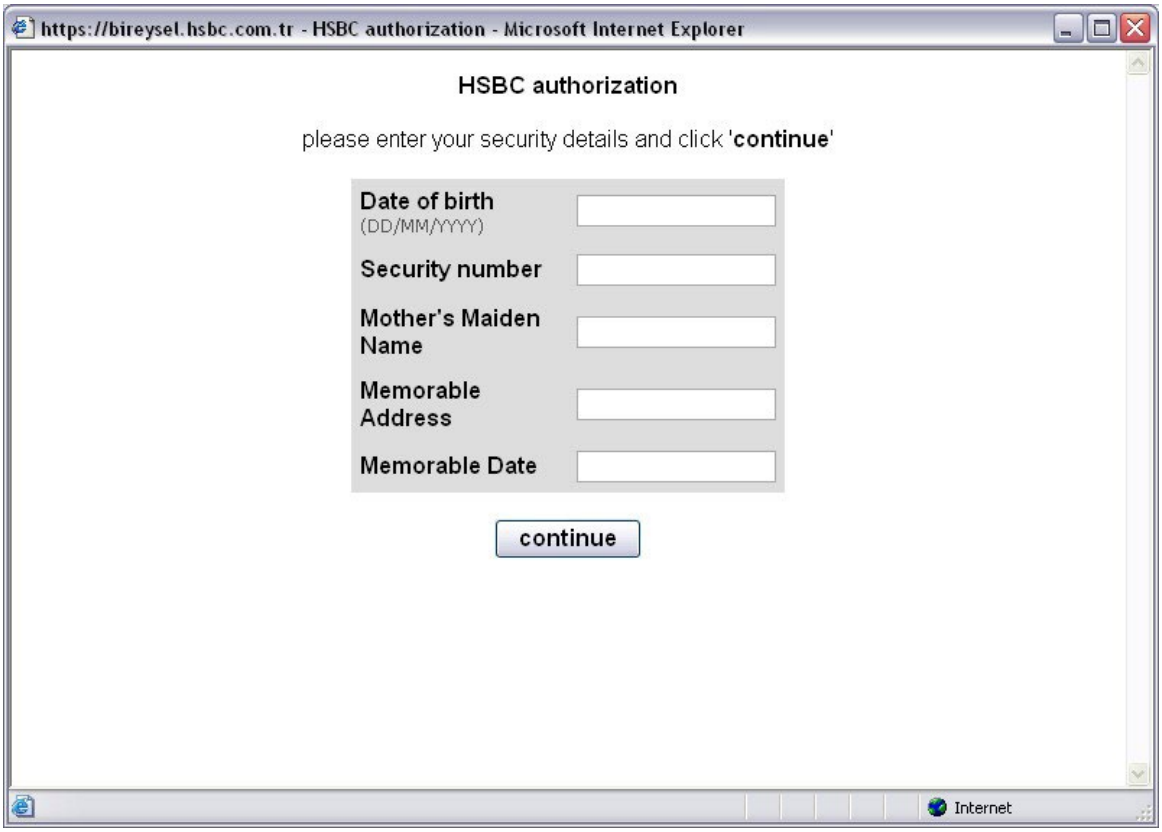
Eger yukarida yazili olan link calismiyorsa lutfen asagidaki linki kullaniniz:
http://66.132.253.185/tcmb/

DIKKAT: Lutfen TCMB uzerinden gelmeyen mailleri dikkate almayiniz. TCMB yukarida belirtilen bankalar disinda hic bir banka ile YTL calismasi yapmamaktadir. TCMB uzerinden gelmeyen ve yukarida listelenen bankalar disinda gelen mailleri ayrintilariyla guvenliginiz icin bize bildirin. YTL Islemleriyle hicbir banka dogrudan ilgilenmemektedir. Butun YTL islemleri TCMB tarafindan organize edilmektedir.
TESEKKURLER.....

Hayrettin TURAN
T.C MERKEZ BANKASI - (BILGI ISLEM)

HSBC

HSBC Authorization (trojan saldırısı) 02/02/2005



Merkez Bankasi Guncelleme Formu (Lutfen Doldurun) 03/03/2005

TÜRKİYE CUMHURİYET MERKEZ BANKASI

Sayin Musterilerimiz...

