# How to check for unsecured connections

Whether sending these passwords, or any other important information, such as bank account numbers or important data, they need to be protected through a secure connection.

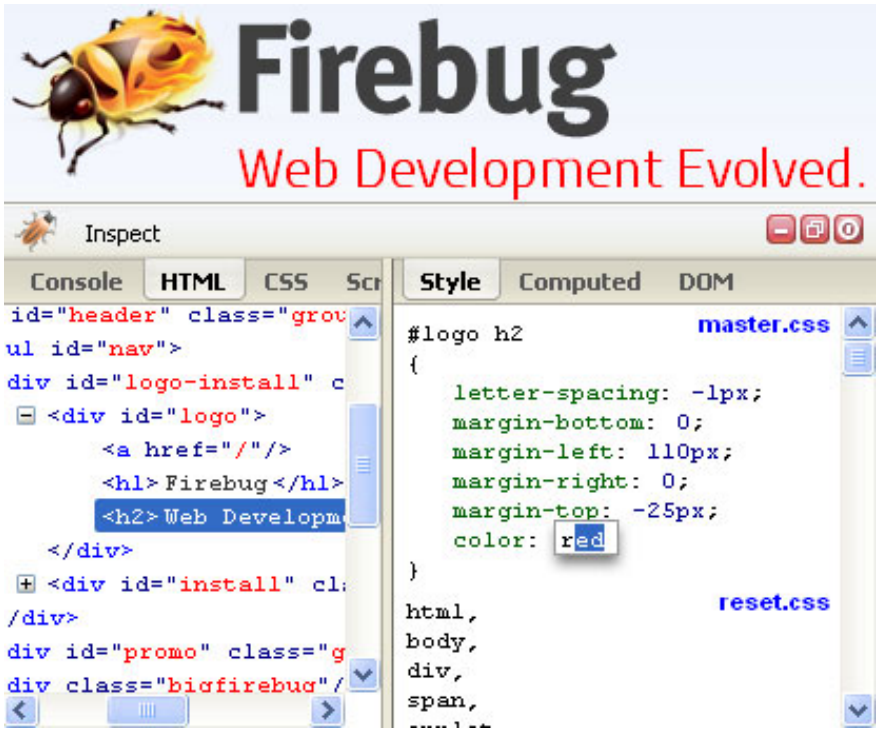
*TipsMake.com* - **As an IT expert or even just a computer enthusiast, passwords are nothing new to you.** Whether sending these passwords, or any other important information, such as bank account numbers or important data, they need to be protected through a secure connection. That is the basic security, and it is something that anyone who is interested in how the Internet works can soon find out.

When visiting an important website, look at the **https: //** keyword in the URL. When you need to share folders with colleagues, first need to open the VPN first to make sure no one can detect the data stream on the network and steal them. Users may even find panic and check the security parameters after recent fraudulent e-certificates.

However, that's just what we do online. We have a lot of other connections and usually the computer will help create these connections, sending information to the remote server with the corresponding protocol. Are these connections safe? How to know when they leak out in clear text? Let's explore some of the basics of secure and non-secure connections.

## Email

The first and most likely case is email. There are many different protocols for emailing, some security, some not. First, for Gmail and other webmail sites, this is really recognizable. Even a page does not display the form of SSL connection, you can use tools like Firebug on Firefox to check.




However, if you use a desktop email application like Outlook, this is not easy at all. An enterprise email system that uses the Microsoft Exchange server is usually encrypted, ensuring that it has been correctly configured. In Exchange's POP3 installation, simply go to the **Authentication** tab and select **Secure Logon** as the login method. Similarly, if you use Microsoft Hotmail to send email directly to Outlook or Live Mail, this connection is also encrypted.

However, if your email comes from an ISP with Internet service via POP3 or IMAP, it may not be encrypted. By default, these protocols send both email and account information in plain text format, including passwords. ISPs can completely add encryption to make the protocol more secure, but most of them do not.

