Index.html

<!DOCTYPE html>

**<html** lang="en"**>**

**<head>**

**<meta** charset="utf-8"**>**

**<meta** http-equiv="X-UA-Compatible" content="IE=edge"**>**

**<meta** name="viewport" content="width=device-width, initial-scale=1"**>**

**<title>**Anti Spam E-Mail techniques**</title>**

*<!-- bootstrap styles -->*

**<link** href="bootstrap/dist/css/bootstrap.min.css" rel="stylesheet"**>**

*<!-- my styles -->*

**<link** href="starter-template.css" rel="stylesheet"**>**

**</head>**

**<body>**

**<nav** class="navbar navbar-inverse navbar-fixed-top"**>**

**<div** class="container"**>**

**<div** class="navbar-header"**>**

**<button** type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar"**>**

**<span** class="sr-only"**>**Toggle navigation**</span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**</button>**

**<a** class="navbar-brand" href="#"**>**Spam**</a>**

**</div>**

**<div** id="navbar" class="collapse navbar-collapse"**>**

**<ul** class="nav navbar-nav"**>**

**<li** class="active"**><a** href="index.html"**>**Home**</a></li>**

**<li><a** href="techniques.html"**>**List of Techniques**</a></li>**

**<li><a** href="new.html"**>**New Solutions**</a></li>**

**</ul>**

**</div>***<!--/.nav-collapse -->*

**</div>**

**</nav>**

**<div** class="container"**>**

**<div** class="starter-template"**>**

**<h1>**Anti EMail Spam Techniques**</h1>**

**<p** class="bodyClass"**>**Various anti-spam techniques are used to prevent email spam (unsolicited bulk email).

**<br>**

**<br>**

No technique is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate email (false positives) vs. not rejecting all spam (false negatives) – and the associated costs in time and effort.

**<br>**

**<br>**

Anti-spam techniques can be broken into four broad categories: those that require actions by individuals, those that can be automated by email administrators, those that can be automated by email senders and those employed by researchers and law enforcement officials.**</p>**

**</div>**

**</div>**

**<script** src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"**></script>**

**<script>**window.jQuery || document.write('<script src="../../assets/js/vendor/jquery.min.js"><\/script>')**</script>**

**<script** src="bootstrap/dist/js/bootstrap.min.js"**></script>**

**</body>**

**</html>**

new.html

<!DOCTYPE html>

**<html** lang="en"**>**

**<head>**

**<meta** charset="utf-8"**>**

**<meta** http-equiv="X-UA-Compatible" content="IE=edge"**>**

**<meta** name="viewport" content="width=device-width, initial-scale=1"**>**

**<title>**Anti Spam E-Mail techniques**</title>**

*<!-- bootstrap styles -->*

**<link** href="bootstrap/dist/css/bootstrap.min.css" rel="stylesheet"**>**

*<!-- my styles -->*

**<link** href="starter-template.css" rel="stylesheet"**>**

**</head>**

**<body>**

**<nav** class="navbar navbar-inverse navbar-fixed-top"**>**

**<div** class="container"**>**

**<div** class="navbar-header"**>**

**<button** type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar"**>**

**<span** class="sr-only"**>**Toggle navigation**</span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**</button>**

**<a** class="navbar-brand" href="index.html"**>**Spam**</a>**

**</div>**

**<div** id="navbar" class="collapse navbar-collapse"**>**

**<ul** class="nav navbar-nav"**>**

**<li><a** href="index.html"**>**Home**</a></li>**

**<li><a** href="techniques.html"**>**List of Techniques**</a></li>**

**<li** class="active"**><a** href="new.html"**>**New Solutions**</a></li>**

**</ul>**

**</div>***<!--/.nav-collapse -->*

**</div>**

**</nav>**

**<div** class="container"**>**

**<div** class="starter-template"**>**

**<h1>**New Solutions**</h1>**

**<ol>**

**<h2><li>**Cost based Systems**</li></h2>**

**<p>**Since spamming is facilitated by the fact that large volumes of email are very inexpensive to send, one proposed set of solutions would require that senders pay some cost in order to send email, making it prohibitively expensive for spammers. Anti-spam activist Daniel Balsam attempts to make spamming less profitable by bringing lawsuits against spammers.**</p>**

