HACK THE HOUSE

Frequent questions. Fully answered.

Everything about handling your printer at home.

1. How can I update / patch my printers and other IoT devices?

Using the Auto Update feature whenever available is a good practice in maintaining the latest updates on printers and IoT devices. We also recommend consulting with the specific device manufacturers for other best practices.
See HERE for more information.

2. What are some of the common threats and attack vectors for home users?

Some of the most common threats and attack vectors we are seeing amongst home users are social engineering attacks, phishing attacks, use of default credentials and weak password practices, and the exploitation of unpatched systems and devices.
Click HERE to learn more about cyber security best practices.

3. What are some of the phishing red flags to watch out for?

Pelling and grammatical mistakes are easy to detect phishing red flags, other warning signs are embedded links (hover over links before clicking), unsolicited requests to update credentials, and petitions to support charitable causes, especially related to Covid-19/pandemic.

4. How can I better prepare my home office workers to be more security aware?

Steady communications to users about the threats they face, how to respond and where to report incident can help home office users to be more security aware. Ongoing training with end-user signoff to acknowledge understanding is also good practice.

5. How can I identify all devices connected to my home network?

The use of router administration tools can help identify devices connected to networks.
Click HERE to learn more about cyber security best practices.

6. What can I do if I don't recognize a device connected to my network?

If an unknown device is connected to your network, immediately change the Wi-Fi password and put in place a password that uses strong complexity rules.

7. What are some password managers you would recommend?

As policies vary, our response is to follow your corporate guidance relating to password managers and password vaults.