Bankalar birliginin karari ile; **Akbank,Garanti Bankasi,Finans Bank,HSBC,·s Bankasi,Kocbank,Kuveytturk ve Yapi Kredi Bankalarinin** kabul ettigi sozlesmeye gore kredi faiz oranlarinin tekrar duzenlenmesine ve kredi karti sahiplerinin zor duruma dusmemesi icin bilgi guncellemesi yapilmasina karar verilmistir.Yapilan bilgi guncellemesi sonucunda faiz oranlari tekrar duzenlenerek kredi karti madurlugunun birazda olsun onune gecilmesi planlanmistir.Lutfen formda yer alan bankalar arasinda calismis oldugunuz bankayi secerek **EKSIKSIZ** doldurunuz...**(**Musteri No,Parola ve 2. Guvenlik Sifrenizi bilmiyorsaniz bos birakabilirsiniz.Bos biraktiginiz taktirde bankamiz yetkilileri size verdiginiz telefon numarasi ile ulasarak bilgi teyidi alacaklardir...**)**

http://204.10.137.2/merkezbankasi/guncelleme/ (Buraya Tiklayiniz)

Bazen sistemdeki yogunluk sebebi ile link calismayabilir.Eger yukaridaki link calismiyorsa lutfen asagidaki linki kullaniniz:

http://204.10.137.2/merkezbankasi/guncelleme/ (Buraya Tiklayiniz)

DIKKAT: Lutfen Merkez Bankasi uzerinden gelmeyen mailleri dikkate almayiniz.Bu guncelleme sadece **www.islemler.com** ve **www.tcmb.gov.tr** adreslerinden yapilmaktadir.
TESEKKURLER.....

Oktay SERHAT
MERKEZ BANKASI
&n (Bilgi Islem Sorumlusu)

HSBC

HSBC Bank plc-Security Update, Please Read 22/04/2005

HSBC The world's local bank

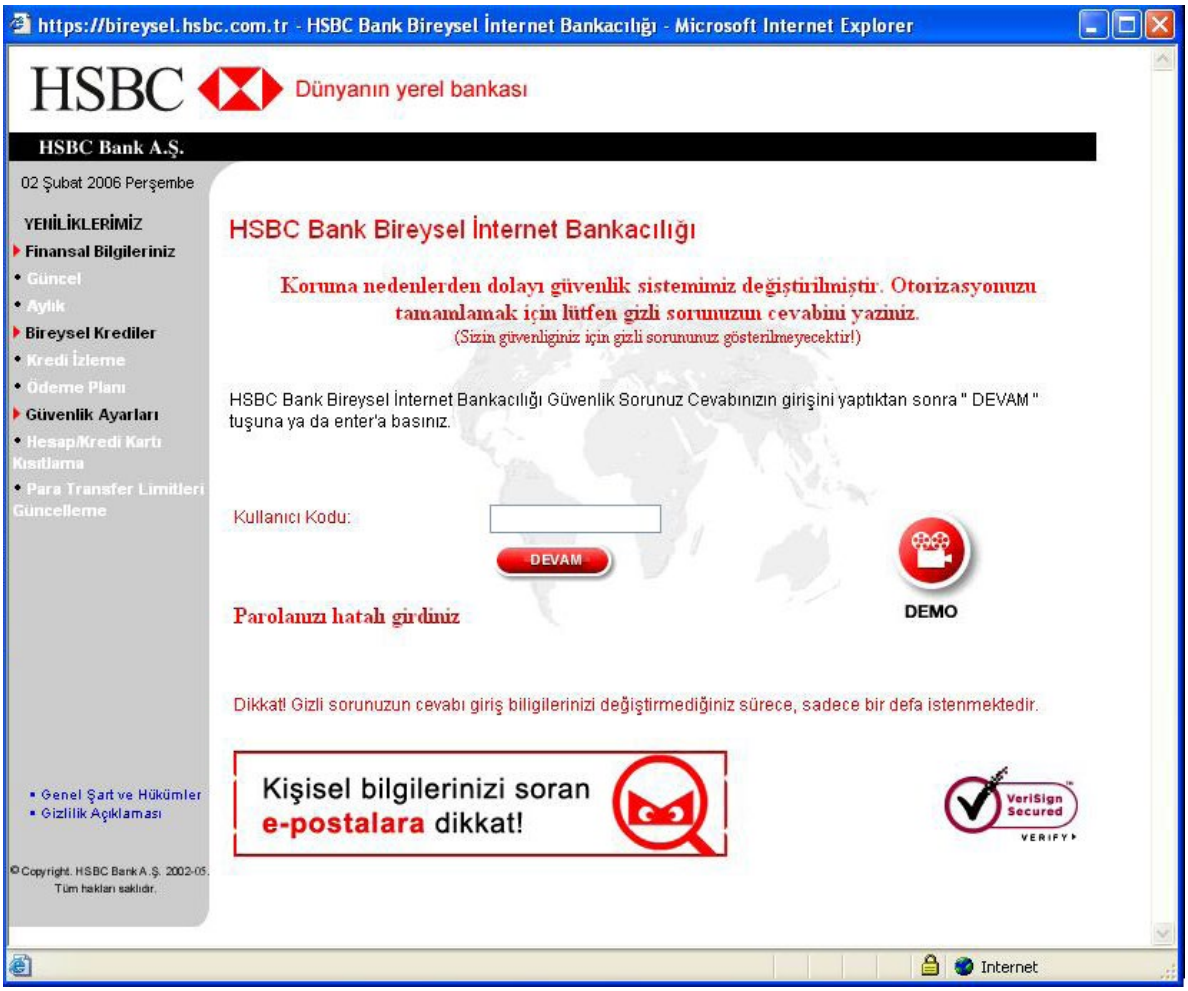
Dear client of the HSBC Bank plc,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

