

Home Network Security

By Bruce W. Roeckel

<http://www.immaculatetechnology.com>

Securing your home network is a critical step in protecting important assets that are stored on your computers. These assets may include financial data, such as tax returns (e.g. TurboTax files) or checking account books (e.g. Quicken files, Microsoft Money files), legal records (e.g. Trust Documents, Wills), personal information (e.g. Resumes, Credit Card Numbers), and contact information (e.g. Address Books). Hackers can extract information from these assets to steal your identity, access your bank accounts and otherwise create major problems for you and your loved ones.

The first step in securing your home network is to understand what products and methods are at your disposal and, more importantly, what products you should steer clear of due to high risks and/or flawed design. So lets start out with the basics ...

Password Parley

Following good password standards is critical in protecting your assets. Don't make the mistake of using passwords that are easily guessed – hackers regularly use password cracking programs that can very quickly decipher simple passwords. So ...

Don't ...

- Don't use a password that can be found in the dictionary
- Don't use a password such as your child's name or pet's name
- Don't use the word "password" as your password

Do ...

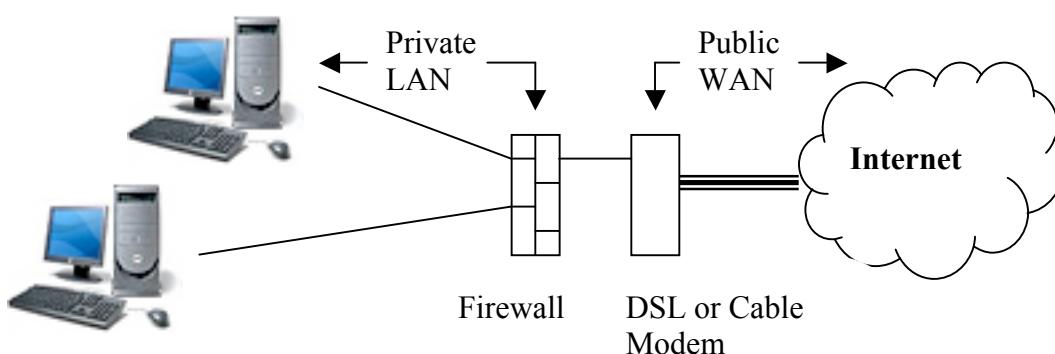
- Do create passwords that are at least 8 characters in length
- Do create passwords that are a combination of letters and numbers
- Do create passwords that use both upper and lower-case letters

The most straightforward approach to creating a password is to look around your home for an appliance model number, such as your TV, Oven, Printer, or other device. They typically contain both letters and numbers, and can easily be recovered if you happen to forget the exact combination of letters and numbers since you will more than likely remember which appliance you used to create the password in the first place.

Network Nomenclature

Every network should have a hardware-based firewall in place. Commonly referred to as a NAT (Network Address Translation) firewall, this hardware device “hides” your home network from the hackers lurking on the Internet. This type of firewall creates a private LAN (Local Area Network) in your home, “translating” messages between your private LAN and the public Internet.

Some people feel safe and secure using the firewall software built into their computer. However, this is a false sense of security! The Microsoft Windows operating system contains so many bugs and holes, and hackers can easily bypass the firewall software. So don't bother with any software-based firewalls – they are simply too prone to hacking.



Setup and Installation is Key

Now we start to really drill down into the details. Did you know that all consumer-grade routers and firewalls come pre-configured as “open” access devices? This means that anyone – especially the hackers – could access the inner workings of your router/firewall and modify its settings. They could easily open up “back doors” into your network and, worse yet, use the router/firewall to discover every computer on your home LAN. Yikes! So follow these steps to ensure your router/firewall is locked down:

- Set an administrator password
- Ensure NAT is enabled (Working Mode=Gateway on some routers)
- Disable “Respond to PING” (Enable “Block WAN Request” on some routers)
- Disable IPSec and PPTP Passthrough
- Disable Remote Upgrade capabilities
- Disable Remote Management
- Disable UPnP services
- Disable DMZ Host
- Disable Port Forwarding
- Enable WEP (for Wireless Routers)

Super Secure

Do you store lots of personal/financial data on your computers? If so, you may want to consider some additional steps to limit access to your home network. Each one of these options, when implemented, provide one more barrier to unauthorized access.

- ❑ Enable MAC Address Filtering: you can control which computers are allowed access to your home network. Like a Social Security Number, MAC Addresses are unique to each and every computer built. You can allow access to your network by only authorized computers by activating MAC Address Filtering and configuring the router with the individual MAC Addresses only your computers. All other computers that attempt access to your network will be denied.
- ❑ Disable SSID Broadcasting: if you are running a wireless network, then you can “hide” the network by disabling SSID Broadcasting. SSID Broadcasting is the method used for any computer to “discover” a wireless network – if you disable this function then your wireless network will be invisible to the world!

Remember that implementing any of the above recommendations will make the setup and configuration of your computers more difficult. But after spending the time figuring out the exact configuration necessary, you can rest assured that your network is secure.

Welcome to IT Operations 101

One last point to always remember – configuration parameters can be changed! This can happen for a variety of reasons, including your router/firewall resetting itself, having your router/firewall “lose its mind,” or by simply making a mistake while modifying some other parameters. These consumer-grade routers/firewalls are cheap and run software that is buggy (yes, all software contains bugs, especially consumer-grade products – heck, Microsoft software is the worst on the planet! It’s filled with bugs that are exploited by Hackers every day!) So make it a normal course of action – say, on the first of every month – to double check that all your settings are correct. Follow these three simple steps:

- ❑ Power off then back on your router/firewall
- ❑ Access the router/firewall from your computer – does your password still work?
- ❑ Check all the settings, comparing them to the original settings (when you initially setup your router/firewall, “print screen” each configuration window to create a simple yet very functional set of documentation)

Immaculate Technology

About the Author

With more than 24 years as an information technology professional, Bruce has significant experience in IT management and operations. Working for a variety of Fortune 500 companies, he has established consulting practice areas, managed a variety of IT departments -- including application developers, quality assurance professionals, systems and network engineers, R&D analysts, and project managers -- and led efforts in establishing standards and methodologies in varying capacities.

For the past three years, Bruce has been instrumental in building up an IT Outsourcing firm serving the small-to-medium business market in San Diego, CA. Known as Immaculate Technology, Bruce's firm has built a customer base consisting of businesses in the publishing, home building, real estate, and medical industries. He established a level of service based on a simple concept -- bring his experience and know-how of more than 24 years working in the Fortune 500 business world to the small business owners of Southern California.