Securing your Home Router

Introduction

1. This document provides basic guidance on how to secure a home router. For device-specific instructions and advanced configuration, see the original manufacturer’s user guide.

2. This guideline has been issued by the Chief Information Officer to supplement the Working Remotely standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Basic Recommendations

Login to your home router and do the following:

1. Check for firmware updates, and upgrade if available by:
   a. turning on automatic firmware updates whenever possible; or
   b. setting up a monthly task as a reminder to log in to see whether any new versions are available.

2. Verify that "Remote Administration" or "Administration from WAN/Internet" are disabled. If enabled, these settings allow access to the management UI from the Internet.

3. Review firewall settings for any open or proxied ports. If you're unsure of the origin of a particular entry, disable it.

4. Check Wi-Fi network settings, if applicable, and verify that you're using WPA3 Wi-Fi security standard (if supported), or at least WPA2 with AES encryption.


6. Make sure your network password is complex and not related to the network name.

7. Review your attached devices list for anything suspicious, and verify the identity of unknown hosts.

8. Give proper consideration to your IoT Devices:
   a. ensure you know how to recognize these on your home router;
   b. regularly check for security patches;
   c. protect with a complex password and do not use the same passwords across your devices; and
   d. consider adding your IoT devices to a “guest” network.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Working Remotely standard

Securing Internet of Things (IoT) Devices standard