

HSBC Şirket Bankacılığı

Online Güvenlik

Bilgi | Beş Altın Kural | **Güvenli Şirket Bankacılığı**

Online Terimler | **Phishing** | Diğer Online Dolandırıcılık Yöntemleri

HSBC Uyarı Sistemi | Kaynaklar | **IP ve ISS ayarları**

Online güvenlik hizmetleri

Bilgi

Online işlemlerinizi güvenin ve gizliliğin sizin için ne kadar önemli olduğunu biliyoruz ve sizi türlü dolandırıcılıklardan korumak için pek çok önlem alıyoruz. Hem bizim aldığımız önlemler, hem de sizin yapmanız gerekenler için gerekli bilgilere bu sayfalarımızdan ulaşabilirsiniz.

Beş Altın Kural

Beş Altın Kural, uyduğunuz takdirde PC'nizin korumasını, sadece HSBC İnternet Bankacılığı hizmetimizi kullanırken değil, aynı zamanda genel olarak interneti kullandığınızda da önemli ölçüde artıran kurallardır. Bu önlemler, alınabilecek önlemlerin tamamı olmamakla birlikte iyi bir başlangıç oluştururlar. Bunlar, firma sahipleri ve bireyler için eşit derecede uygulanabilirliğe sahiptir:

Güncellemeler ve Yamalar

Bazı programlarda zaman zaman saldırıya açık noktalar keşfedilir. Bu durumda yayıncı bu zayıflığı düzeltici bir "yama" yayınlar. Bu zayıflıklar, virüs yazan programcılar ve program kırıcılar (hacker) tarafından yama ile onarılmamış olan kişisel bilgisayarlara yetkisiz erişim sağlamak üzere sürekli istismar edilir.

Yama ve güncellemeleri kontrol etmek için yayıncının web sitesini, özellikle Program İndirme (Download) bölümünü ziyaret edebilirsiniz.

Microsoft® kullanıcıları, hem işletim sistemi hem de tarayıcı programları (browser) için gerekenlerin otomatik olarak kontrol edilerek isterlerse bilgisayarına indirmelerine olanak sağlayan aşağıdaki web sitesini ziyaret edebilirler: <http://windowsupdate.microsoft.com>

Antivirüs Yazılımları

Halen bir antivirüs yazılımı kullanıyor olabilirsiniz. Ancak, bu yazılımın etkili olabilmesi için en yeni virüs tanımlamaları ile düzenli olarak güncellenmesi gerekir. Bunun nasıl yapılabileceğinden emin değilseniz, programın Yardım işlevine başvurun.

Ticari olarak piyasada bulunan pek çok etkili antivirüs programı bulunmaktadır. Ancak, en yaygın ticari ürünler arasında [McAfee®](#), [Symantec \(Norton\)™](#) ve [Sophos](#) sayılabilir.

Ayrıca, antivirüs korumasını ücretsiz sağlamak da mümkündür. Google™'da "free anti-virus" (ücretsiz antivirüs) araması yaparak en yaygın ücretsiz programların listesini elde edebilirsiniz.

Kişisel Güvenlik Duvarları (Firewalls)

Güvenlik duvarı, bilgisayarınızı ve bilgisayarınızda bulunan bilgileri internet üzerindeki yabancılardan korumaya yardımcı olan diğer bir küçük programdır. Kişisel bilgisayarınıza gelen ve bilgisayarınızdan giden yetkisiz trafiği kontrol eder.



Aralarından birini seçebileceğiniz birçok etkin program vardır. En yaygın ticari ürün örnekleri arasında [Zone Labs®](#), [McAfee®](#) ve [Computer Associates™](#) sayılabilir.

Yaygın kabul görmüş olan pazar lideri ücretsiz güvenlik duvarı [Zone Labs®](#) şirketinin ürettiği "Zone Alarm®" programıdır. Zone Alarm®, günümüzde 20.000.000'un üzerinde kişisel bilgisayarda kullanılmaktadır ve En İyi Güvenlik Duvarı için verilen PC World 2003 "World Class Award" ödülünü almıştır.

Şifre Önerisi

Şifreler, online hesap bilgilerinize erişimin anahtarıdır. Sizin için önemli olan farklı sistemlerde, aynı şifreyi kullanmaktan kaçının. Aksi takdirde, herhangi bir kişinin bu tek şifreyi keşfetmesi durumunda, riskiniz artmış olur. Bu nedenle, İnternet Bankacılığı işlemlerinizi kadar kritik olan her bir hizmet için ayrı bir şifre kullanmanızı şiddetle öneririz.

Uygun bir şifre seçerken, lütfen aşağıdaki noktaları göz önünde bulundurun:

Farklı şifreler kullanın:

Aynı şifreyi farklı hizmetler için kullanmaktan kaçının.

Kişisel olmayın:

Örneğin çocuk/evcil hayvan adları, doğum tarihleri, telefon numaraları gibi kolayca tahmin edilebilecek şifreleri kullanmaktan kaçının.

Şifreleri hiçbir şekilde bir yere not etmeyin:

Şifrelerinizi hiçbir şekilde bir yere not etmemenizi önemle öneriyoruz. Ancak, eğer kaydetmek dışında bir seçeneğiniz olmadığını düşünüyorsanız, şifrelerinizi hiçbir zaman başka birisi tarafından anlaşılabilir şekilde yazmadığınızdan emin olmalısınız. İnternet Bankacılığı login detaylarınızı asla bir e-posta'nın içindeki linkten ulaşılacak bir alana girmeyin.

Anti-spyware Yazılımlar

Casus Yazılımlar (Spyware) bilgisayarınızda çalışan ve web üzerinde gezinirken yaptıklarınızı ve ziyaret ettiğiniz internet sitelerini izlemeye/kaydetmeye yarayan programlardır. Örneğin, bir casus yazılım siz ve diğer birçok kullanıcının davranışlarını birleştirerek piyasa araştırma verisi üretmek için kullanılabilir. Bu bilgiler internetin nasıl kullanıldığı ve web sitelerinin nasıl daha iyileştirebileceği ile ilgilenen şirketler tarafından alınıp satılabilir.

İnternet kullanımınızın bu şekilde izlenmesini isteyebilir ya da istemeyebilirsiniz. Ancak bunlara ek olarak, casus yazılımlar sizin internet sitelerine girmiş olduğunuz şifre, telefon numarası, kredi kartı numarası, kimlik numarası gibi kişisel bilgilerinizi elde etmek için de kullanılabilirler.

Casus yazılımlar genelde başka bir servisin (Örn: Bilgisayarınızın performansını arttıracak bir servis) bilgisayarınıza ücretsiz olarak indirilmesi aşamasında bilgisayarınıza yüklenir. Bazen bilgisayarınıza yazılım indirme aşamasında sizden bir sözleşmeyi kabul etmeniz talep edilir. Ancak casus yazılımlar size herhangi bir bilgi verilmeden veya bu şekilde bir sözleşme olmadan da bilgisayarınıza yüklenebilir.



Casus yazılım bir virüs yazılımı değildir. Virüs gibi bilgisayarınızın çalışma şeklini değiştirmekten çok, sizin yaptıklarınızı kaydeder. Bu nedenle antivirüs yazılımları, casus yazılımları tespit etmek ve yok etmekte etkili değildir. Casus yazılımlara karşı özel anti-spyware programları kullanmanız gerekmektedir.

Piyasada casus yazılımlar için McAfee®, Spybot Search and Destroy, AdAware, Spyware Eliminator, Spyware Doctor® ve Microsoft® Antispyware gibi güvenlik programları bulunmaktadır. Bilgisayarınızı casus yazılımlara karşı koruyabilmeniz için bilinen anti-spyware ürünlerinden birini kurmanız ve kullanmanız şiddetle önerilmektedir. Daha ayrıntılı bağımsız bilgi almak için www.banksafeonline.org.uk adresini ziyaret edebilirsiniz.

Güvenli Şirket Bankacılığı

Online işlemlerinizi güvence altında!

Bir banka olarak, güvenlik konusunu düşünmeye alışkınsınız. İnternet'in yaygınlaşması hepimiz için daha fazla esneklik sağladı. Ancak, düşünülmesi gereken yeni riskleri de beraberinde getirdi. HSBC'de hesabınızı herhangi bir yetkisiz erişime karşı korumak için, üç temel alana (gizlilik, teknoloji ve kimlik saptama) odaklanan sektörde standart haline gelmiş olan güvenlik teknolojisi ve uygulamaları kullanılır.

Bizim Önlemlerimiz

HSBC'de hesabınızı herhangi bir yetkisiz erişimden korumak için üç temel alana odaklanmış olan ve sektörde standartlaşmış güvenlik teknolojisi ve uygulamalarını kullanıyoruz.

Gizlilik

İnternet Bankacılığı hizmetlerimizde sektörde standartlaşmış şifreleme tekniğini kullanıyoruz.

Güvenli Oturumlar

İnternet Bankacılığı'na girdiğinizde size güvenli bir oturumda olduğunuz bildirilir. Güvenli bir oturumda olduğunuzu URL adresinin, <https://> ile başlamasından ya da tarayıcı programınızın sağ alt köşesinde gösterilen [kilit sembolünden](#) anlayabilirsiniz.

Şifreleme

İnternet Bankacılığı oturumunuz süresince, kişisel bilgileriniz bilgisayarı terketmeden önce SSL teknolojisi kullanılarak şifrelenir. Bu, söz konusu bilgilerin kimse tarafından okunamamasını garanti eder. Tarayıcı ayarlarınıza bağlı olarak, güvenli bir sayfaya gireceğiniz yeni açılan bir pencere ile bildirilir.

Şifreleme, verilerinizi internet üzerinden gönderilmeden önce kodlanmış bir şekle dönüştürerek yetkisiz kullanıcıların bu bilgileri okumasını engeller. HSBC'de, sektörün standart seviyesi olarak kabul edilen 128-bitlik Güvenli Soket Kademesi (Secure Socket Layer, SSL) Şifreleme kullanılmaktadır.

