Cyber Security Blocking

To help protect our customers and Canada's communications networks, we use cyber security blocking measures. The following explains what is being blocked, why, and how you can reach us if you have any questions or concerns.

Purpose of Cyber Security Blocking

This blocking follows the terms and conditions set out in *Development of a framework to limit botnet traffic, Compliance and Enforcement and Telecom Decision CRTC 2025-142 (13 June 2025).*

- The blocking is done **exclusively for the purpose of protecting against cyber attacks.**
- It is **not used for any other purpose,** such as blocking other illegal activities, or for commercial, competitive, or political reasons.
- The goal is to protect your devices from:
    - **Botnets** (networks of malware-infected devices controlled without the owner's knowledge or consent),
    - **Malware**, and
    - **Phishing threats.**
- This blocking does **not involve looking at the content of websites you visit.** For example, it does not target websites offering illicit goods or services, false or misleading news, abusive comments, or obscene material.

How Cyber Security Blocking Works

- Blocking is applied **at the network level by default.** Customers cannot opt in or opt out.
- The blocking is based on a **blocklist of indicators** that have been vetted as malicious.
- Indicators may include:

- IP addresses
- IP addresses with port numbers
- Domain names

Complaints and Questions

If you believe that a website, service, or connection has been blocked in error (“false positive” or over-blocking), you may contact us blocking), you may contact us email us at securityblocking@hay.net or contact us through any of our customer service locations.

Complaint process:

1. We will acknowledge receipt of your complaint.
2. Our cyber security team will investigate and review the blocklist entry.
3. We will notify you of the outcome once the investigation is complete.

Your Role in Staying Protected

Cyber security blocking helps make your Internet service safer, but it is **not a replacement** for protecting your own devices. Customers remain responsible for safeguarding their computers, smartphones, and networks.

We strongly recommend that you:

- Install and update antivirus or anti-malware software
- Keep your devices and applications updated with the latest patches
- Use and manage a firewall
- Choose strong and unique passwords
- Enable two-factor authentication where possible
- Secure your home Wi-Fi connection