O que é HTTP

HTTP é sigla de **HyperText Transfer Protocol** que em português significa **"Protocolo de Transferência de Hipertexto"**. É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na **World Wide Web (www - Internet)**.

O **HTTP** é o protocolo utilizado para transferência de páginas **HTML** do computador para a Internet. Por isso, os endereços dos websites (URL) utilizam no início a expressão "http://", definindo o protocolo usado. Esta informação é necessária para estabelecer a comunicação entre a URL e o servidor Web que armazena os dados, enviando então a página **HTML** solicitada pelo usuário.

Para que a transferência de dados na Internet seja realizada, o protocolo **HTTP** necessita estar agregado a outros dois protocolos de rede: **TCP (Transmission Control Protocol)** e **IP (Internet Protocol)**. Esses dois últimos protocolos formam o modelo **TCP/IP**, necessário para a conexão entre computadores clientes-servidores.

Na prática funciona assim: quando você digita um endereço no navegador, ele precisa enviar alguma coisa para algum lugar dizendo que você quer ler alguma coisa. Imagine que você digitou o endereço do Google. Seu navegador prepara uma carta, isso mesmo, literalmente uma carta para o servidor onde fica o site do Google. O conteúdo dessa carta é mais ou menos isso:

```
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-BR; rv:1.9.0.6)
Gecko/2009011913 Firefox/3.0.6 (.NET CLR
3.5.30729)
Accept: text/html,application/xhtmlxml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-br,pt;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

Não se apegue aos códigos, como já disse isso são apenas padrões. Esses padrões em especifico são conhecidos como HTTP. Se você não entende é porque não tem muito contato com esse tipo de linguagem, e se não é um desenvolvedor WEB não há problema algum. O importante nessa carta é o seguinte:

Bom dia Google.com,
Gostaria de ler sua página.
Estou usando o navegador Firefox na versão 3.0.6.
No momento eu aceito HTML.
Gostaria de receber o conteúdo em português, mas também entendo inglês.
Uso o padrão de caracteres (letras) ISO-8859 e UTF-8.

Seu navegador vai envelopar essa carta e enviar ao servidor do Google, que você solicitou (sobre TCP e outros protocolos que seriam esse envelope). Essa carta é tecnicamente conhecida como **Request HTTP**.

Esse servidor vai ler sua carta, porque ele lê TODAS as cartas que chegam, diferente do Papai Noel. Com base nas solicitações feitas na carta, o Google vai criar a resposta:

Location: http://www.google.com.br/
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Mon, 08 Feb 2009 22:00:00 GMT
Server: gws
Content-Length: 222
...

O Google está dizendo o seguinte:

Olá,

Aqui é o Google.com.
Estou enviando a página que pediu.
Você pode guardar as informações em seu computador e usa-las em outras visitas.
Estou enviando apenas texto e HTML como você pediu.
Essa carta foi feita as 22:00 horas do dia 08/02/2009 utilizando servidor GWS.
O conteúdo é formado por 222 letras, segue:
...

Coloquei três pontinhos substituindo o conteúdo da página. Esse conteúdo é um pouco mais extenso, mas não é nada de outro mundo. Nada mais é do que a forma codificada do que você vê no navegador. Essa carta de resposta também é conhecida como Response HTTP.

Claro que eu abordei de forma simplista, há muito mais o que se falar sobre esse protocolo e isso vou fazer em outros artigos. O próximo será um pouco mais técnico e sua avó realmente não vai entender. Falarei sobre Cookie e Sessão. Para saber mais detalhes e dar uma treinadinha no inglês técnico nada melhor do que a especificação oficial do HTTP, aqui.

Qual a diferença entre HTTP e HTTPs?

Sempre que você acessa um site na Internet, eles iniciam por **"HTTP"** ou **"HTTPS"**. É apenas um "S" a mais, mas faz toda a diferença e é importante conhecer as especificações para saber se a navegação, em determinada página da web, é segura ou não.

HTTP (Hyper Text Transfer Protocol) é um protocolo, ou seja, uma determinada regra que permite ao seu computador trocar informações com um servidor que abriga um site. Isso significa que, uma vez conectados sob esse protocolo, as máquinas podem receber e enviar qualquer conteúdo textual – os códigos que resultam na página acessada pelo navegador.

O problema com o HTTP é que, em redes Wi-Fi ou outras conexões propícias a phishing (fraude eletrônica) e hackers, pessoas mal intencionadas podem atravessar o caminho e interceptar os dados transmitidos com relativa facilidade. Portanto, uma conexão em HTTP é insegura.

Nesse ponto entra o HTTPS (Hyper Text Transfer Protocol Secure), que insere uma camada de proteção na transmissão de dados entre seu computador e o servidor. Em sites com endereço HTTPS, a comunicação é criptografada, aumentando significativamente a segurança dos dados. É como se cliente e servidor conversassem uma língua que só as duas entendessem, dificultando a interceptação das informações.

Para saber se está navegando em um site com criptografia, basta verificar a barra de endereços, na qual será possível identificar as letras HTTPS e, geralmente, um símbolo de cadeado que denota segurança. Além disso, o usuário deverá ver uma bandeira com o nome do site, já que a conexão segura também identifica páginas na Internet por meio de seu certificado.

Como se proteger com HTTPS

Infelizmente, não há HTTPS em todo lugar. O usuário, na verdade, depende que os sites ofereçam suporte a esse tipo de conexão para poder aproveitar da codificação. Porém, em muitos casos, a conexão segura está presente mas deve ser habilitada manualmente, caso você deseje mais privacidade.

É o caso do Facebook, que incluiu a conexão via HTTPS em 2011. Por padrão, os usuários da rede social acessam o site via HTTP, mas isso pode ser mudado facilmente por meio das configurações do seu perfil. Outras redes sociais como Twitter, Pinterest e Google+ também contam com acesso via HTTPS. O Google, aliás, inclui HTTPS até em suas pesquisas no buscador.

O que é importante ter em mente é que qualquer serviço online no qual seja necessário digitar uma senha para logar ou, principalmente, enviar dados de cartão de crédito, precisa de conexão via HTTPS. Por essa razão, os sites de banco utilizam esse protocolo para garantir a privacidade dos dados fornecidos pelos clientes.

Sempre procure utilizar o HTTPS nos sites que oferecerem o recurso, e tome cuidado ao enviar suas informações para páginas sem segurança, já que há chances significativas de que hackers acessem as informações e senhas, utilizando os dados os mais diversos fins.

Uma maneira fácil de ativar o HTTPS é com extensões, como o HTTPS Everywhere para Mozilla Firefox, Google Chrome e Opera. O aplicativo coloca em ação, automaticamente, a conexão criptografada nos sites em que isso é possível. Com isso, o usuário evita de ficar procurando e ativando a opção segura em todas as páginas que visitar.

Precauções

É bom lembrar que o HTTPS não é perfeito. Mesmo que tenha uma conexão desse tipo ativa, fique atento para tentativas de fraude. Há casos de phishing que levam o usuário para sites com HTTPS mas, na verdade, é uma página errada – eles criam uma conexão segura entre você e um servidor falso. Em outras situações, alguns sites imitam o símbolo de cadeado para atrair desavisados, ou mesmo mudam o ícone do site para que você acredite que está seguro.

No final, todas as dicas sobre navegação segura continuam valendo. Mas, desde que saiba que o site acessado é verdadeiro, procure sempre optar por uma conexão segura. Embora não seja infalível, HTTPS é, com certeza, mais seguro do que um protocolo convencional.