İnternet Bankacılığı içerisinde tüm E-posta hizmetleri de, genellikle güvenli olmayan normal elektronik postanızdan farklı olarak, yukarıdakine benzer bir şifreleme teknolojisi ile korunur.



Oturum Zaman Aşımı

Online bankacılık işlemlerinden sonra oturumdan çıkmayı unutmanız ya da bir oturum esnasında bilgisayarınızdan belli bir süre işlem yapılmaması durumunda sistemlerimiz sizi otomatik olarak oturumdan çıkartır. Güvenli bir oturum esnasında izlemiş olduğunuz sayfalar kişisel bilgisayarınızın geçici dosyalarına kaydedilmez.

Teknoloji

Çok sayıda güvenlik kademesi kullanmaktayız. Doğal olarak bunların tümünü açıklamamız mümkün olmamakla birlikte aşağıdaki örnekleri verebiliriz:

- Bütün işletim sistemlerimiz en son güvenlik yamaları ile güncellenmektedir
- Antivirüs yazılımlarımız sürekli güncellenmektedir
- Yetkisiz saldırıları önlemek için güvenlik duvarları kullanılmaktadır

Kimlik Gizliliği

Sizinle işlem yaptığımızdan emin olmak için oturum girişleri (log-in) ve şifreler kullanıyoruz.

Hesabınıza online olarak erişebilmeniz sadece doğru Internet Bankacılığı kullanıcı kodu ve şifrenizi kullanarak kendinizi tanıtmanızdan sonra mümkündür. Bu nedenle, şifrenizi başkaları ile paylaşmamanız ve diğer hizmetlerle (örneğin, Yahoo®, Hotmail gibi) aynı şifreyi kullanmamanız hayati önem taşır.

Otomatik Giriş Kilitleme

Internet Bankacılığı'na, belli bir sayıda doğru olmayan giriş teşebbüsü yapıldığında hesabınıza online erişimi iptal ediyoruz. Hesabınızı tekrar aktif duruma geçirmek için HSBC Bank Telefon Bankacılığı 0850 211 0 424'i arayabilir ya da HSBC ATM'lerinden yeni şifre oluşturabilirsiniz.

Siz de önleminizi alın!

Kendinizi online bağlantıdayken korumak için yapabileceğiniz çok şey var. Bunlardan bazıları basit önlemler olmakla beraber, bazıları da biraz zaman ayırmanızı ya da başkalarından yardım istemenizi gerektirecek niteliktedir.

Sizin Önlemleriniz

Kendinizi online işlemler esnasında korumak için yapabileceğiniz çok şey vardır. Bunlardan bazıları basit önlemler olmakla birlikte bazıları da biraz zaman ayırmanızı ya da başkasından yardım almanızı gerektirebilecek niteliktedir.

Diğerlerinden hiçbirini uygulamazsanız dahi lütfen aşağıdaki [Beş Altın Kural](#)'ı uygulayın.

İşletim sisteminizin (örneğin, Windows XP®) ve Internet tarayıcınızın en son güvenlik güncellemelerine ve "yama"larına sahip olduğundan emin olun.

Antivirüs yazılımı kullanın ve bunu düzenli olarak güncelleyin.

Bir "kişisel güvenlik duvarı" (personal firewall) kullanın.

Şifrelerinizi gizli tutun ve bütün gereksinimleriniz için aynı şifreyi kullanmayın.



Daha ayrıntılı bilgi için lütfen aşağıdaki bilgileri okuyun

Kişisel kimlik ve diğer bilgilerinizi gizli tutun

Kimlik hırsızlığı bir bireyin kişisel bilgilerini kendi bilgisi ya da rızası olmaksızın, örneğin yasadışı olarak kredi başvurusunda bulunmak, alışveriş yapmak ya da fonlarına erişim sağlamak gibi, çalma ya da kullanma eylemidir. Dolandırıcı tarafından yaratılan hesap özetleri veya faturalar genellikle farklı bir adrese gönderildiğinden, mağdurun, kredi verenlerce durum araştırılana ya da kredi talebinin bunlar tarafından reddedilmesine kadar, artan borçlanmadan haberi olmayabilir. Kimlik hırsızlığının saptanması aylar alabilir, aydınlatılması ise daha da uzun sürebilir.

Aşağıdaki önerilere uyarak riskinizi azaltabilir ve ister Internet üzerinden ister normal bankacılık faaliyetleriniz esnasında olsun, bütün finansal işlemlerinizde kişisel bilgilerinizi koruyabilirsiniz:

Bu Önerilere Kesinlikle Uyun

- Nereden online bağlandığınıza dikkat edin
- Bilgilerinizin kopyalanıp sizden sonra tekrar girilme riskini önlemek için, mümkün olduğunca, Internet kafelerde, kütüphanelerde ve diğer halka açık yerlerde Internet Bankacılığını ya da herhangi bir kritik şifreyi kullanmaktan kaçının.
- Online dolandırıcılığın hilelerinden haberdar olun
- Sizi aldatarak kişisel bilgilerinizi toplamak üzere sahtekarlık amacı ile tasarlanmış web sitelerinin var olduğunu bilin. Bazen bu tür web sitelerinin bağları (link) finansal kurumlardan geliyormuş gibi görünen e-postalarda yer alabilir. Banka sayfalarına geçmek için, mümkün olduğunca bilinen bir web adresini ya da Sık Kullanılanlar seçeneğini kullanmayı deneyin.
- Şifrelerinizi değiştirin
- Tehlikeye maruz kalmış olabilecek şifrelerinizi daima değiştirin.
- Internet Bankacılığı şifrenizin bir başkası tarafından bilindiğinden kuşkulaniyorsanız bankanıza başvurun
- Bilgisayarınızı şifre ile koruyun
- Yetkisiz kişilerin bilgilerinize erişmesine engel olmak için bilgisayarınızda şifre kullanın.
- Tarayıcınızdaki "Otomatik Tamamlama" (AutoComplete) işlevini devre dışı bırakın
- Bu işlem başkalarının kişisel bilgilerinizi görmesine engel olacaktır. Örneğin Internet Explorer'da "Otomatik Tamamlama" işlevi, daha önce giriş yapmış olduğunuz verileri, bazen şifreler de dahil olmak üzere hatırlar. Genellikle tarayıcının kendi yardım sayfası bu işlemin nasıl yapılacağını anlatır.
- İyi tanınan şirketlerden ürün satın alın ve banka bilgilerini sadece güvenli oturumlarda girin.

Şifrenizi Gizli Tutun

Şifreler online hesaplarınızın, online mağazalardaki hesaplarınızın ve çok sayıda diğer faaliyetlerin anahtarıdır. HSBC Internet Bankacılığı şifreniz, banka hesaplarınıza erişebilmenize izin verir. Bu nedenle bu şifre tek olmalıdır ve iyi korunmalıdır.



Bu Önerilere Kesinlikle Uyun

- Şifrelerinizi saklı tutun
- Şifrelerinizi kesinlikle başka biri ile paylaşmayın.
- Benzersiz şifreler kullanın
- Başka birisi tarafından kolayca tahmin edilemeyecek benzersiz şifreler yaratmaya çalışın.
- Farklı şifreler kullanın
- Farklı hizmetler için aynı şifreyi kullanmaktan kaçının.
- Kişisel bilgiler kullanmayın
- Hatırlaması kolay olduğu için, adınız, doğum tarihiniz, telefon numaralarınız, evcil hayvanınızın adı gibi kolay tahmin edilebilecek şifreler kullanmayın.
- Şifreleri hiçbir zaman not etmeyin
- Eğer şifrenizi kaydetmeniz gerçekten gerekiyorsa bir kodlama sistemi kullanın, örneğin bazı harflerin sırasını değiştirin.

HSBC çalışanları hiçbir zaman size Internet Bankacılığı şifrenizi sormayacaktır. Eğer birileri size bunu soruyorsa, HSBC'yi temsil etmiyorlardır.

Bilgisayarınızın güvenliğini sağlayın

Internet, program kırıcılarına (hacker) sisteminize erişme olanağı sunmaktadır. Gerçekten Internet, web, film, müzik ve dosya vb.. indirmek için harika bir araç olmasına karşın, sizi çok büyük riskler altına sokabilir. Kendinizi korumak için alabileceğiniz birçok önlem bulunmaktadır.

İşletim sisteminizi (örneğin Windows XP®) ve tarayıcınızı düzenli aralıklarla güncelleyin.

Antivirüs programı kullanın ve bunu düzenli olarak güncelleyin.

Bir "Kişisel güvenlik duvarı" (personal firewall) kullanın.

Bu Önerilere Kesinlikle Uyun

• Bilgisayarları paylaşma açmayın

Yetkisiz erişimi engellemek için bilgisayarınızın 'Dosya ve Yazıcı Paylaşımı' fonksiyonunu kullanım dışı bırakın. Talimatlar için bilgisayarınızın Yardım işlevini kullanabilirsiniz.

• Dosya Adı uzantıları

Çoğu işletim sistemi dosya adı uzantıları kullanır. Örneğin bir Word belgesinin adı .doc ve bir fotoğraf görüntüsünün adı ise .jpg uzantısı ile sona erebilir.

Özellği gereği bazı işletim sistemleri bu uzantıları göstermez. Bu, daha net izlenebilen dosya adları sağlarken, bir yandan da virüslerin saklanabilmelerine yol açar. Dosya uzantılarının nasıl gösterileceğini öğrenmek için bilgisayarınızın Yardım işlevini kullanabilirsiniz.

Çift dosya uzantısına sahipmiş gibi görünen -örneğin wow.jpg.pif- bir dosya çok büyük bir ihtimalle bir virüs içermektedir ve kesinlikle açılmamalıdır.



