Wightman

As part of Wightman's commitment to protecting our customers, and in alignment with Compliance and Enforcement and Telecom Decision

CRTC Decision 2025-142, Development of a framework to limit botnet traffic, 13 June 2025,

Wightman utilizes a network-level cyber security blocking framework. This framework is designed to safeguard Wightman customers from malicious botnets and other cyber threats.

Purpose of Blocking

The blocking is conducted **exclusively for customer protection against cyber-attacks**. Specifically, it aims to:

- Prevent your devices from being infected by malicious software by blocking access to known bad Internet sites which serve no legitimate content. This blocking includes malicious sites hosting malware, phishing, adware, and sites associated with botnets.

This blocking is **not** used for:

- Censoring or filtering content based on its nature or legality
- Blocking websites offering illicit goods or services
- Suppressing political, commercial, or competitive content
- Evaluating or restricting access to websites based on opinions, misinformation, or offensive material
- Tracking internet usage

How Blocking Works

- **Type of Blocking:** Wightman uses a domain-based approach. This means we block traffic based on a list of known bad domains that have been vetted by trusted cyber threat intelligence sources.
- **Indicators Used:** Domain names
- **Application:** Blocking is applied by default at the network level. This means:
    - You do not need to opt-in
    - You cannot opt-out

This ensures consistent protection for all users on our network.

Transparency and Accountability

We are committed to transparency and accountability in how we implement this framework. Our blocking practices follow the terms and conditions set out in CRTC Decision 2025-142, and we are subject to oversight by the CRTC.

Filing a Complaint or Reporting a False Positive

If you believe a website or service has been blocked in error (a “false positive”), or if you have concerns about over-blocking, you can contact us by calling at **1-888-477-2177**.

Complaint Process

1. Submit your complaint with as much detail as possible with account number, name and URL, and time of access attempt.
2. Our technical support team will investigate the issue.
3. We will respond with findings and, if applicable, take corrective action.

Your Role in Cyber Security

While Wightman is responsible for protecting our network, you are responsible for protecting your devices. Wightman recommends the following best practices:

- Install and regularly update antivirus and anti-malware software
- Keep your operating system and applications up to date
- Use strong, unique passwords and enable two-factor authentication where possible
- Secure your home Wi-Fi network
- Be cautious of suspicious emails, links, and downloads

Updates to Blocking Mechanisms

If Wightman implements a new blocking mechanism or modifies an existing one, we will update this disclosure at least **30 days** in advance. This ensures you are always informed about how your Internet service is being protected.

Accessibility

This page is designed to be accessible in accordance with the CRTC's Accessibility Policy (Broadcasting and Telecom Regulatory Policy CRTC 2009-430 and 2009-430-1). If you require this information in an alternative format (for example, large print, braille, or audio), please contact our Customer Service Department at 1-888-477-2177, or visit https://www.wightman.ca/residential/commitment-to-accessibility/

This disclosure is made in accordance with: Compliance and Enforcement and Telecom Decision CRTC 2025-142