**<h2><li>**Other techniques**</li></h2>**

**<p>**

There are a number of proposals for sideband protocols that will assist SMTP operation. The Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF) is working on a number of email authentication and other proposals for providing simple source authentication that is flexible, lightweight, and scalable. Recent Internet Engineering Task Force (IETF) activities include MARID (2004) leading to two approved IETF experiments in 2005, and DomainKeys Identified Mail in 2006.

**</p>**

**<p>**

DMARC, which stands for "Domain-based Message Authentication, Reporting and Conformance" standardizes how email receivers perform email authentication using the well-known Sender Policy Framework (SPF) and DKIM mechanisms.

**</p>**

**<p>**

Channel email is a new proposal for sending email that attempts to distribute anti-spam activities by forcing verification (probably using bounce messages so back-scatter doesn't occur) when the first email is sent for new contacts.**</p>**

**<h2><li>**Research conferences**</li></h2>**

**<p>**Spam is the subject of several research conferences, including**</p>**

**<ul>**

**<li><a** href="https://en.wikipedia.org/wiki/MAAWG"**>**Message Anti-Abuse Working Group**</a></li>**

**<li><a** href="https://en.wikipedia.org/wiki/Text\_Retrieval\_Conference"**>**TREC**</a></li>**

**</ul>**

**</ol>**

**</div>**

**</div>**

**<script** src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"**></script>**

**<script>**window.jQuery || document.write('<script src="../../assets/js/vendor/jquery.min.js"><\/script>')**</script>**

**<script** src="bootstrap/dist/js/bootstrap.min.js"**></script>**

**</body>**

**</html>**

techniques.html

<!DOCTYPE html>

**<html** lang="en"**>**

**<head>**

**<meta** charset="utf-8"**>**

**<meta** http-equiv="X-UA-Compatible" content="IE=edge"**>**

**<meta** name="viewport" content="width=device-width, initial-scale=1"**>**

**<title>**Anti Spam E-Mail techniques**</title>**

*<!-- bootstrap styles -->*

**<link** href="bootstrap/dist/css/bootstrap.min.css" rel="stylesheet"**>**

*<!-- my styles -->*

**<link** href="starter-template.css" rel="stylesheet"**>**

**</head>**

**<body>**

**<nav** class="navbar navbar-inverse navbar-fixed-top"**>**

**<div** class="container"**>**

**<div** class="navbar-header"**>**

**<button** type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar"**>**

**<span** class="sr-only"**>**Toggle navigation**</span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**<span** class="icon-bar"**></span>**

**</button>**

**<a** class="navbar-brand" href="index.html"**>**Spam**</a>**

**</div>**

**<div** id="navbar" class="collapse navbar-collapse"**>**

**<ul** class="nav navbar-nav"**>**

**<li><a** href="index.html"**>**Home**</a></li>**

**<li** class="active"**><a** href="techniques.html"**>**List of Techniques**</a></li>**

**<li><a** href="new.html"**>**New Solutions**</a></li>**

**</ul>**

**</div>***<!--/.nav-collapse -->*

**</div>**

**</nav>**

**<div** class="container"**>**

**<div** class="starter-template"**>**

**<h1>**Techniques for reducing email spam.**</h1>**

**<div** class="container-fluid"**>**

**<div** class="row"**>**

**<div** class="col-sm-6"**>**

**<div** class="well"**>**

**<h3>**For End Users**</h3>**

**<ul>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Discretion"**><li>**Discretion**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Address\_munging"**><li>**Address Munging**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Avoid\_responding\_to\_spam"**><li>**Avoid Responding to Spam**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Contact\_forms"**><li>**Contact Forms**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Disable\_HTML\_in\_email"**><li>**Disable HTML in Email**</li></a>**