- **Ekler içeren ve beklemediğiniz herhangi bir elektronik postayı açarken tedbirli olun**

Bir virüsün yayılması için en fazla kullanılan yol elektronik postadır. Bazı virüsler bulaştıkları kişisel bilgisayarın adres defterinde yer alan herkese kendilerinin kopyalarını gönderir. Bu da elektronik postanın sizin tanıdığınız birinden geliyormuş gibi görünmesi demektir.

Uzantı adı .exe, .pif, .vbs olan dosyaların eklenmiş olduğu bir e-postayı açarken dikkatli olun, zira bunlar virüsler tarafından en yaygın şekilde kullanılanlardır.

İnternet Bankacılığı oturumunuzun güvenliğini sağlayın

Sizin ve ailenizin diğer bireylerinin olası tuzaklardan ve bunlarla nasıl en iyi şekilde baş edilebileceğinden haberdar olduğundan emin olun. Üzerinde yoğunlaşılması gereken iki temel alan vardır.

- **Oturum açma (Logging in)**

Doğru şifre(leri)nizi, başka biri tarafından gözlenmediğinizden emin olduğunuz zamanlarda girin.

- **Oturum kapatma (Logging off)**

Online bankacılık işlemlerinizi sona erdiğinde hiçbir zaman İnternet Bankacılığı seansından çıkmayı ve tarayıcınızı kapatmayı unutmayın. Bu işlem ziyaretinizin kişisel bilgisayarın belleğindeki bütün izlerini silecektir.

Bu Önerilere Kesinlikle Uyun

- **Erişiminizi hatırlayın**

Online hizmetlerinize erişmek için İnternet Bankacılığı kimliğiniz (ID) ve şifreniz anahtarlarınızdır. Sadece bunların doğru kombinasyonları erişiminizi sağlayacaktır.

- **Sitemize erişmek için bağ (link) kullanmayın**

Daima web adresini girin ya da bir Sık Kullanılanlar seçeneğini kullanın. Teorik olarak, sizi aynen bizim sitemiz gibi görünen sahtekâr bir web sitesine yönlendirebilmesi mümkün olduğundan herhangi bir bağ (link) kullanmayın.

- **İnternet Bankacılığı için paylaşımlı bilgisayarları kullanmaktan kaçının**

İnternet Bankacılığına erişmek için İnternet kafelerdekiler gibi paylaşımlı, halka açık kişisel bilgisayarları kullanmaktan kaçınmaya gayret edin.

E-postalarınızın güvenliğini sağlayın

- Genellikle normal bir e-posta adresine gönderilen ya da böyle bir adresten gelen (örneğin adınız@hotmail.com) bir e-posta, içeriği korunmak üzere güvenliği sağlanmamıştır ya da şifrelenmiş değildir. Bu nedenle, bir e-posta içerisine dahil ettiğiniz herhangi bir kişisel bilgi, yetkisiz kişilerin eline geçme riski taşır. İnternet Bankacılığı kimliğinizi (ID) ve/veya şifrelerinizi hiçbir zaman kimseye e-posta ile göndermeyin.

Bu Önerilere Kesinlikle Uyun

- **Hassas bilgileri hiçbir zaman e-posta ile göndermeyin**

Kişisel bilgi talep eden ve beklemediğiniz e-postalara hiçbir zaman yanıt vermeyin.

- **Ekler içeren ve beklemediğiniz e-postaları açarken tedbirli olun**

Bir virüsün yayılması için en fazla kullanılan yol elektronik postadır. Bazı virüsler bulaştıkları kişisel bilgisayarın adres defterinde yer alan herkese kendilerinin kopyalarını gönderir. Bu da elektronik postanın, sizin tanıdığınız birisinden geliyormuş gibi görünmesi demektir. Hiçbir zaman uzantı adı .exe, .pif, .vb olan dosyaların eklenmiş olduğu bir e-postayı açmayın, zira bunlar virüsler tarafından en yaygın şekilde kullanılanlardır.



- **Internet Hizmet Sağlayıcısı (Internet Service Provider, ISP) olarak kimi kullandığınızı gözden geçirin**

Değişen fiyatları bir yana bırakılırsa, günümüzde ISP'ler gelen e-postalarda virüs koruması dahil olmak üzere çeşitli hizmetler sunmaktadır.

Bilgisayarınızı online olmadığınız zamanlarda bile koruyun

Online bağlantı yapmadığınız zamanlarda dahi, kendinizi korumak için yapabileceğiniz çok şey vardır.

Bunları, gizli bilgilerin kesinlikle gizli olarak saklanması olarak özetleyebiliriz.

Bu Önerilere Kesinlikle Uyun

- **Kişisel kimlik ve diğer bilgilerinizi gizli tutun**

Kullanıcı Kimliklerinizi (ID), şifrelerinizi ya da size özgü herhangi bir kişisel tanıtıcı bilgiyi/ ayrıntıyı başka birisi ile kesinlikle paylaşmayın.

Ayrıca kişisel bilgilerinizi, kaynağı doğrulanmadan ya da aramayı kendiniz yapmadığınız takdirde telefondaki bir kişiye ya da bir web sitesine aktarmamanız gerekir. HSBC çalışanları size hiçbir zaman telefonda Internet şifrenizi sormayacaktır. Şifrelerinizi hatırlamalısınız. Bu bilgileri cüzdanınıza ya da para çantanıza kesinlikle not etmeyin.

- **Hesap özetlerinizi okuyun**

Banka ve kredi kartı hesap özetlerinizi olağandışı herhangi bir işlem ya da para çekme olup olmadığını kontrol etmek üzere gözden geçirin ve herhangi bir farklılıktan şüphelendiğiniz takdirde derhal bankanızı durumdan haberdar edin.

- **Herhangi bir değişiklik olduğunda bankaya bildirin**

Kişisel bilgilerinizde herhangi bir değişiklik olduğunda (örneğin adres değişikliği) bize bildirin.

- **Banka bilgilerinizi, yani hesap özetlerini, çek defterlerini, güvenli bir yerde muhafaza edin**

- **Kredi ve Banka kartları**

Bir kartı iptal etmeyi planlıyorsanız (ya da geçerlilik süresi dolmuşsa), hesap numarası ve manyetik şeridi ikiye ayrılacak şekilde kartı keserek imha edin.

- Soyulma riskinizi en düşük düzeye indirin; kendinizin ve mallarınızın güvenliğini sağlayın
Çöpe attığınız herhangi bir kişisel bilgi konusunda dikkatli olun. Eğer mümkünse, makbuzları, önceden onaylanmış kredi kartı başvurularını, banka hesap özetlerini ve kişisel bilgi içeren herhangi bir belgeyi imha edin.



Online Terimler

Antivirüs Yazılımı

Antivirüs yazılımı (genellikle e-posta yoluyla) gelen bilinen virüsleri algılayıp bunların kişisel bilgisayarını kirletmesini önlemek üzere tasarlanmıştır.

Yeni virüsler çok hızlı bir şekilde yayılabilir. Bu nedenle, antivirüs yazılımınızın daima çalışır durumda ve düzenli olarak -en azından haftada bir- güncellenmiş olmasını sağlamanız gerekir.

Yaygın olarak kullanılan antivirüs koruma yazılımı kaynakları McAfee®, Symantec (Norton)™ ve Sophos'dur. Bireyler bu tip yazılımların ücretsiz sürümlerini internetten bilgisayarlarına indirebilir.

Casusluk Yazılımı (Spyware)

Bunlar halen kişisel bilgisayarınızda bulunması olası programlar/dosyalardır. Bu programlar genellikle "ücretsiz" programların saklı bileşenleri olarak gelir. Bunlar, web kullanımını izler ve bu toplanan istatistikleri daha sonra satabilecek olan gerçek şirketlere rapor eder. Göreceli olarak tehlikesizdirler, ancak, daha aşırı şekilleri klavye vuruşu kaydetme ve gerçekten her kişisel bilgisayar faaliyetinizi incelemeyi de içerir.

Dijital Sertifikalar

Dijital sertifika internet üzerinden ticaret yaptığınızda güvenilirliğinizin saptanmasına yardımcı olan bir elektronik kimliktir. Bu tür sertifikalar tarayıcı temelli (Yazılım Sertifikaları) ya da bir akıllı karta (smart card) saklı (Donanım Jetonu) olabilir ve özel kart okuyucuları ile kullanılabilir.

Dosya Adı uzantıları

Bir dosya adı uzantısı basit anlatımıyla tam dosya adının son üç harfidir (ya da rakamıdır). Bunlar normal olarak işletim sistemi tarafından bir programın belli bir dosyayla ilişkilendirilmesi için kullanılır.

Güvenlik Duvarı (Firewall)

Güvenlik duvarı, bilgisayarınızı ve bilgisayarınızda bulunan verileri internet ya da ağ (Network) üzerindeki yabancılardan korumanıza yardımcı olan küçük bir programdır. Uygun şekilde kurulduğunda, kişisel bilgisayarınıza gelen ve bundan giden yetkisiz trafiği önler. Aralarından seçim yapabileceğiniz çok sayıda etkin program vardır. Zone Labs®, Symantec (Norton)™, McAfee® ve Computer Associates™, yaygın ticari yazılımlara örnek olarak verilebilir.

Çoğu kez, ticari yazılımın kişisel kullanıcılar için ücretsiz bir sürümü de mevcuttur.

Geniş Bantlı

Geleneksel modeme oranla internete daha hızlı bağlanma yöntemidir. İnternet bağlantısının açık bırakılması maliyeti yükseltmemesine karşın, risklere maruz kalma olasılığını azaltmaya yardımcı olması açısından, kullanılmadığında bağlantının kesilmesi daha doğru bir uygulamadır.



Gizlilik Politikaları

Günümüzde, çoğu şirketin, müşterilerine şirketin bilgileri nasıl gizli tuttuğuna, paylaşıldığına ve ne amaçla toplandığına ilişkin ayrıntıları sunmaları için bir Gizlilik Politikası yayınlamaları gerekir. Hesap açabileceğiniz ya da finansal işlemler yapabileceğiniz bir şirketin Gizlilik Politikasını okumanız yerinde bir davranış olacaktır. Çoğu Gizlilik Politikası ayrıca müşterilerine tanıtım postalama listelerinden adlarının çıkartılmasını nasıl talep edebileceklerini de açıklar. HSBC'nin Gizlilik Politikası hakkında bilgi sahibi olabilirsiniz.

