



AUP Enforcement

**A Guide to the Network Policy
Management Department**

Excite @ Home



Presentation Overview

- Our Process
- Abuse Topics
- MSO and NPM Relationship



Our Process

- Report of abuse
- Investigate the Report
- Take Action
- Document the Events



Where the reports come from

- Mail is received to abuse@home.com
- Phone calls to 650-556-5399
- Email sent to abuse-team, abuse-policy



We Investigate the Report

We evaluate the report

- Is it ours?
- Is it legitimate?
- Is it complete?

We determine action taken

- No Action
- Warn
- Suspend
- Terminate



We Act

- Actions are defined in the Interpretation Guidelines
- Each MSO has provided a contact name for abuse consultation
- Suspension generally requires MSO notification
- Termination always requires MSO involvement

Excite @ Home



We Document the Events

Tickets are created in Remedy for abuse reports. We connect the incident to the customer's record, along with our actions.



Common Abuse Mailbox Topics

- Spam Email
- USENET postings that are off-topic
- Port Scanning
- Copyright Issues with Servers
- Invalid Reports



More Serious Abuse Reports

- Illegal Activity- Law Enforcement Reports
- Copyright Infringement - RIAA - agreement
- IP theft - Trends of Hacking Reports
- Deliberate Intrusion / Hacking - Sys Admin



MSO Involvement

- We contact the MSO for notification of suspension.
- We contact the MSO to work with us to terminate a problem customer.
- We want the MSO to work with us to ensure one message.
- MSO maintains ownership of the customer relationship.
- We would like to maintain clear communication between the MSO and the NPM team.



What we do for you

- We sort through the reports of abuse and identify the real from the invalid
- We notify you of problems before they get larger
- We can work with you to understand how our subscribers are behaving



Conclusion

- We follow a fairly rigorous process to handle abuse reports.
- We see a variety of types of abuse, from simple Email Spam to complicated hacks.
- We work with our Cable Partners to ensure that our AUP enforcement is fair and mindful of the subscriber relationship we both maintain.



Common Questions

- Customers receiving spam
- Ops-Scans
- Port Scans
- Bandwidth
- Abuse does nothing?



Answers to those questions

- Spam Received- technological fix- short term in Server Admin longer term in Brightmail solution
- Ops-Scans- we are continuing to scan the network to keep our subscriber base safe from vulnerability
- Port Scans- We sort through Black Ice reports versus persistent trojan attacks
- Bandwidth- based on current staffing and goals, we address subscribers who are severely degrading network performance. Hiring 2 people Q2 to expand some of the resource efforts.
- Abuse does nothing? Replies coming, implementing Kana



Direction - 3 Tier Model

- Policy Development
- Policy Management
- Policy Enforcement



Goals for Y2K

- Tools
- Abuse Mail Management
- @Work
- Residential Product Enforcement
- MSO Communications



UDP as an example of Goals

- **Tools- Ops Scan to look at open port 119 connections; longer term looking at capacity planning software to give us some network wide traffic data**
- **Abuse Mail Management- identification of key Internet correspondents; longer term- Kana**
- **@Work- Newshub1 guidelines; develop AUP Interpretation Guidelines for @Work; @Work Enforcement staffing**
- **Residential Product Enforcement- working with Product Development to set limits for residential news usage. Beyond news, working on definitions for all core services.**
- **MSO Communications- Aggressive communications from me during the UDP events. Sent out 5 emails over a week explaining the global view of the current situation. Collecting policy contacts and presenting at MSO events (Product Strategy, Engineering Ops, and Customer Care) Regular communications via conference call or email?**