Manchester-Hartland Telephone Company Network Management

Practices:

MHTC goal is to provide the best and most reliable internet possible for its customers. MHTC seeks to provide and maintain adequate bandwidth and network capacities within our network. MHTC also seeks to provide adequate facilities and bandwidth capacity to upstream providers that allow our customers access to the Internet.

MHTC does not generally block, throttle or prioritize internet traffic. If MHTC receives notification or determines that a MHTC customer's internet connected device is knowingly or unknowingly causing internet disruption outside of our network, MHTC may throttle or disconnect the MHTC customer until the device causing the disruption is removed or the issue with the internet device remediated. An example of a possible issue: An MHTC customer has a device or devices that has been hacked as an internet bot and is causing DDOS attack on other MHTC customers, on another internet provider or a customer of another internet provider.

Congestion Management Practices:

MHTC works to maintain adequate network and bandwidth capacity. MHTC has deployed a fiber network that consists of almost 100% active fiber. An active fiber network means there is a strand of fiber from the MHTC Central Office equipment to each customer premise. This allows for maximum bandwidth capacity with minimum latency to the customers. MHTC monitors bandwidth utilization on our network. Also, MHTC monitors the connection to our upstream provider for bandwidth utilization, connection, and latency problems.

Application-Specific Behavior Practices:

MHTC does not favor or discriminate against lawful applications, protocols or content. Copyright, trademark infringements or the circumventing Digital Millennium Copyright Act (D.M.C.A.) are illegal and could result in the termination of services.

MHTC may temporarily or permanently terminate a customer's service if an application is determined to be harmful to the network or if there is illegal activity.

Device Attachment Rules:

Customers may use any lawful device that is compatible with MHTC's network. Generally compatible devices include computers, wireless routers or access points. Cable or DSL modem wireless routers are generally not compatible with MHTC's network. MHTC reserves the right to protect MHTC network or other another Internet providers network by temporarily disconnecting service until the incompatible, infected or malicious device is removed or the device's issue is corrected.

Security:

MHTC highly recommends customers use a router that utilizes a firewall for security. Additionally, MHTC recommends customers use software that helps prevent viruses, spam and malware.

Inbound and Outbound filtering of specific network devices or address may be implemented to protect MHTC's network. This filtering may be used during a DoS, DDoS attack, address spoofing or any other type of malicious traffic.

MHTC will work with customers, other ISP's and Government agencies, if the need arises, to determine the source of the malicious traffic and attempt to prevent further disruptions. If our customer is determined to be a source of the malicious traffic, their service may be temporarily or permanently terminated.

Privacy Policies

MHTC follows guidelines set by the Government, as an ISP we are required to maintain a record of certain traffic information. This information follows the Communications Assistance for Law Enforcement Act (CALEA) and the Foreign Intelligence Surveillance Act (FISA).

MHTC does not collect data from its customers in order to target them for additional sales or services.