Güvenli Oturumlar

İnternet Bankacılığı'na girdiğinizde size bir "güvenli oturumda" olduğunuz bildirilir.

Başka kişilerin bilgileri okuyamamasını garanti edecek şekilde, verilerinizi internet üzerinden gönderilmeden önce kodlanmış bir şekle dönüştürmek için SSL teknolojisi kullanılır.

Tarayıcı ayarlarınıza bağlı olarak, güvenli bir sayfaya girdiğinizi bildirmek üzere yeni bir pencere açılabilir.

Web adresinden önce "https://" gördüğünüzde "güvenli" bir oturumda olduğunuzu anlayabilirsiniz. Ayrıca, tarayıcı programınızın sağ alt köşesinde kapalı durumda kilit sembolü de gösterilir.

Güvenlik Açıkları

Güvenlik açıkları, hatalar, arızalar ya da programlama hatalarıdır. Bunlar, yetkisiz kullanıcılar tarafından bilgisayar ağlarına ya da web sunucularına internetten erişmek için istismar edilir. Zayıf noktalar ortaya çıktığında, yazılım yayıncıları, bilgisayarınıza indirerek sorunları giderebilmeniz için 'yamalar', 'tamirler' ya da 'güncellemeler' geliştirir.

Kimlik Hırsızlığı (Identity Theft)

Kimlik hırsızlığı, dolandırıcının kişisel bilgiler, doğum tarihi, bankadaki ayrıntılar ya da sürücü belgesi numaraları gibi temel parçaları elde ederek, başkasının kimliğine bürünmesi suçudur.

Keşfedilen kişisel bilgiler daha sonra yasadışı olarak kredi başvurusunda bulunmak, mal ve hizmet satın almak ya da banka hesaplarına erişim sağlamak için kullanılır.

Dolandırıcılar genellikle insanların doğal olarak kendileri için anlamlı olan, ancak kolayca tahmin edilebilen (çocuklarının veya evcil hayvanlarının adları, adresler ya da doğum tarihleri) şifreleri seçme eğilimlerinden yararlanırlar.

Klavye vuruşu Yakalama/Kayıt tutma (Keystroke Capturing/Logging)

Bilgisayara girişini yaptığınız her şey yakalanarak kaydedilebilir. Bu gizli faaliyet, kişisel bilgisayara eklenmiş olan bir donanımla ya da makine üzerinde hemen hemen fark edilmeyecek şekilde çalışan bir yazılım tarafından gerçekleştirilebilir.

Klavye vuruşu kaydı genellikle dolandırıcılar tarafından şifreler de dahil olmak üzere kişisel bilgileri ele geçirmek için kullanılır. Son zamanlarda ortaya çıkan bazı virüsler, kullanıcının haberi olmaksızın bu tür yazılımları kurabilecek yeteneklere sahiptir.



Bu tür klavye vuruşu kaydı ile karşılaşmanın riski, internet kafelerdekiler gibi, birden fazla kullanıcı tarafından kullanılan kişisel bilgisayarlarda daha yüksektir.

Casus yazılımları önleyici (spyware) bir yazılım çalıştırılarak, bu tür bir yazılımın kişisel bilgisayarınızda mevcut olduğu tespit edilebilir. Kullanıcılar, bilgisayarlarına ücretsiz “casus yazılımı önleyici (spyware)” yazılımı indirebilirler.

Oturum Zaman Aşırımları

Bunlar, güvenlik nedenleri ile herhangi bir güvenli oturumun, sunucu belli bir süre boyunca faaliyetine ara verdiğinde, sona erdirilerek otomatik olarak bağlantının kesilmesidir. Bu işlem, bir sayfaya ya da veri alanına bir şeyler yazarken dahi ortaya çıkabilir. Çünkü olay, klavye ya da farenin kullanılmamasından ziyade, sunucularımız ile iletişime ara verilmesi ile tetiklenir. Bütün İnternet Bankacılığı hizmetlerimizde bu koruma mevcuttur.

Plug-in

Plug-in web tarayıcısına belli bir özellik ekleyen bir yazılım modülüdür.

Örneğin, Netscape Navigator® ve Internet Explorer tarayıcıları için plug-in'ler tarayıcıların çeşitli tiplerdeki ses ve görüntü mesajlarını çalabilmelerine/oyatabilmelerine ya da yaygın şekilde kullanılan Adobe® Acrobat® (PDF) dosyalarını görüntüleyebilmelerine olanak sağlar.

Rahatsız Edici E-Posta (Spam)

Şüpheli faydalar vadeden ürün ve hizmetler teklif eden istenmeyen e-postalara genellikle Rahatsız Edici e-posta (Spam) denir. Çeşitli tiplerde rahatsız edici postaları önleyici (anti-spam) yazılımları temin edilebilir, ancak, ilk savunma hattı, çoğu istenmeyen e-posta filtreleme hizmetleri sunan kendi İnternet Hizmet Sağlayıcınız olabilir.

SSL

Güvenli Soket Kademesi (Secure Socket Layer, SSL) protokolü internet iletişimi için yüksek seviyeli bir güvenlik sağlar. SSL web tarayıcınız ile web sunucusu arasında şifrelenmiş (kriptolanmış) bir iletişim oturumu sağlar. SSL hassas bilgilerin (örneğin kredi kartı numaraları, hesap bakiyeleri ve diğer özel finansal ve kişisel veriler) tarayıcınız ile bir web sunucusu arasında online işlemler esnasında gizli kalmasını sağlamaya yardımcı olur.

Solucan (Worm)

Kendini bir sürücü ya da ağ üzerindeki bütün saklama alanını doldurana kadar kopyalayan kötü niyetli bir programdır.

Bu tür solucanlar, kendilerini kopyalarken, bilgisayar çalışma süresini, saklama alanını ve hızını kötü niyetli bir şekilde kullanarak bütün web sunucularını yavaşlatabilir ya da tamamen çökertebilir ve internet kullanımını tahrip edebilir.



Şifreleme (Kriptolama, Encryption)

Şifreleme, yetkisiz kullanıcıların bilgileri okumasını engelleyecek şekilde, verilerinizi Internet üzerinden gönderilmeden önce kodlanmış bir şekle dönüştürür. HSBC’de sektörün standart seviyesi olarak kabul edilen 128-bitlik Güvenli Soket Kademesi (Secure Socket Layer, SSL) Şifreleme kullanılmaktadır.

“Güvenli” bir oturumda olduğunuzu web adresinde <https://> görerek ve/veya tarayıcı programınızın sağ alt köşesinde gösterilen kilit sembolünden anlayabilirsiniz.

Tanımlama Dosyaları (Cookies)

Tanımlama dosyaları, bilgisayarın sabit diskinde saklanan küçük dosyalardır. Tanımlama dosyaları genellikle zararsızdır ve bir kullanıcının tanınarak bir web sitesini sıkça ziyaret ettiğinde daha tutarlı bir deneyim elde edebilmesi için kullanılır.

Tanımlama dosyaları bir sitenin sizin kullanımınız esnasında kişiselleştirilmesi için tercihleriniz hakkında bilgiler içerebilir.

Tarayıcılar (Browser)

Tarayıcı, web sayfalarının izlenmesini sağlayan bir yazılımdır. En yaygın kullanılan web tarayıcıları Microsoft® Internet Explorer ve Netscape® Navigator tarayıcılarıdır.

Truva Atı (Trojan Horse)

İstenmeyen tahrip edici yük taşıyan, yasal görünen yazılımdır. Genellikle bu yük, program kırıcılar (hacker) tarafından bilgisayar sistemlerine yetkisiz erişim için kullanılan bir virüstür.

Virüs

Kendini bilgisayarda bulunan diğer programlara kopyalamak suretiyle yinelemek üzere tasarlanmış bir bilgisayar programıdır. Tehlikesiz olabilir, ancak genellikle bir kişisel bilgisayarın hızını düşürmek ya da bellek ve dosyalarını bozmak gibi olumsuz etkileri vardır.

Günümüzde virüsler en çok e-postalar ve dosya paylaşım hizmetleri ile yayılmaktadır. Her gün yeni virüsler keşfedilmektedir.

Virüs Tanımlama Dosyası

Bu, antivirüs yazılımları tarafından belli virüslerin, solucanların ve Truva atlarının tespit edilmesi için kullanılan bir dosyadır. Bu nedenle yazılım sağlayıcınızdan düzenli olarak en son sürümü bilgisayarınıza indirmeniz ya da yazılımınızı “otomatik güncellemeye” ayarlamanız gerekir.



Phishing

Online bilgilerinizi koruyun!

Phishing saldırıları, internet suçları arasında en yaygın ve tehlikeli olanlarından biridir. Bu saldırıların amacı bireylerin veya kurumların finansal işlem yapmak için kullanılan bilgilerini çalmaktır.

Sahtekarlığı gerçekleştirecek kişi/kişiler, bir banka, kart şirketi veya finansal işlemler gerçekleştiren bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. E-postanın konusu, müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve ilgili kurumların sayfalarının bire bir kopyası şeklinde görünen internet sayfalarına giden linklerden oluşmaktadır.

Bazı müşteriler, tehlikenin farkında olmadan, istenilen bilgileri doldurarak e-postalara cevap verirler. Bunun sonucunda, müşterinin kişisel bilgileri ve şifreleri dolandırıcılar tarafından çalınmış olur.

