Problem
Home computers are insecure, and are frequently compromised and combined into botnets by hackers. Home computer users have resisted security technologies that require knowledge and effort. Security companies try to make one-size-fits-all solutions, but these solutions inevitably fall short because of the diversity of computer uses. Unfortunately, the only person who has the information needed to customize security technologies to the actual uses of the computer is the end user, who generally lacks the training and incentive to put such knowledge to good use.

Basic Idea: Social Firewall
Built on the idea of a personal firewall, we propose a technology that encourages users to share security information with each other.

Benefits
- Help users customize security to individual needs
- Information uses language that users understand
- Doesn’t require effort from experts

Approach and Impact

<table>
<thead>
<tr>
<th>New approach</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build on existing technology -- personal firewalls</td>
<td>Botnets are primarily built from insecure home computers</td>
</tr>
<tr>
<td>Information sharing among home users</td>
<td>Has potential to improve not only security of home computers, and thus to increase cost of creating a botnet</td>
</tr>
<tr>
<td>Design incentives to share, reduce attack surface</td>
<td></td>
</tr>
<tr>
<td>Incorporate ideas from economics &amp; psychology into design of security technology</td>
<td></td>
</tr>
</tbody>
</table>

Primary Challenge
Design technology to induce users to contribute useful information

How?
Utilize theories from the social sciences:
• Motivation from Psychology
• Strategic Incentives from Economics

Details
We are exploring a number of theoretically grounded ideas for inducing contribution:
• Comments provide private benefits. Specifically, the ability to organize and revisit policy decisions
• Voting on comments, using a proper scoring rule, to encourage high quality contributions
• Forming small groups of friends and sharing comments among the group
• Evaluating small-group performance, and providing a benchmark