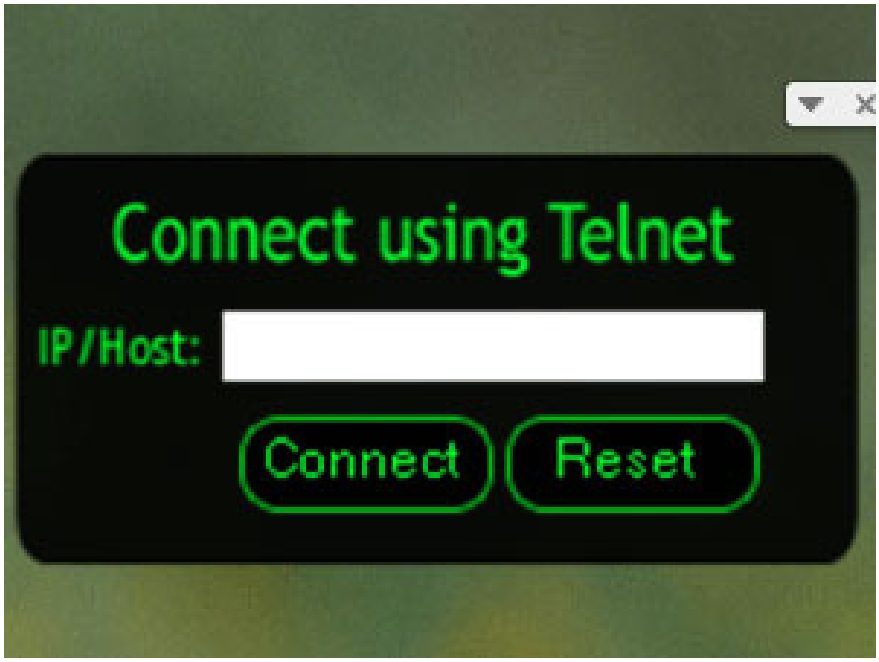
# File Transfer Protocol

When transferring files, there are many ways to do this, such as using shared folders or simply transferring them using a web service like Dropbox. One of the simplest and oldest ways is to transfer files using FTP. By default, FTP does not use encryption. However, it can be safely created if the user configures correctly and the customer supports it. Suppose you are running a Microsoft FTP server, just configure **FTP SSL Settings** in the **Connections** panel in **IIS Manager** .


A typical case of FTP is to transfer files to a web server. We have seen a few cases where people use a web host with a web table, where they can be sure that the web connection to the configuration table is secure. However, after going straight to the FTP application to send the file to the host, it sends both the username and password in plain text format.

## Telnet

Telnet is no longer used much, but it is still preferred by some people. There are many hosts that provide the ability to connect to the server and allow users to have access to a command. Telnet, software and protocols used to connect, are not encrypted. Meanwhile, SSH is worth the user to keep an eye on and is often supported by these hosts.



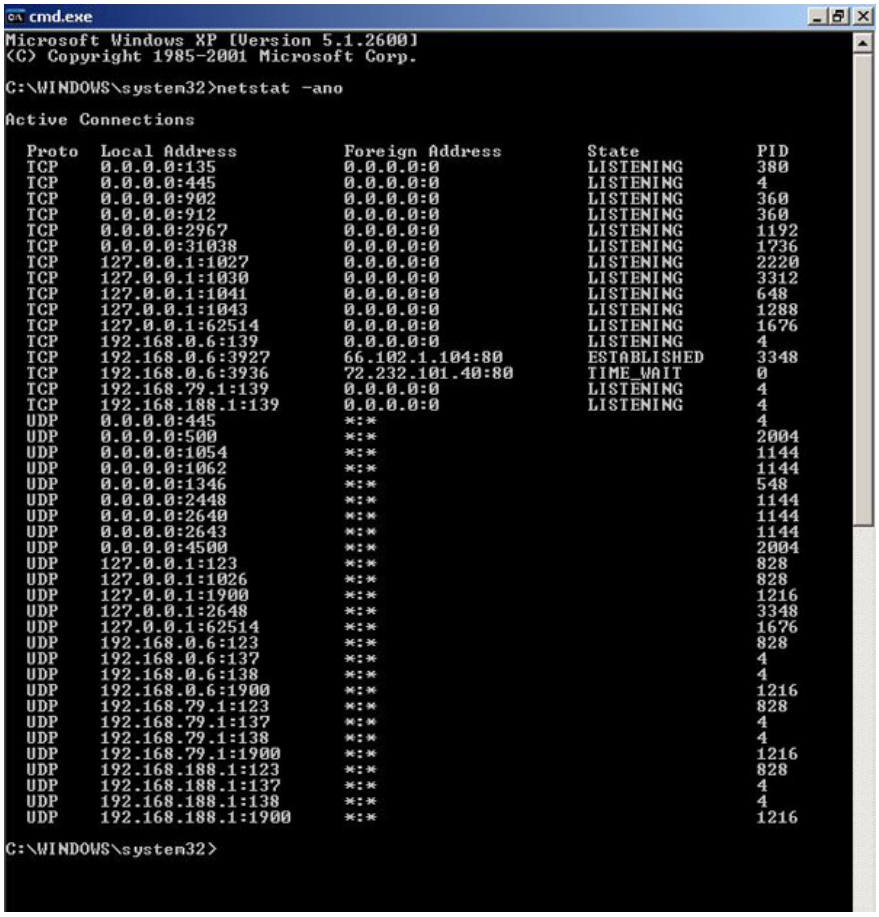

Note that Telnet is not used with hosts. If you are an expert and have to configure the router, you probably have to use Telnet. If not, only unless you configure SSH manually. On some routers, this can be a bit confusing when asking users to create a certificate - certificate - and assign it before it allows you to enable SSH. So, users may prefer to use a console connection directly to the device by using a cable instead of sending all data over the

network.

## Other software

The opportunity for users to have a lot of software is able to continuously connect to the remote server, some of which is transferring account information. Whether it's Adobe AIR on Twitter, widget Gmail Notifier, Dropbox application, IM chat application like Windows Live or AIM, . the list is not all that. So, how do I know if each of them sends your data in encrypted form?

Instead of looking at each software manufacturer's website and reading the FAQ carefully, try to find out if they create security software. Users can quickly view a list of ongoing connections from the computer using the *netstat* command. Users can type it in the command window and on the third line you will see a list of remote hosts with the ports used. Whenever a remote host uses port 443 or HTTPS, this means it is secure.




Our favorite solution is to use a packet sniffer. What better way to know if your confidential information is leaking from your computer? The way we use it is Microsoft Network Monitor, which is available for free on the Microsoft site. However, you can also use Wireshark.