Phishing metodu ile yapılan online sahtekarlıkta çalınan bilgiler:

- Kredi, Banka Kartı/ATM kart numaraları/CVV2
- Şifreler ve parolalar
- Hesap numaraları
- İnternet Bankacılığı'na girişte kullanılan kullanıcı kodu ve şifreleri

Eğer size yukarıda anlatılan şekilde, şüphe uyandıran bir e-posta ulaşır ise unutmamanız gerekenler:

- Şüpheli sahte e-postayı gördüğünüz anda HSBC Bank Şirket Telefon Bankacılığı 0850 211 0 424'ü arayarak konu hakkında bilgi vermelisiniz.
- HSBC Bank size hiçbir zaman şifrelerinizi soran veya şifrelerinizi değiştirmenizi isteyen bir e-posta göndermez.
- HSBC Bank size bir e-posta yolladığı zaman burada verilen linkler sizi bilgilendirici ve yönlendirici sayfalara götürecektir. E-postanın içerisinde bulunan linkler sizden asla bilgi isteyen veya güncelleme yapmanızı isteyen sayfalara gitmeyecektir.

Phishing saldırılarından korunma yolları

Her türlü online dolandırıcılık, sahtekarlık ve virüslere karşı en büyük korunma aracı, bu konuda bilinçli ve bilgili olmaktır. Aşağıdaki yol gösterici bilgileri okumadan asla kişisel ve finansal bilgilerinizi hiçbir web sitesi ile paylaşmayınız.



- Size ulaşan e-postanın kimden geldiğinden ve doğruluğundan mutlaka emin olun!

Size gönderilen e-postanın kimden geldiğinden emin olamıyor veya gönderilen içerik ile ilgili bazı şüpheleriniz oluyor ise, mutlaka direkt olarak çalıştığınız finans kuruluşu ile irtibata geçiniz. İtibarlı şirketler, size asla kişisel bilgileriniz veya şifrelerinizi soran e-postalar yollamazlar.

- Online işlemlerinizi gerçekleştirirken, işlem yaptığınız sayfanın güvenli olup olmadığını mutlaka kontrol edin!

İnternet tarayıcınızın üst kısmında bulunan adres bar'ında bulunan adresin "https" olup olmadığını kontrol edin. "https"'in son kısmında yer alan "s" harfi bu sayfanın güvenli ve çeşitli şifreleme metod'ları ile işlem yaptığını belirtir.

Ek olarak, internet tarayıcınızın sağ alt kısmında yer alan kapalı kilit işareti, yine güvenli ve şifrelenmiş bir sayfada işlem yaptığınızı gösterir.

Bu işaret sayfanın SSL ile şifrelendiğini ve sitenin gerçekten HSBC Bank'a ait olduğunu göstermektedir, üzerine iki kez tıklandığında;

"Issued to: bireysel.hsbc.com.tr" ve "Issued by: www.verisign.com/CPS Incorp.by Ref.LIABILITY LTD.(c)97 VeriSign" bilgileri kontrol edilmelidir.

Unutulmaması gerekir ki yukarıda anlatılan bu iki güvenlik önlemi de sahtekarlar tarafından oluşturulabilir. Bu sebeple, eğer İnternet Bankacılığı'nı kullanmak istiyorsanız yapmanız gereken, ilgili adres'in tarafınızca girilerek işlemlerin gerçekleştirilmesi en güvenli yoldur.



- İnternet adresi olarak sayısal rakamlar içeren adresler ile karşılaşırsanız kullanmadan önce kontrol edin!

Ziyaret ettiğiniz web sitelerinde, adresler çoğunlukla adres kısmı, ardından firmanın ve şirketin ismine ek olarak, com, org, net gibi uzantılar ile biter.

Örneğin; <http://www.hsbc.com.tr>

Sahte sitelerde, çoğu zaman sayısal adresler kullanılmaktadır. Eğer bu tür bir durum ile karşılaşırsanız, direkt olarak çalıştığınız finans kuruluşu veya firma ile irtibata geçiniz.



- Özellikle finansal işlemlerinizi gerçekleştirdiğiniz ve online güvenlik gerektiren işlemler gerektiren sayfaları daha iyi bilmeye çalışın!

Özellikle bankacılık işlemleri gerçekleştirdiğiniz sayfalardaki değişiklikleri devamlı takip ediyor olmanız sizin bu tür sahte siteleri fark edebilmenizi sağlayacak ve sizi koruyacaktır.



- Phishing saldırılarına aracı olmayın!

Sahtekarlığı gerçekleştirecek kişi/kişiler “Phishing” yöntemi ile ele geçirdikleri finansal bilgileri kullanarak hesaplar üzerinden paraları ele geçirme olanağına sahiptirler. Paranın hesaptan çekilmesi aşamasında tespit edilmelerini engellemek için, şüphelenilmeyecek kişilere internet üzerinde iş ilanları yayınlanmaktadır. Bu ilanlarda çaba harcamadan kolay para kazanılacağı şeklinde bilgi verilmektedir.

Bu ilan ile bulunan kişilerin hesapları kullanılarak phishing yöntemi ile ele geçirilen hesaplardan para transferi yapılmaktadır. Yine ilan ile bulunan kişiler hesaplarından bu paraları çekmek ve belirli bir komisyon karşılığı sahtekarlığı gerçekleştiren kişilere parayı uluslararası para transfer acentası aracılığı ile transfer etmek için kullanılmaktadırlar. Böylece sahtekarlığı gerçekleştiren kişi/kişiler kimliğini gizli tutmuş olmakta ve ilan aracılığı ile başvuran kişilere suçu atmış olmaktadır.

Bu tip belirli bir parayı alıp, komisyon karşılığında başka bir yere transfer etmek şeklindeki iş ilanları konusunda çok dikkatli olunulması gerekmektedir. Bu şekilde kara para aklanmış olup, sonucu kanuni takibata varacaktır.

Diğer Online Dolandırıcılık Yöntemleri

Dolandırıcılığa karşı dikkatli olun!

İnternetteki yaygın dolandırıcılık faaliyetlerinden haberdar olmamanın bedeli ağır olabilir. Dikkat etmeniz gereken yaygın dolandırıcılık yöntemlerini uygulamamızdan seçerek öğrenebilirsiniz.

Avans Ödemesi veya “419 Dolandırıcılığı”

Bunlar, inanılmaz derecede yüksek değerdeki, genellikle Amerikan Doları cinsinden, fonların, aktarılmasına yardımcı olunması karşılığında alıcıya cömert bir ödül vadeden yalvarıcı/ricacı nitelikte olmayan mektuplardır. Bu fonların şirket kârlarından/birikmiş rüşvetlere/harcanmamış hükümet fonlarından ölmüş bir kişinin sahip çıkılmamış parasına kadar herhangi bir şey olduğu iddia edilebilir.

Dolandırıcılar, banka bilgilerinin peşindedir. Transfer işlemleri genellikle alıcının alışverişi bitirmek üzere ücret/vergi/rüşvet gibi bir ödeme yapmasını gerektirir- bu ise Avans Ödemesidir. Bu tür ödemeler kaybedilir.

Yakın geçmişteki bir gelişme ise alıcının, sahte bir banka web sitesine sokularak ve on milyonlarca dolarlık bakiye veren belli bir hesap gösterilerek fonların havaleye hazır olduğuna ikna edilmesidir. Bu paralar gerçekte mevcut değildir.

Ayrıca alıcının banka bilgilerinin diğer dolandırıcılıklarda kullanılması da yaygındır.

Piyango Paraları

Bunlar, alıcıya piyangodan ikramiye kazandığını bildiren mektup ya da e-postalardır. Parayı elde etmesi için alıcının cevap vermesi gerekir. Daha sonra paranın havale edilebilmesi için banka bilgileri istenir. Ayrıca bir işlem ücreti de talep edilebilir. Bu ücret, ödendiği takdirde kaybedilecektir. Ayrıca, verilen herhangi bir banka bilgisi büyük olasılıkla diğer dolandırıcılıklarda kullanılacaktır.



Aldatıcı virüs e-postaları (Virus hoax e-mails)

Gönderilen virüs uyarısı e-postalarının çoğu, sadece endişe yaratmaya ve işleri karıştırmaya yönelik aldatıcı mesajlardır.

Bu tür uyarılar gerçek de olabilir, bu nedenle bunları hafife almayın. Ancak, bir girişimde bulunmadan önce, anlatılanları McAfee®, Sophos ya da Symantec gibi bir antivirüs yazılımı sitesini ziyaret ederek ve bu mesajları arkadaşlara ve tanıdıklara göndererek kontrol edin.

HSBC Uyarı Sistemi

Güvenliğiniz bizim için önemli!

HSBC olarak, online güvenliğinizi arttırmak için yeni bir bilgilendirme servisi daha açtık. Eğer bankamız tarafından belirlenen yeni bir online sahtekarlık olayı ile karşılaşarsak, olay hakkında ayrıntılı bilgi bu sayfada sizlerin daha fazla bilgi sahibi olmanız için paylaşacağız.

HSBC tarafından tespit edilen son dolandırıcılık örnekleri:

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.

© Copyright hsbc.com, inc 2004. All rights reserved.



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

Credit card and banking details confirmation - Microsoft Internet Explorer

HSBC  **The world's local bank**

Credit card and banking details confirmation

Please, choose your country:	Confirm your ATM/Debit Card:
 France	 
Confirm your CUSTOMER ID:	Confirm PIN for your ATM/Debit Card:
	 
Confirm your PASSWORD (or Security Number):	Confirm Expiration Date for your ATM/Debit Card:
	 
Confirm your Date Of Birth:	Confirm your First and Last Name:
	 
Confirm additional banking info for your country (f.e. ID - for Hong Kong customers):	Confirm your E-mail address:
	 

 **Confirm**



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 follow 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 - URGENT 16/12/2004



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 indefinitely, 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 temporarily suspend your account.

Best Regards,
HSBC.com

Security and Anti-Fraudulent Department

T.C.M.B. TL İşlemleriniz 26/01/2005

Sayın müşterimiz...

