Securing products when connecting to a network

Published: October 11, 2021
Canon. Inc.

Many products and their various functions can be used more conveniently by connecting to a network. However, connecting products to a network introduces the possibility of security risks such as unauthorized access by malicious third parties.

For example, if a product is connected to a network with a default password or a password that is easy to guess, there is a risk of undesired changes to settings or data extraction. In addition, connecting a product to the internet without using a wired router or Wi-Fi router poses a greater risk of unauthorized access.

In order to minimize the risk of security issues, it is necessary to apply the appropriate settings and use your products in a secure environment.
Below we have outlined a number of security measures intended to help customers use Canon products in a more secure way.

Security measures when using Canon products

When setting up the product

1. Only connect products to trusted networks.
2. It is not recommended that a product is connected directly to the internet. When connecting to the internet, use a private IP address in an environment where the internet can be accessed from a secure private network built with firewall products, wired routers or Wi-Fi routers.
3. Change the product's default password to a new password.
4. Set up administrator and general users IDs and passwords if possible.
5. Ensure that passwords and other similar settings for various functions are sufficiently difficult to guess.
6. If the product has authentication functions, use them to manage who can use the product.

7. If the product has network filters, use them to limit the addresses that can communicate with the product.
8. Use any encryption functions the product may have.
9. When possible, disable functions and ports that aren't being used.
10. Set the product's security function settings as strong as possible
11. Be aware of physical security needs, including those related to the location of the product etc.

When operating the product

12. When using functions that communicate via a network, ensure you are using a trusted connection destination (e.g. server) before connecting.
13. Regularly check the Canon website to ensure you are up to date with security-related information.
14. Use the latest firmware.
15. If the product saves communication logs, check them regularly to find any unauthorized access.
16. If you won't be using the product for a long period, switch it off.
17. Back up the data and settings stored in the product regularly

When disposing of the product

18. When disposing of the product, delete all data and set-points saved on the device.