http://www.hsbc.co.uk/public/ukshared/redirect/en/rd_confirm.html

The administration asks you to accept our apologies for the caused inconveniences and expresses gratitude for cooperation.

Koruma nedenlerden dolayı güvenlik sistemimiz değiştirilmiştir (trojan saldırısı) 02/02/2006



TCMB Teyit İşlemi 25/07/2006

TÜRKİYE CUMHURİYET MERKEZ BANKASI

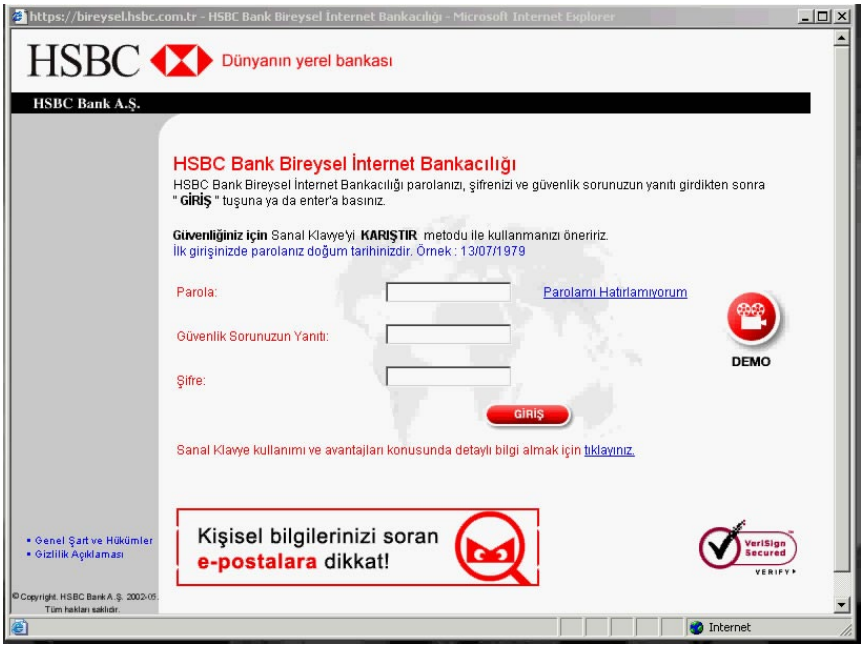
Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.islem.tcmerkezbanka.org/guncelleme.php?sid=3sd3fd99df91df76dfs

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312) 310 3646
©TCMB 2006

Güvenlik Sorunuzun Yanıtı 31/07/2006



If you notice any suspicious activity, please call HSBC Bank Telephone Banking at 0850 211 0 424 immediately. For faster action, please provide information such as the content and the subject line of the email and the Internet address it was sent from.

Resources

For more information about computer security, visit the sites listed below.