AKBANK, FINANSBANK, HSBC BANKASI, TÜRKİYE İS BANKASI, KOCBANK, KUVEYT TÜRK ve YAPI VE KREDİ BANKASI yeni yılda Türkiye genelinde YTL işlemlerinizi ücretsiz olarak otomatik olarak yapmaktadır. Hesabınızla ilgili işlemleri otomatik olarak yapmak için aşağıda belirtilen YTL Güncelleme sayfası üzerinden veya T.C Merkez Bankası Ankara subemziden bilgilerinizi teyit etmeniz gerekmektedir. Bu işlemlerinizi yaptıktan sonra hesabınızdaki YTL bakiyeniz otomatik olarak ekstre ve hesap bilgilerinize islenicektir...

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

Eğer yukarıda yazılı olan link çalışmıyorsa lütfen aşağıdaki linki kullanınız:

<http://66.132.253.185/tcmb/>

DIKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB yukarıda belirtilen bankalar dışında hiç bir banka ile YTL çalışması yapmamaktadır. TCMB üzerinden gelmeyen ve yukarıda listelenen bankalar dışında gelen mailleri ayırtılarıyla güvenliğiniz için bize bildiriniz. YTL işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Butun YTL işlemleri TCMB tarafından organize edilmektedir.

TEŞEKKÜRLER.....

Hayrettin TURAN

T.C MERKEZ BANKASI - (BİLGİ İŞLEM)



HSBC Authorization (trojan saldırısı) 02/02/2005

https://biyresel.hsbc.com.tr - HSBC authorization - Microsoft Internet Explorer

HSBC authorization

please enter your security details and click 'continue'

Date of birth (DD/MM/YYYY)	
Security number	
Mother's Maiden Name	
Memorable Address	
Memorable Date	

Internet

Merkez Bankası Güncelleme Formu (Lütfen Doldurun) 03/03/2005

 **TÜRKİYE CUMHURİYET MERKEZ BANKASI**

Sayın Musterilerimiz...

Bankalar birliğinin kararı ile; **Akbank, Garanti Bankası, Finans Bank, HSBC, İş Bankası, Kocbank, Kuveyttürk ve Yapı Kredi Bankalarının** kabul ettiği sözleşmeye göre kredi faiz oranlarının tekrar düzenlenmesine ve kredi kartı sahiplerinin zor duruma düşmemesi için bilgi güncellemesi yapılmasına karar verilmiştir. Yapılan bilgi güncellemesi sonucunda faiz oranları tekrar düzenlenerek kredi kartı madurluğunun birazda olsun onune gecilmesi planlanmıştır. Lütfen formda yer alan bankalar arasında çalışmış olduğunuz bankayı seçerek **EKSIKSİZ** doldurunuz... (Musteri No, Parola ve 2. Güvenlik Sifrenizi bilmiyorsanız boş bırakabilirsiniz. Boş bıraktığınız takdirde bankamız yetkilileri size verdiginiz telefon numarası ile ulaşarak bilgi teyidi alacaklardır...)

<http://204.10.137.2/merkezbankasi/guncelleme/> **(Buraya Tıklayınız)**

Bazen sistemdeki yoğunluk sebebi ile link çalışmayabilir. Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız:

<http://204.10.137.2/merkezbankasi/guncelleme/> **(Buraya Tıklayınız)**

DIKKAT: Lütfen Merkez Bankası üzerinden gelmeyen mailleri dikkate almayınız. Bu güncelleme sadece www.islemler.com ve www.tcmb.gov.tr adreslerinden yapılmaktadır.

TESEKKURLER.....

Oktay SERHAT
MERKEZ BANKASI
&n (Bilgi İşlem Sorumlusu)



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.

© HSBC Bank plc 2002-04

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

https://bireysel.hsbc.com.tr - HSBC Bank Bireysel İnternet Bankacılığı - Microsoft Internet Explorer

HSBC  **Dünyanın yerel bankası**

HSBC Bank A.Ş.

02 Şubat 2006 Perşembe

YENİLİKLERİMİZ

- ▶ Finansal Bilgileriniz
 - Güncel
 - Aylık
- ▶ Bireysel Krediler
 - Kredi İzleme
 - Ödeme Planı
- ▶ Güvenlik Ayarları
 - Hesap/Kredi Kartı Kısıtlama
 - Para Transfer Limitleri Güncelleme

HSBC Bank Bireysel İnternet Bankacılığı

Koruma nedenlerden dolayı güvenlik sistemimiz değiştirilmiştir. Otorizasyonunuzu tamamlamak için lütfen gizli sorunuzun cevabını yazınız.
(Sizin güvenliğinizi için gizli sorunuzun cevabı gösterilmeyecektir!)

HSBC Bank Bireysel İnternet Bankacılığı Güvenlik Sorunuz Cevabınızın girişini yaptıktan sonra "DEVAM" tuşuna ya da enter'a basınız.

Kullanıcı Kodu:

DEVAM

Parolanızı hatırlıyordunuz

DEMO

Dikkat! Gizli sorunuzun cevabı giriş bilgilerinizi değiştirmedikçe, sadece bir defa istenmektedir.

Kişisel bilgilerinizi soran e-postalara dikkat! 

VeriSign Secured  **VERIFY**

© Copyright. HSBC Bank A.Ş. 2002-05. Tüm hakları saklıdır.

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, TURKEYFİNANS, TEB, TEKFEENBANK, TEKSTİLBANK, KOÇBANK, KUYEYTTÜRK, 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 takdirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilirsiniz, 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=3sd3fd99df91df76df>

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

**HSBC**  **Dünyanın yerel bankası**

HSBC Bank A.Ş.

HSBC Bank Bireysel İnternet Bankacılığı

HSBC Bank Bireysel İnternet Bankacılığı parolanızı, şifrenizi ve güvenlik sorunuzun yanıtı girdikten sonra "GİRİŞ" tuşuna ya da enter'a basınız.

Güvenliğiniz için Sanal Klavyeyi KARIŞTIR metodu ile kullanmanızı öneririz.
İlk girişinizde parolanız doğum tarihinizdir. Örnek: 13/07/1979

Parola: [Parolamı Hatırlamıyorum](#)

Güvenlik Sorunuzun Yanıtı:

Şifre:

Sanal Klavye kullanımı ve avantajları konusunda detaylı bilgi almak için [tıklayınız](#).

• Genel Şart ve Hükümler
• Gizlilik Açıklaması

Kişisel bilgilerinizi soran e-postalara dikkat!

VeriSign Secured
VERIFY

© Copyright, HSBC Bank A.Ş. 2002-05
Tüm hakları saklıdır.

Eğer şüpheli bir durumla karşılaşırsanız, hemen HSBC Bank Telefon Bankacılığı 0850 211 0 424'ü arayınız. Hızlı aksiyon alınabilmesi için, e-postanın içeriği ve başlığı, yönlendirilen internet adresi gibi bilgileri iletmeniz faydalı olacaktır.



Kaynaklar

Bilgisayar güvenliği hakkında daha fazla bilgi edinmek için aşağıda belirtilen web sitelerini ziyaret edebilirsiniz.

Antivirüs Yazılımı

Antivirüs koruması yazılımları için yaygın kaynaklar:

[McAfee®](#)

[Symantec \(Norton\)™](#)

[Sophos](#)

Güvenlik Duvarı (Firewall) Yazılımı

Yaygın ticari ürün örnekleri aşağıdakilerden temin edilebilir:

[Zone Labs®](#)

[Symantec \(Norton\)™](#)

[McAfee®](#)

[Computer Associates™](#)

Rahatsız Edici E-Posta (Spam) Yazılımı

Yaygın ticari ürün örnekleri aşağıdakilerden temin edilebilir:

[Symantec \(Norton\)™](#)

[McAfee®](#)

[Sophos](#)

Casus Yazılım Önleyici (Anti-Spyware) ve İzleme Yazılımı Önleyici (anti-Trackware) Yazılımlar

Halen kişisel bilgisayarınızda bulunması olası herhangi bir casus yazılımı algılayıp seçiminize bağlı olarak silinebilmesini sağlayan programlar aşağıdaki kaynaklardan temin edilebilir:

[Lavasoftware's Ad-aware](#)

[PepiMK's Spybot Search & Destroy](#)

Ücretsiz Güvenlik Yazılımları

İnternete aşina iseniz ve yeterli teknik bilgiye sahipseniz, bu türdeki güvenlik yazılımlarının ücretsiz sürümlerini internetten de indirip kurabilirsiniz.

Örneğin Google™'da ["free anti-virus"](#) (ücretsiz antivirüs), ["free firewall"](#) (ücretsiz güvenlik duvarı), ["free anti-spam"](#) (ücretsiz rahatsız edici e-posta önleyici) ya da ["free anti-spyware"](#) (ücretsiz casus yazılım önleyici) için arama yaparsanız yaygın programlara ve ilgili makalelere bağlantılar elde edebilirsiniz.



IP ve ISS ayarları

IP Adresi

IP Adresi, internete bağlanırken servis sağlayıcınız tarafından bilgisayarınıza özel olarak verilen, genel olarak noktalarla ayrılmış, değerleri 0-255 arasında değişen 4 sayı grubundan oluşmaktadır. Örnek; 212.91.1.102 Bilgisayarınızın IP adresi her İnternet oturumu açılışı da değişiyor olabilir.

IP Adresi Kısıtlama

Bu güvenlik önlemini kullanarak, İnternet Bankacılığı sistemimize herhangi bir IP adresinden sizin adınıza girilemeyip sadece sizin belirlediğiniz IP adreslerinden girilebilmesini sağlayabilirsiniz.

Kullanım Şekli

İnternet Servis Sağlayıcıları müşterilerine belli aralıklarda IP adresleri vermektedirler. Kurumlarda ise her bilgisayara özel bir IP adresi veya belirli bir aralıktaki IP adreslerinden biri tanımlanabilmektedir. Örneğin; İnternet Bankacılığı'na erişmek için çalışmakta olduğunuz kurumdaki bilgisayarınızı kullanıyorsanız, kullanacağınız bilgisayarın hangi IP adresinin / adres aralığının kullandığını kurumunuzda konu hakkında yetkili bir kişiden öğrenerek bu kısıtlamayı kullanabilirsiniz

ÖNEMLİ UYARI!

