



December 2025.

Should we worry about ‘Default Passwords’?

Default passwords feature on most devices manufactured for online use. These passwords are pre-set during the manufacturing stage to simplify the initial setup of the device.

When we consider the Internet of Things (IOT) and how many internet connected devices we have, either at home, within industry, healthcare and transport i.e. wi-fi routers, doorbells, security cameras, heating controls, speakers, refrigerators, air quality monitors, printers and devices linked to improve the performance of systems, these will all have been allocated default passwords.

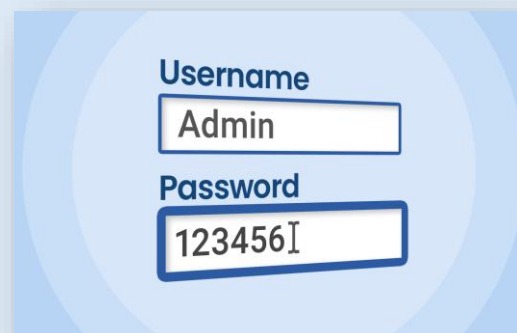
When we consider presents that will be received this Christmas, how many of these will be internet enabled with default passwords?

Whilst default passwords are meant to be temporary, many users leave them unchanged, considering this too difficult or an inconvenience.

Leaving default passwords unchanged is a security risk, especially when you consider most devices will have a sticker applied to them with that privileged data. It is important to consider this as a potential security risk, remove that information, whilst ensuring renewed passwords remain private only to those with the privilege to know that information.

It is incumbent on us, as individuals and organisations, to change default passwords on internet enabled devices, not only during the initial set up phase but also retrospectively if, we are currently using them with the default password.

Attackers can exploit default passwords to gain access to systems, networks and devices. Some of the associated risks include unauthorised access to data and the compromise of some critical operating systems. So, changing default passwords should apply to all current, new, modified or replaced systems and devices, unless of course you have changed the default password at the setup phase.



Username
Admin

Password
123456

Warning!! You are using the default password

For your security please change the default password using three random words [Three random words - NCSC.GOV.UK](https://www.ncsc.gov.uk/3-random-words)

OFFICIAL

To mitigate these risks, it is crucial to change default passwords using strong, unique passwords and of course renaming the device, so it is not easily recognised out with your environment. [Three random words - NCSC.GOV.UK](#)

Internet connected devices may also be subject to software updates, and it is extremely important to run these updates as they provide critical security patches and bug fixes, whilst also improving performance of the device itself. [Install the latest software and app updates - NCSC.GOV.UK](#)

The NCSC also have this guidance to support you manage [Smart devices: using them safely in your home - NCSC.GOV.UK](#)

In summary, whilst there is a [New security law for smart devices: Your rights as a consumer](#) urging manufacturers to comply with the legislation to ban default passwords, it is still good practice to change these and mitigate any risk.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

OFFICIAL