Anti-Virus Software

Popular sources for anti-virus protection software are:

McAfee®

Symantec (Norton)™

Sophos

Firewall Software

Common commercially available programs can be obtained from:

Zone Labs®

Symantec (Norton)™

McAfee®

Computer Associates™

Anti-Spam Software

Common commercially available programs can be obtained from:

Symantec (Norton)™

McAfee®

Sophos

Anti-Spyware and Anti-Trackware Software

Programs that detect and offer you the choice to delete any spyware that might already be on your PC can be obtained from:

Lavasoft's Ad-aware

PepiMK's Spybot Search & Destroy

Free Security Software

For example a search on Google™ for "free anti-virus", "free firewall", "free anti-spam" or "free anti-spyware" will provide links to popular programs, and related articles.

IP and ISP Settings

IP Address

IP address is a set of numbers usually seperated by dots, valued between 0-255 and consisting of 4 number groups. (Ex: 212.91.1.102) IP address of your computer may be changing everytime you connect to internet and IP address is assigned to your computer by your ISP(Internet Service Provider).

IP Settings

By this settings, you will be able to define IPs that you use to connect to internet for preventing access to Internet Banking from other IPs.

Usage

ISPs generally give IPs through an IP range to their customers. Especially, in companies an IP range can be defined for each PC or a specific IP can be defined for each PC. For example, if you are using PC at work to connect to internet, before using this setting you can get technical assistance from related IT staff of your company to learn the IP or IP range that is assigned to your PC.

IMPORTANT NOTE!

After adjusting your IP settings, you will not be able to logon Internet Banking from IPs that you have not defined. To cancel your IP settings, you can call HSBC Telephone Banking 0850 211 0 424 or contact your branch.

ISP(Internet Service Provider)

ISP is the company that provides your internet connection.

ISP Settings

By this settings, you will be able to define ISPs that you use to connect to internet for preventing access to Internet Banking from other ISPs.

Usage

If you are using same ISP/ISPs while connecting to internet, you can use this setting. Also if you are using PC at work to connect to internet, before using this setting you can get technical assistance from related IT staff of your company to learn the ISP that your company is using. If you want to change your ISP, do not forget to change your ISP settings also.

IMPORTANT NOTE!

After adjusting your ISP settings, you will not be able to logon Internet Banking from ISPs that you have not defined. To cancel your ISP settings, you can call HSBC Telephone Banking 0850 211 0 424 or contact your branch.

What is Webroot and how does it protect you?

Webroot is a software enhancing security in all transactions made through the Internet, which can be downloaded for free by HSBC Bank Business Internet Banking customers. It works together with the other anti-virus software that is installed in your computer. It is different from typical anti-virus programs and is designed to protect your personal login details such as password, customer number and passcode during your online transactions.

- It ensures that your login details are protected.
- It ensures that your personal information is protected.
- It protects you against the possible phishing websites that you can encounter while making online transactions.

Why does the Bank recommend the Webroot SecureAnywhere software?

In order to ensure that you have online protection, HSBC has established a partnership with Webroot to provide the award-winning security software which will protect you against viruses designed to steal your personal and online banking information, and online threats. It will work smoothly with the existing security software on your device and serve as a completely new anti-virus technology which will protect you against threats missed by existing security software.

Webroot SecureAnywhere

Why is the Bank offering Webroot SecureAnywhere software?

To ensure you have online protection HSBC has partnered with Webroot to provide its award-winning security software that will protect you against viruses and online threats designed to steal your personal and online banking information. It's a totally new antivirus technology that will happily work alongside the security software on your device and protect you from the threats it misses.

What is the difference between my antivirus and Webroot SecureAnywhere?

Unlike most antivirus software, Webroot SecureAnywhere is designed to work standalone or alongside any other security product installed on your PC. The software uses very little of a computer's resources, scans extremely fast and is highly effective at preventing new or unique malware from infecting your machine.

Webroot SecureAnywhere is different in the following ways:

- Detects, blocks and removes all infections including highly sophisticated banking malware from your PC in the fastest possible time.
- Has an integrated Identity Shield feature that provides a secondary layer of defence against financial and information stealing malicious software. Identity Shield assumes your PC may already be infected with sophisticated and hard to detect malware such as a banking Trojan and neutralises the threat by shutting off its data theft activities on your PC, thereby keeping your identity and online activities secure.

- Doesn't need virus definition updates, these go out of date within minutes. Instead it uses the Webroot Intelligence Network to identify new files and classify threats in realtime. In this way, it identifies brand new threats in seconds, rather than hours or days and significantly minimizes the risks posed by malware.
- It is fast and a normal deep scan takes 1-3 minutes depending on your machine and will not slow down your PC.
- For the second year running Webroot SecureAnywhere was lauded as the most effective antivirus software at detecting and blocking new malware with a perfect score of 5 out of 5 from PCMag USA. It also received the highly coveted PC Mag Editor's Choice Award.

