Five blatant security mistakes you should avoid when setting up a wireless router (also known as an access point)

The first mistake, using old equipment that doesn't support the WPA or WPA2 security protocols. This can be a serious security mistake.

Why? WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA or WPA2, so you should specifically look for gear that supports encryption via WPA2

The second mistake is not resetting the router's internal administration logon name and password. After powering on the router and accessing its admin tool for the first time (refer to the routers manual), you should immediately change the admin tool's password and, if applicable, the admin tool's logon name.

Why? Because, router manufacturers use standard login names and passwords for all their devices, and a quick Internet search is all it takes to uncover this default information.

The third mistake goes hand-in-hand with the second one, and that's not choosing a strong enough router admin or network password.

Weak passwords are vulnerable to brute force, social engineering, and dictionary attacks. It's bad enough when you do this for other login accounts but you shouldn't make this mistake when setting up your router.

The forth mistake is relying on a hidden SSID or MAC address filtering for security.

Years ago, both techniques were widely recommended as ways to improve wireless security. But that time has passed.

Using wireless sniffers like ViStumbler, NetStumbler and Kismet, an attacker can easily uncover hidden SSIDs. It's also relatively easy to spoof another machine's MAC address.

Do yourself a favor, use meaningful SSID names so users will know they're connecting to the right network and rely on true security measures for protection.

The fifth and last mistake is abandoning a router once it's setup.

Too many people install routers, configure them to operate, and then forget about them until there's a problem. And, this can be a very long time -- years even.

- **As mentioned earlier, if you still have old equipment running WEP, you should replace it.**
- **If you've been relying on WPA with TKIP encryption, you should switch to WPA2 with an AES-based encryption mechanism.**
- **If you can't afford to replace your equipment, check if your equipment manufacturer has an updated driver that avoids sending weak Initialization Vectors (IVs)**