Issue 6

April 2005

M&H CONSULTING

THE M&H MONITOR

Avoiding Identity Theft

As anyone who watches the news knows, identity theft has become an increasing problem. Adding to this problem is the increasing use of email, and the advancement of the techniques used to get your information.

There are many easy steps one can take to help prevent this from happening. One of the best is to never respond to an email requesting account information. If there is any need for a company to get information from you, they will never request it via email. Also, if you click on a link in an email that brings you to a login page, never log in. A popular way to get your account username and password is to create a dummy site that looks like an official site login page.

Another excellent piece of advice is if you use the internet for financial purposes, such as purchases or paying credit card bills, never use the same password. As complex as it may seem, if your password is discovered then whoever has it could possibly access all of your financial websites. Each site should have its own password, and the password should be secure. Secure passwords are ones that have nothing to do with names, dates, or personal likes. Also, it should consist of letters and numbers, and not be the name of a family member. Personal information is surprisingly easy to obtain.

Along with these precautions you should always use anti-virus software, keep it up to date, and run regular scans. There are thousands of viruses out there that are designed to get personal information – some even go so far as to log every key stroke made. This means that if you are on your credit card website and are infected with a key-logging virus, it can record down what website you are on and get your username and password. It could then send this information to anyone on the internet.

Follow these steps and your chances of getting scammed are significantly reduced. If you ever do believe you are a victim of identity theft, you should call 1-877-IDTHEFT (438-4338).

TAKE $$$CASH$$$ FROM M&H CONSULTING

Refer a new client to M&H Consulting and mention this offer to us,

and you will receive $25 for each PC the new client has. Call for details.

Firewall Protection

Firewalls, while not the only part of good network security, are certainly an integral part. A firewall is sometimes incorporated into your router, and these routers do give some form of network security, but it is generally limited and not nearly as robust as it could be. Problems arise when we need to allow some access to the outside world (i.e. for email to come through, remote access to the network, etc.). We need this access to be secure and also configured in such a way that other, unneeded access, is not allowed. To do this we create an opening on your firewall or router, and this is where the kind of firewall/router you have comes into effect.

If you have a standard router like a Linksys, Dlink or Belkin then it will accept any traffic that comes into that port and forward it to your server or PC. Someone trying to break into your network can use this opening to try to gain access. If someone were to scan your router it would tell them exactly what openings your router has.

If you want more security, which is not always a necessity, you can purchase a router that has a higher end firewall built-in. Some of the best ones that we recommend are Sonic Wall and Cisco routers. While these are more expensive, they do provide a great deal more security. If someone on the internet scans your router it will not tell them what openings it has. It will block many of the known attacks that people use on the internet. It also monitors the traffic that goes through the openings you have created. If the traffic going through one of the openings is recognized as potentially being a hacker, the firewall can block it. This means that if you create an opening specifically for viewing your website and someone tries to use it to attack your network, then they are blocked. The differences between most Sonic Walls and Cisco routers is that a Cisco router is usually more complicated to setup because they provide more options while a Sonic Wall requires only a bit more work to setup than a normal router. Also there are many small differences between the two that depend on which model of each you buy and of course the more features the router comes with the more expensive it is. Cisco routers are great tools for managing complex networks and are the industry standard for large companies while Sonic Walls are used in normal small business offices that just want more security.

Whatever type of firewall security you feel is best for your company, it is certainly a topic that should be looked at. If you have any questions about your current firewall security setup, contact the M&H technical support line at 866-9MH-Tech x2.

"The game has changed."