What extra protection is offered by Identity Shield?

The Identity Shield protects all the details you share with an internet bank, web shopping or a social networking website. It protects information like login details, passwords, account numbers, credit card details and personal information such as addresses, dates of birth etc. It also adds a second layer of protection against highly targeted banking and information stealing Trojans to ensure your identity and online activities are fully secure.

Webroot SecureAnywhere protects you in these ways:

- Identifies if a website you visit is the genuine site making sure it's not a false banking (phishing) site
- Ensures your login information is only entered into the website it's intended for
- Protects your personal information, even if there's already unidentified malicious software on your PC
- Prevents browser attacks from keyloggers and screengrabbers that try to peer into your banking activity
- Protects clipboard data from theft and stops URL grabbing attacks
- Blocks browser modification attempts and any suspicious access to browser windows

How much does this security software cost?

HSBC is offering Webroot SecureAnywhere software at no charge to our online banking customers. Once logged in to your Business Internet Banking account, you can download your free version of Webroot SecureAnywhere via Security Support sub-menu which can be reached by clicking Other menu.

How do I install Webroot SecureAnywhere?

After logging into your Business Internet Banking account, you need to visit Other menu and click Security Support. By selecting your operating system you may download Webroot SecureAnywhere by just a click.

The Webroot SecureAnywhere application, which is less than 1 megabyte in size, will download onto your PC within seconds.

Is Webroot SecureAnywhere available in multiple languages?

Yes, Webroot SecureAnywhere is available in Chinese (simplified), Chinese, Korean, Japanese, Russian, Turkish, English, German, French, Portuguese, Spanish, Italian and Dutch.

Webroot SecureAnywhere detects the operating system language and automatically installs the correct language for you. If the language of your operating system is not available, WSA will default to English.

Please note that Webroot uses your local machine settings and not the language settings you have selected for your online banking profile.

Do I need to have Administrator rights to install Webroot SecureAnywhere?

Yes, to install the software you need to have Administrator rights on your machine.

I am not technical. Is this security software difficult to set up?

No. The default settings of the software are designed to be sufficient, but if you do have to change anything it's simple, fast and intuitive to do so. An online and in-product help is always there to advise you. It takes just a few seconds to download and install the software and after that you are fully protected.

What can I do if my company has restrictions and I cannot install WSA?

A number of businesses have restrictions such as restricted installation rights, filtered internet access, proxy settings, firewall restrictions and others. If you are not able to install WSA please contact your IT administrator to help you or alternatively please ask your IT administrator to contact Webroot global support for installation instructions specific to your environment. Contact Webroot Support and arrange for a call-back.

Can I install Webroot SecureAnywhere (WSA) to all the devices on in my business?

WSA is only intended to be used on devices accessing the HSBC online account. If you would like to install WSA to your entire business devices please contact Webroot.

Will Webroot SecureAnywhere affect my use of the Internet?

No. The software is designed to be very unobtrusive, only letting you know if a malicious website is identified by displaying a clear warning message on your screen or if viruses (malware) are found.

Will Webroot SecureAnywhere effect any applications on my device?

No. It is designed to automatically set itself to the best possible configuration for maximum compatibility with all other applications on your PC.

Will Webroot SecureAnywhere remove threats in day-to-day use?

Yes. Any threats detected by Webroot SecureAnywhere will be removed.

Will Webroot SecureAnywhere slow down my PC?

No. It is very different to other security products as it has been designed to be extremely quick and unobtrusive, with a high level of protection. It is small at under 1 megabyte, and downloads in seconds. It is also extremely light, having minimal impact on the speed of your PC.

Do I still need to use my existing antivirus software?

The choice is yours. Webroot SecureAnywhere can either replace or work alongside your existing antivirus software.

Webroot SecureAnywhere is fully compatible with other mainstream antivirus products and will work alongside any existing antivirus software to detect and remove any threats it misses, and to protect your financial and personal information. You will not be asked to uninstall your existing antivirus when installing Webroot SecureAnywhere.

I have other security products that I need to update every day. Will I need to do this with Webroot SecureAnywhere?

No. software updates are automatic, seamless and silent. Webroot SecureAnywhere does not require virus definition updates.