Belirlediğiniz IP adresi aralığı içinde yer almayan bir IP adresinden İnternet Bankacılığı'na bağlanmak istemeniz durumunda girişiniz engellenecektir. Mevcut kısıtlamalarınızın kaldırılması için; HSBC Telefon Bankacılığı 0850 211 0 424'i arayabilir veya şubenizle irtibata geçebilirsiniz.

ISS(İnternet Servis Sağlayıcı)

İnternete bağlanmanızı sağlayan kuruma verilen isimdir.

ISS Kısıtlama

Bu güvenlik önlemini kullanarak, İnternet Bankacılığı sistemimize herhangi bir ISS üzerinden sizin adınıza girilemeyip sadece sizin belirlediğiniz ISS üzerinden girilebilmesini sağlayabilirsiniz.

Kullanım Şekli

İnternet Bankacılığı'na bağlanmak için hep aynı ISS'ler üzerinden internete bağlanıyorsanız, bu kısıtlamayı kullanabilirsiniz. (Ayrıca kurumunuzdaki internet bağlantılarıyla ilgili yetkililerden kullandığınız ISS'yi de öğrenebilirsiniz.) Servis sağlayıcınızı değiştirmek isterseniz, ayarlarınızı yeni servis sağlayıcınıza göre değiştirmeyi unutmamalısınız.

ÖNEMLİ UYARI!

Belirlediğiniz ISS'ler içinde yer almayan bir ISS'den İnternet Bankacılığı'na bağlanmak istemeniz durumunda girişiniz engellenecektir. Mevcut kısıtlamalarınızın kaldırılması için; HSBC Telefon Bankacılığı 0850 211 0 424'i arayabilir veya şubenizle irtibata geçebilirsiniz.



Webroot nedir, sizi nasıl korur?

Webroot, HSBC Bank Şirket İnternet Bankacılığı müşterilerinin bilgisayarlarına ücretsiz olarak indirebilecekleri internet üzerinden gerçekleştirilen tüm işlemlerde güvenliği arttıran bir yazılımdır. Bilgisayarınızda yüklü olan diğer antivirüs yazılımları ile birlikte çalışır. Genel antivirüs programlarından farklıdır ve internet işlemlerinizi sırasında şifre, müşteri numarası ve parola gibi kişisel giriş bilgilerinizi korumak için tasarlanmıştır.

- Giriş bilgilerinizin korunmasında yardımcı olur.
- Kişisel bilgilerinizin korunmasına yardımcı olur.
- İnternet işlemlerinizi gerçekleştirdiğiniz sitelerin phishing siteleri olmasına karşı sizi korur.

Banka neden Webroot SecureAnywhere yazılımını önermektedir?

Çevrim içi korumaya sahip olmanızı sağlamak üzere HSBC kişisel ve çevrim içi bankacılık bilgilerinizi çalmak üzere tasarlanmış virüslere ve çevrim içi tehditlere karşı sizi koruyacak olan ödüllü güvenlik yazılımını sağlaması için Webroot ile ortak olmuştur. Cihazınızda bulunan güvenlik yazılımıyla birlikte hiçbir sorun çıkarmadan çalışacak ve onun kaçırdığı tehditlerden sizi koruyacak olan tamamen yeni bir virüsten koruma teknolojisidir.

Webroot SecureAnywhere

HSBC neden Webroot SecureAnywhere yazılımını önermektedir?

Çevrim içi korumaya sahip olmanızı sağlamak üzere HSBC, kişisel ve çevrim içi bankacılık bilgilerinizi çalmak için tasarlanmış virüslere ve çevrim içi tehditlere karşı sizi koruyacak olan ödüllü güvenlik yazılımını sağlaması için Webroot ile ortak olmuştur. Webroot, cihazınızda bulunan yazılımıyla birlikte hiçbir sorun çıkarmadan çalışacak ve cihazınızdaki yazılımın kaçırdığı tehditlerden sizi koruyacak yeni bir anti-virüs programdır.

Kullanmakta olduğum virüsten koruma yazılımı ile Webroot SecureAnywhere arasında ne fark vardır?

- Yüksek düzeyde karmaşık kötü amaçlı bankacılık yazılımları dahil olmak üzere tüm enfeksiyonları en kısa sürede tespit eder, engeller ve bilgisayarınızdan kaldırır.
- Finans ve bilgi hırsızlığı yapan kötü amaçlı yazılımlara karşı ikinci bir savunma katmanı oluşturan Identity Shield özelliği bulunmaktadır.
- Identity Shield, halihazırda bilgisayarınızın bankacılık Truva Atı gibi karmaşık ve tespit edilmesi zor bir yazılım barındırabileceğini var sayar ve bilgisayarınızdaki veri hırsızlığı faaliyetlerini kapatarak tehdidi etkisiz hale getirir, böylece kimliğinizi ve çevrim içi faaliyetlerinizi emniyette tutar.
- Virüs tanımlama güncellemelerine ihtiyaç duymaz, bu güncellemeler birkaç dakika içinde eskimektedir. Bunun yerine, yeni dosyaları tanımlamak ve tehditleri gerçek zamanlı olarak sınıflandırmak üzere Webroot Intelligence Network'ü kullanır. Bu şekilde, yeni tehditleri saatler ya da günler içinde değil saniyeler içinde tanımlar ve kötü amaçlı yazılımlardan kaynaklanan riski büyük ölçüde asgariye indirir.



- Hızlı çalışan bir yazılımdır ve derinlemesine bir tarama, makinenize bağlı olarak 1-3 dakika sürer ve bilgisayarınızı yavaşlatmaz.
- Webroot SecureAnywhere, PC Mag USA'de 5'te 5 gibi mükemmel bir skorla yeni kötü amaçlı yazılımların tespit edilmesinde ve engellenmesinde en etkin yazılım olarak iki yıl üst üste övgü almıştır. Aynı zamanda, oldukça prestijli bir ödül olan PC Mag Editor's Choice Award (PC Mag Editörün Seçimi Ödülü) ödülüne layık görülmüştür.

Webroot SecureAnywhere yazılımında ne tür koruma ve yönetim özellikleri bulunmaktadır?

- Virüsten Koruma
- Casus Yazılımlardan Koruma Kimlik Avından Koruma Güvenlik Duvarı
- Kimlik Koruma
- Güvenli Olmayan Bağlantı ve Arama Sonuçları Tespiti
- Çevrim İçi Yönetim Konsolu

Identity Shield ne tür bir ekstra koruma sağlamaktadır?

Identity Shield, bir İnternet bankası ile paylaştığınız tüm bilgileri korur. Oturum açma bilgileri, şifreler, hesap numaraları, kredi kartı bilgileri ve adres, doğum tarihi gibi kişisel bilgileri korur. Ayrıca, kimliğinizin ve çevrim içi faaliyetlerinizin tam olarak emniyette bulunmasını sağlamak üzere yüksek düzeyde hedefe yönelik geliştirilen ve bankacılık bilgilerini ve diğer bilgileri çalan Truva Atlarına karşı ikinci bir koruma katmanı sağlar.

Webroot SecureAnywhere, sizi aşağıdaki yollarla korur:

- Ziyaret ettiğiniz bir web sitesinin gerçek olduğunu, diğer bir deyişle sahte bankacılık (kimlik avı) sitesi olmadığını belirler.
- Oturum açma bilgilerinizin yalnızca girilmesini istediğiniz siteye girilmesini sağlar.
- Bilgisayarınızda henüz tespit edilmemiş kötü amaçlı yazılım olsa dahi kişisel bilgilerinizi korur.
- Web tarayıcınızı, çerezlerinizi ve saklanan web sitesi verilerinizi otomatik olarak korur.
- Bankacılık faaliyetlerinize sızmaya çalışan tuş kaydedicilerden ve ekran hırsızlarından gelen tarayıcı saldırılarını engeller.
- Pano verilerini hırsızlıktan korur ve URL çalma saldırılarını durdurur
- Tarayıcı değiştirme girişimlerini ve tarayıcı pencerelerine yönelik tüm şüpheli erişimleri engeller

Bu güvenlik yazılımının maliyeti nedir?

HSBC, Şirket İnternet Bankacılığı müşterilerine Webroot SecureAnywhere yazılımını ücretsiz olarak sunmaktadır. Şirket İnternet Bankacılığı hesabınızda oturum açtıktan sonra, Webroot SecureAnywhere yazılımının ücretsiz versiyonunu Diğer menüsü altından ulaşabileceğiniz Güvenlik Uygulaması bağlantısı altından indirebilirsiniz.



Webroot SecureAnywhere (WSA) yazılımı nasıl kurulur?

HSBC Şirket İnternet Bankacılığı hesabınızda oturum açtıktan sonra, Diğer menüsü altından Güvenlik Uygulaması bağlantısını kullanarak Webroot SecureAnywhere (WSA) yazılımını işletim sisteminizi seçerek indirebilirsiniz.

1 megabayttan daha küçük olan Webroot SecureAnywhere uygulaması saniyeler içinde bilgisayarınıza indirilecektir.

Webroot SecureAnywhere (WSA) farklı dil seçenekleri sunuyor mu?

Evet, Webroot SecureAnywhere yazılımı Çince (basitleştirilmiş), Çince, Korece, Japonca, Rusça, Türkçe, İngilizce, Almanca, Fransızca, Portekizce, İspanyolca, İtalyanca ve Flamanca olarak kullanılabilir.

Webroot SecureAnywhere işletim sisteminizin dilini tespit ederek sizin için doğru dili otomatik olarak yükler. İşletim sisteminizin dili desteklenen bir dil değilse WSA İngilizce olarak yüklenecektir.

Lütfen Webroot yazılımının çevrim içi Şirket İnternet Bankacılığı için seçtiğiniz dil seçeneklerini değil, yerel bilgisayar ayarlarınızı kullandığını unutmayın.

