Seguridad de los productos al conectarse a una red

Publicado: 11 de octubre de 2021
Canon Inc.

Muchos productos y sus diferentes funciones se pueden utilizar de forma más conveniente mediante la conexión a una red. Sin embargo, la conexión de productos a una red conlleva la posibilidad de riesgos de seguridad, como el acceso no autorizado por parte de terceros malintencionados.

Por ejemplo, si un producto está conectado a una red con una contraseña predeterminada o una contraseña fácil de descifrar, existe el riesgo de que se produzcan cambios no deseados en las configuraciones o la extracción de datos. Además, la conexión de un producto a Internet sin utilizar un enrutador por cable o enrutador Wi-Fi representa un mayor riesgo de acceso no autorizado.

Con el fin de minimizar el riesgo de problemas de seguridad, es necesario aplicar las configuraciones adecuadas y utilizar sus productos en un entorno seguro.
A continuación, se describen una serie de medidas de seguridad destinadas a ayudar a los clientes a utilizar los productos Canon de forma más segura.

Medidas de seguridad al utilizar productos Canon

Al configurar el producto

1. Conecte los productos únicamente a redes de confianza.
2. No se recomienda que un producto esté conectado directamente a Internet. Al conectarse a Internet, utilice una dirección IP privada en un entorno al que se pueda acceder a Internet desde una red privada segura creada con productos de servidores de seguridad (firewall), enrutadores por cable o enrutadores Wi-Fi.
3. Cambie la contraseña predeterminada del producto por una nueva.
4. Si es posible, configure las ID y las contraseñas del administrador y de los usuarios generales.
5. Procure que las contraseñas y otras configuraciones similares para diferentes funciones sean lo bastante difíciles de descifrar.

6. Si el producto tiene funciones de autenticación, utilícelas para administrar quién puede usar el producto.
7. Si el producto tiene filtros de red, utilícelos para limitar las direcciones que pueden comunicarse con el producto.
8. Utilice cualquier función de encriptación que pueda tener el producto.
9. Cuando sea posible, inhabilite las funciones y los puertos que no se estén utilizando.
10. Defina las configuraciones de la función de seguridad del producto del modo más estricto posible.
11. Tome en cuenta las necesidades de seguridad física, incluidas las relacionadas con la ubicación del producto, etc.

Al utilizar el producto

12. Cuando se utilicen funciones que se comunican mediante una red, asegúrese de usar un destino de conexión de confianza (por ejemplo, un servidor) antes de conectarse.
13. Consulte regularmente el sitio web de Canon para mantenerse actualizado sobre la información relacionada con la seguridad.
14. Utilice el firmware más reciente.
15. Si el producto guarda los registros de comunicación, verifíquelos regularmente para encontrar cualquier acceso no autorizado.
16. Apague el producto si no lo va a utilizar por un largo periodo.
17. Realice una copia de seguridad de los datos y las configuraciones almacenadas en el producto con regularidad.

Al desechar el producto

18. Al desechar el producto, borre todos los datos y los valores configurados que estén guardados en el dispositivo.