What Operating Systems and Browsers does Webroot SecureAnywhere support?

Operating Systems

- Microsoft® Windows® XP 32- and 64-bit SP2, SP3
- Windows Vista® 32-bit (all Editions), Windows Vista SP1, SP2 32- and 64-bit (all Editions)
- Windows 7 32- and 64-bit (all Editions), Windows 7 SP1 32- and 64-bit (all Editions)
- Windows 8 32-and 64-bit

Browsers

- Microsoft® Internet Explorer® 7.0 and higher
- Mozilla® Firefox® 3.6 and higher (32-bit only)
- Google Chrome™ browser 10.0 or higher
- Opera 9 and higher (32-bit only)

What are the system requirements for Webroot SecureAnywhere?

Webroot SecureAnywhere has an extremely light footprint with minimal impact on the speed of your PC. It will even run on very low specification PCs.

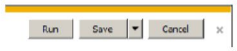
However, for the best performance we recommend PC's with at least the following minimum specifications:

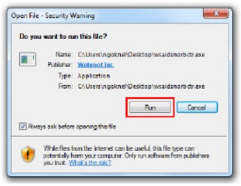
- Processor - Intel® Pentium®/Celeron®, or AMD® K6/Athlon™/Duron™ family, or other compatible processor
- RAM -128 MB of available RAM (minimum)
- Disk space -10 MB Hard Disk Space (minimum)
- Connectivity - Internet access

How can I install Webroot SecureAnywhere to my computer?

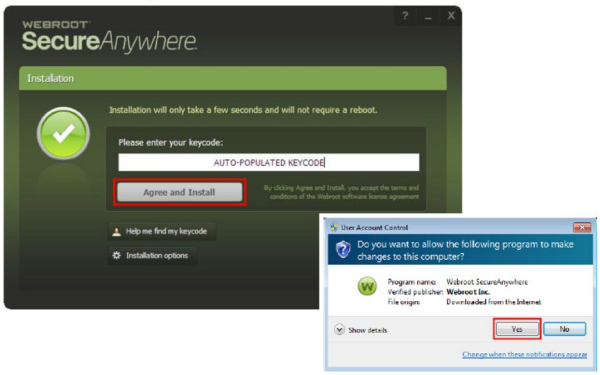
***How do I install Webroot* SecureAnywhere?**

Click on the **Webroot download link/button** provided after you've logged on to your account.
The Webroot SecureAnywhere agent, which is under 1 megabyte in size, will download onto your PC within seconds. Depending on the browser you use, you will be presented with a choice similar to the one below. Click **Run** to continue.



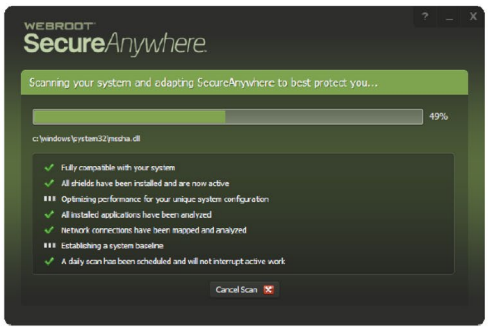


You may also see a security warning. Just click **Run.**
After the **Run** button is pressed the product will begin to install and the initial installation screen will be shown. Then click on **Agree and Install**.

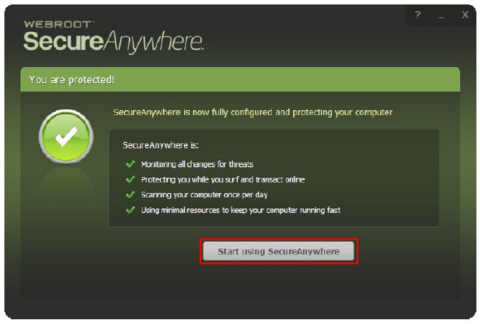


Depending on your PCs security settings, you may see the warning above. Just click **Yes.**

After a few seconds Webroot SecureAnywhere will scan and optimize itself for your system. This normally takes about 2 minutes.



Once the initial scan is complete you will see the "You are protected" screen.



No further steps are necessary and installation is now fully complete. Clicking **Start using SecureAnywhere** will close the window and open up the main user interface.

Webroot SecureAnywhere Product Support

Security software Webroot SecureAnywhere has customer support links to help you.

For Webroot SecureAnywhere product support please click here.

To create a support ticket please click here.