



Securing Your Home Wireless Network - Do's and Don'ts

- When creating passwords for your networks devices, ensure that they are sufficiently long and complex by using uppercase letters, lowercase letters, numbers, and symbols. Consider a multi-word phrase that does not consist of dictionary-based words. An example of a satisfactorily long and complex password would be lLuvF00tb@77 from the phrase "I love football."
- Use a cable to directly access the internet for any computers that remain stationary.
- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest access set up for your network, ensure that it is password protected.
- If possible, turn on automatic updates for your network device's firmware. If automatic updates are not offered, periodically check for firmware updates on the network devices' websites and manually download and install them.
- If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button located on the back of the router.
- Position the router away from windows and further into the interior of your house to decrease the exterior reach of the signal.

Glossary of Commonly Used Terms

Wireless Router - Physical hardware that allows users to connect their devices to a shared internet network.

Service Set Identifier (SSID) - The public name of a wireless network.

Wired Equivalent Privacy (WEP) - Older security algorithm for wireless networks that has numerous security flaws.

Wi-Fi Protected Access (WPA) - More recent security algorithm for wireless networks. Also has many security flaws.

Wi-Fi Protected Access II (WPA2) - The most secure algorithm for wireless networks. Improved upon and replaced WPA.

Pre-shared key (PSK) - An authentication mechanism that mandates a password. Adds additional security to wireless networks.

Hypertext Transfer Protocol (HTTP) - Protocol for communication over a computer network.

Hypertext Transfer Protocol Secure (HTTPS) - Uses various encryption protocols to add additional security to HTTP.

Media Access Control (MAC) Address - A unique, individual identifier assigned to computers and devices.

Access Your Router

To access your router, you must enter the appropriate IP address, username, and password. Most routers share similar log-in information.

Router	IP Address	Username	Password
3Com	192.168.1.1	n/a	admin
Apple	192.168.1.1	admin	admin
Asus	192.168.1.1	admin	admin
Belkin	192.168.2.1	admin	n/a
Dell	192.168.1.1	n/a	admin
Linksys	192.168.0.1	admin	admin
Medialink	192.168.0.1	n/a	admin
Motorola	192.168.100.1	admin	motorola
Netgear	192.18.0.1	admin	password
TP-LINK	192.168.1.1	admin	admin
US Robotic	192.168.1.1	admin	admin

Change the Username and Password

Choose a username that does not include you or your family's names and a password that is long and complex.

Creating a Unique SSID

Choose a SSID that does not include you or your family's names or physical address.

Disabling the SSID Broadcast

This prevents the SSID from being listed under available Wi-Fi networks, thereby requiring users to know and enter the SSID before connecting to the network.



Router Firewall

Enable the router's firewall protection to limit the router's vulnerability to viruses and cyber attacks.

Firewall	IPv6 SPI Firewall Protection: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled IPv4 SPI Firewall Protection: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
-----------------	--

Wireless MAC filtering

Enable MAC address filtering to ensure that only approved computers and devices can connect to your router.

Enabled Disabled

Prevent PCs listed below from accessing the wireless network.
 Permit PCs listed below to access the wireless network.

Wireless Client List

MAC 01:	<input type="text" value="00:00:00:00:00:00"/>	MAC 17:	<input type="text" value="00:00:00:00:00:00"/>
MAC 02:	<input type="text" value="00:00:00:00:00:00"/>	MAC 18:	<input type="text" value="00:00:00:00:00:00"/>

Enabling HTTPS

Enable access via HTTPS to add additional security.

Router Password:
 Re-Enter to Confirm:

Access via: HTTP **HTTPS**

Access via Wireless: Enabled Disabled

Limiting Administrative Access

Restrict administrative access through the web to specific devices. Add the MAC addresses for each computer and device you wish to have administrative access.

Local Management

Management Rules

All the PCs on the LAN are allowed to access the Router's Web-Based Utility
 Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:
 MAC 2:
 MAC 3:
 MAC 4:

Your PC's MAC Address:

Remote Access

Check that the Remote Management IP Address is set to **0.0.0.0** to ensure that remote access is disabled.

Remote Management Access

Remote Management: Enabled Disabled
 Access via: HTTP HTTPS
 Remote Upgrade: Enabled Disabled
 Allowed Remote IP Address: Any IP Address
 to

Remote Management Port:

Encryption

Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select **WPA2-PSK** and also **AES** for encryption. The PSK password should be long and complex, but different than the administrative router access password.

WPA-P SK/WPA2-P SK

Version:
 Encryption:
 PSK Password:

Useful Links - For more information or questions regarding this card email smartcards@novetta.com

Practically Networked
Wi-Fi.org
NIST

www.practicallynetworked.com/support/wireless_secure.htm
www.wi-fi.org/discover-wi-fi/security
<http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>