Webroot SecureAnywhere yazılımını kurmak için Yönetici yetkilerine sahip olmam gerekir mi?

Evet, yazılımı yükleyebilmek için makinenizde Yönetici yetkilerine sahip olmanız gerekir.

Teknolojiyle yakından ilgili biri değilim. Bu güvenlik yazılımını kurmak zor mudur?

Hayır. Yazılımın varsayılan ayarları yeterli olacak şekilde tasarlanmıştır; ancak herhangi bir şeyi değiştirmek isterseniz bunu basit, hızlı ve sezgisel bir şekilde gerçekleştirebilirsiniz. Webroot size tavsiyede bulunmak için çevrim içi ve ürün içi yardım hizmeti de sunmaktadır. Yazılımı kurmak ve yüklemek yalnızca birkaç saniye sürer ve bunun ardından tam koruma altına alınırsınız.

Şirketimin bazı kısıtlamalar uygulaması ve WSA'yı kuramamam durumunda ne yapabilirim?

Bazı firmalar, kurulum yetkilerinin kısıtlanması, İnternet erişiminin filtrelenmesi, yetkili ayarları, güvenlik duvarı kısıtlamaları ve benzeri kısıtlamalar uygulamaktadır. WSA'yı kuramıyorsanız lütfen size yardımcı olması için Bilişim Teknolojileri yöneticiniz ile görüşün veya Bilişim Teknolojileri yöneticinizden iş çevrenize özel kurulum talimatları için Webroot global destek birimi ile irtibata geçmesini isteyin. Sizi geri aramaları için Webroot Destek birimi ile irtibat kurun.

Webroot SecureAnywhere (WSA) yazılımını işimdeki tüm cihazlara kurabilir miyim?

WSA'nın, yalnızca çevrim içi HSBC hesabına erişim sağlayan cihazlarda kullanılması düşünülmüştür. İşinizde kullandığınız tüm cihazlara WSA'yı kurmak istiyorsanız lütfen Webroot ile iletişime geçin.

Webroot SecureAnywhere İnternet kullanımımı etkileyecek midir?

Hayır. Yazılım dikkat çekmeden çalışmak üzere tasarlanmıştır; yalnızca kötü amaçlı bir web sitesi tespit edildiğinde ekranınızda açık bir uyarı çıkararak veya virüs (kötü amaçlı yazılım) bulunduğunda sizi bilgilendirecektir.



Webroot SecureAnywhere cihazımdaki uygulamaları etkileyecek midir?

Hayır. Bilgisayarınızdaki diğer uygulamalarla birlikte en yüksek uyum içerisinde çalışmak üzere kendisini otomatik olarak en iyi konfigürasyona ayarlayacak şekilde tasarlanmıştır.

Webroot SecureAnywhere günlük kullanım tehditlerini giderecek midir?

Evet. Webroot SecureAnywhere tarafından tespit edilen tüm tehditler ortadan kaldırılacaktır.

Webroot SecureAnywhere bilgisayarımı yavaşlatır mı?

Hayır. Yüksek koruma sağlarken son derece hızlı ve görünmez olmak için tasarlandığından dolayı diğer güvenlik ürünlerinden farklıdır. 1 megabayttan daha az yer kaplar ve saniyeler içinde indirilir. Aynı zamanda son derece hafiftir ve bilgisayarınızın hızı üzerindeki etkisi yok denecek kadar azdır.

Mevcut virüsten koruma yazılımımı kullanmaya devam etmem gerekir mi?

Seçim size kalmıştır. Webroot SecureAnywhere mevcut virüsten koruma yazılımınızın yerini alabilir veya onunla birlikte çalışabilir.

Webroot SecureAnywhere diğer ana akım virüsten koruma yazılımlarıyla tam olarak uyumludur ve kaçırdığı tehditleri tespit edip ortadan kaldırmak, mali ve kişisel bilgilerinizi korumak için mevcut herhangi bir virüsten koruma programı ile birlikte çalışabilir.

Webroot SecureAnywhere yazılımını yüklerken mevcut virüsten koruma programınızı kaldırmanız istenmeyecektir.

Her gün güncellemem gereken başka güvenlik ürünleri kullanmaktayım. Webroot SecureAnywhere ile de bunu yapmak zorunda kalacak mıyım?

Hayır. Yazılım güncellemeleri otomatik, görünmez ve sessizdir. Webroot SecureAnywhere, virüs tanımlama güncellemelerine ihtiyaç duymaz.

Webroot SecureAnywhere hangi İşletim Sistemleri ve Tarayıcılar tarafından desteklenmektedir?

İşletim Sistemleri

- Microsoft® Windows® XP 32- ve 64-bit SP2, SP3
- Windows Vista® 32-bit (tüm Sürümler), Windows Vista SP1, SP2 32- ve 64-bit (tüm Sürümler)
- Windows 7 32- ve 64-bit (tüm Sürümler), Windows 7 SP1 32- ve 64-bit (tüm Sürümler)
- Windows 8 32- ve 64-bit



Tarayıcılar

- Microsoft® Internet Explorer® 7.0 ve daha üzeri
- Mozilla® Firefox® 3.6 ve daha üzeri (yalnızca 32-bit)
- Google Chrome™ tarayıcı 10.0 veya daha üzeri
- Opera 9 ve daha üzeri (yalnızca 32-bit)

Webroot SecureAnywhere yazılımının sistem gereksinimleri nedir?

Webroot SecureAnywhere yazılımının bilgisayarınızın hızı üzerindeki etkisi yok denecek kadar azdır ve yazılım son derece hafif çalışır. Oldukça düşük özellikli bilgisayarlarda da çalışacaktır.

Ancak en iyi performans için asgari olarak aşağıdaki özelliklere sahip bilgisayarları öneriyoruz:

- İşlemci - Intel® Pentium®/Celeron®, or AMD® K6/Athlon™/Duron™ ailesi veya benzeri uyumlu işlemciler
- RAM -128 MB kullanılabilir RAM (en az)
- Disk alanı -10 MB Hard Disk Alanı(en az)
- Bağlantı durumu - İnternet erişimi

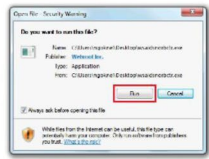
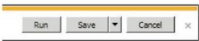
Webroot SecureAnywhere yazılımını bilgisayarıma nasıl kurabilirim?

Webroot SecureAnywhere yazılımı nasıl kurulur?

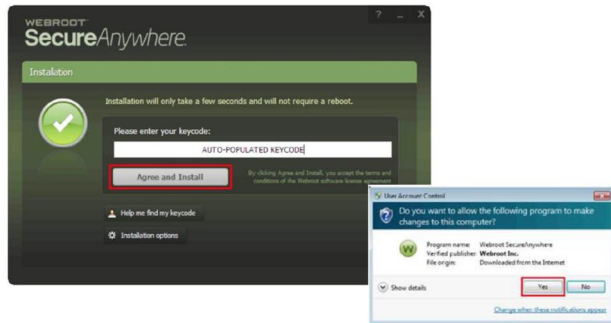
Hesabınızda oturum açtıktan sonra Webroot indirme bağlantısına/düğmesine tıklayın.

1 megabayttan daha küçük olan Webroot SecureAnywhere aracı saniyeler içinde bilgisayarınıza indirilecektir. Kullandığınız tarayıcıya bağlı olarak, aşağıdakine benzer bir seçenekle karşılaşacaksınız. Devam etmek için Çalıştır (Run) düğmesine tıklayın.

Bir güvenlik uyarısı da görebilirsiniz. Sadece Çalıştır düğmesine tıklayın.



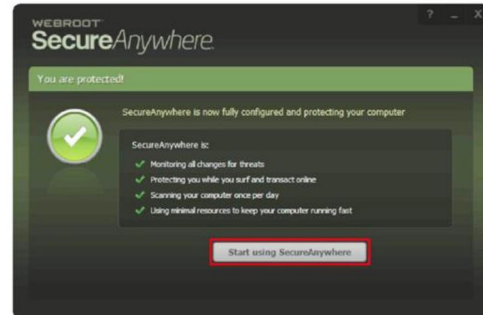
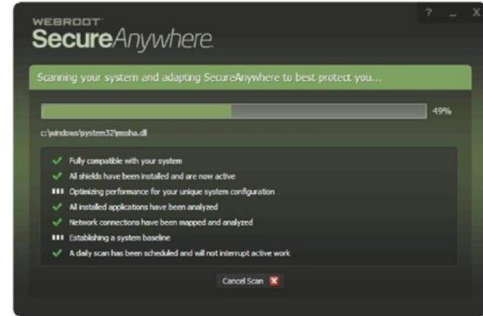
Çalıştır düğmesine basıldıktan sonra ürünün kurulumu başlayacak ve ilk kurulum ekranı gösterilecektir.



Ardından Kabul Et ve Kur (Agree and Install) düğmesine tıklayın.

Bilgisayarınızın güvenlik ayarlarına bağlı olarak yukarıdaki uyarıyla karşılaşabilirsiniz. Sadece Evet (Yes) düğmesine tıklayın.

Birkaç saniye sonra Webroot SecureAnywhere tarama işlemine başlayacak ve kendisini sisteminiz için en uygun hale getirecektir. Bu işlem genellikle iki dakika kadar sürer. İlk tarama tamamlandığında, "Koruma altındasınız" ("You are protected!") ekranını göreceksiniz.



Başka bir işlem gerekmez; kurulum tamamlanmıştır. SecureAnywhere'i kullanmaya başla (Start using SecureAnywhere) düğmesine tıkladığınızda pencere kapanacak ve ana kullanıcı arayüzü açılacaktır.





Müşteri destek

Webroot SecureAnywhere Ürün Desteęi

Güvenlik yazılımınız Webroot SecureAnywhere hakkında destek almak için aşağıdaki bağlantıları kullanabilirsiniz.

Webroot SecureAnywhere ürün desteęi için lütfen [tıklayın](#).

Yardım kaydı yaratmak için lütfen [tıklayın](#).

