Voy a dar unas normas básicas muy sencillas para las personas de a pie, además de ser igualmente válido para empresas o gobiernos.
Si eres una empresa grande puedes contratar servicios a empresas de seguridad.

Normalmente las operadoras facilitan routers preconfigurados o gestionables en remoto. Pero la mayoría a pesar de estar actualizados tienen una serie de puertos abiertos, que de por si es para facilitar labor de actualización y mantenimiento, por contra permiten el acceso desde el exterior. La forma de reparar esto, es o bien poner el router en modo monopuesto y conectar un router-firewall propio completamente diferente (pero si tiene puertos abiertos desde el exterior volvemos a las mismas).

Problemas de tener puertos abiertos, no hace falta que sepan clave del router hay ataques que directamente por fallos de seguridad acceden y permiten el acceso al router, ya sean Botnets (red de robots de router que utilizan mafias), gobiernos, hackers para ataques, o minado de cryptomonedas (como buscar oro pero no para ti, tu lo haces para otro), o propagación de virus. Normalmente apagando y encendiendo el router esto se solventa, así que tranquilidad.

Lo ideal es si tiene un firewall el router activarlo, si no lo está y bloquear los puertos bajos de 1 al 1024 entrantes tanto en TCP como UDP o poner la política por defecto de que todo lo entrante se ignore (DROP).

Si vas a entrar al router, no te preocupes por tocar donde no debes, la mayoría tienen configuración por defecto debajo del router con los datos, si los cambias siempre puedes darle a un botón de reset para resetar la configuración. Y la mayoría de routers permiten salvar tu configuración en un fichero en tu ordenador y restaurarla, para que puedas trastear sin problemas.

Lo mas seguro es el cable, puedes tirar cable de red o utilizar PLC que usa la red eléctrica. Tu instalación eléctrica debe estar libre de ruidos eléctricos, una simple bombilla led mala puede hacer que tu red vaya muy lenta. Como curiosidad los contadores de las eléctricas usan un sistema PLC para enviar datos de tu consumo a la central.
El problema de Wifi es que va por radio, y no es lo mismo escuchar los cuarenta principales que un ruido incomprensible mediante un cifrado. Dentro de los cifrados los hay mas seguros y menos seguros.

- WEP: olvidate de este cifrado es el menos seguro, aunque mas seguro que no tener cifrado.
- WPA2: Es el cifrado mas potente en la actualidad, con salvedades de que no tengas activo WPS

WPS: Wifi Protected Systen. Facilita introducir un pin presionando un botón del router, en vez de poner toda la clave. Esto es una brecha de seguridad por lo que debe desactivarse. Por defecto está activo en todos los routers de las compañías…

Utiliza si es posible cifrado WPA2, con una clave compleja mezclando Letras y símbolos por ejemplo *#@?-

Entrando en la gestión del router puedes cambiar el nombre de tu red wifi, poniendo la que mas te guste.