**</ul>**

**</div>**

**</div>**

**<div** class="col-sm-6"**>**

**<div** class="well"**>**

**<h3>**For Email Administrators**</h3>**

**<ul>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Authentication"**><li>**Authentication**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Challenge.2Fresponse\_systems"**><li>**Challenge / Response Systems**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Country-based\_filtering"**><li>**Checksum Filtering**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#URL\_Filtering"**><li>**URL Filtering**</li></a>**

**<a** href="https://en.wikipedia.org/wiki/Anti-spam\_techniques#Honeypots"**><li>**Honeypots**</li></a>**

**</ul>**

**</div>**

**</div>**

**</div>**

**<h3>**Interesting Solutions**</h3>**

**<dl>**

**<dt>**Tarpits**</dt><dd>**A tarpit is any server software which intentionally responds extremely slowly to client commands. By running a tarpit which treats acceptable mail normally and known spam slowly or which appears to be an open mail relay, a site can slow down the rate at which spammers can inject messages into the mail facility. Many systems will simply disconnect if the server doesn't respond quickly, which will eliminate the spam. However, a few legitimate email systems will also not deal correctly with these delays.**</dd>**

**<dt>**Spamtrapping**</dt><dd>**Spamtrapping is the seeding of an email address so that spammers can find it, but normal users can not. If the email address is used then the sender must be a spammer and they are black listed.**</dd>**

**<dt>**Quit detection**</dt><dd>**An SMTP connections should always be closed with a QUIT command. Many spammers skip this step because their spam has already been sent and taking the time to properly close the connection takes time and bandwidth. Some MTAs are capable of detecting whether or not the connection is closed correctly and use this as a measure of how trustworthy the other system is.**</dd>**

**</dl>**

**<h3>**Hybrid Filtering Example**</h3>**

**<p>**Hybrid filtering, such as is implemented in the open source programs SpamAssassin and Policyd-weight uses some or all of the various tests for spam, and assigns a numerical score to each test. Each message is scanned for these patterns, and the applicable scores tallied up. If the total is above a fixed value, the message is rejected or flagged as spam. By ensuring that no single spam test by itself can flag a message as spam, the false positive rate can be greatly reduced.

Several appliances such as the Barracuda Networks Spam firewall, and services like Postini and Cudamail employ spam scoring and bayesian filtering to arrive at thresholds which determine filtering action. An example of defaults might be:**</p>**

**<table** class="table"**>**

**<thread><tr>**

**<th>**Threshold**</th>**

**<th>**Action**</th>**

**</tr></thread>**

**<tbody>**

**<tr><td>**3**</td><td>**Tag the email (add a "tagged" or "suspected spam" type of string to the email subject line to assist end users in checking their inbox).**</td></tr>**

**<tr><td>**4.5**</td><td>**Quarantine the email (hold it, and email the end user to let them know that it quite possibly is spam and as a result they must log in and see it). Typically this type of action is taken due to more "spammy" features in the email such as hyperlinks, more image content than text, or certain words.**</td></tr>**

**<tr><td>**6**</td><td>**Block the email (do not allow it through). Typically this action is taken due to presence in the email of words like viagra, or links to malware sites, or to urls that are known to be used by spammers, or to have been blacklisted by a variety of online blacklist services like Barracuda Central or SpamHaus.**</td></tr>**

**</tbody>**

**</table>**

**</div>**

**</div>**

**</div>**

**<script** src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"**></script>**

**<script>**window.jQuery || document.write('<script src="../../assets/js/vendor/jquery.min.js"><\/script>')**</script>**

**<script** src="bootstrap/dist/js/bootstrap.min.js"**></script>**

**</body>**

**</html>**

styles.css

*/\*Some example tags for future reference\*/*

*/\*html tag selector\*/*

**body**

{

**padding-top**: 50px;

}

*/\*class selector\*/*

**.classSelector**

{

**text-align**: **right**;

}

*/\*selects all elemetns\*/*

\*

{

}

*/\*selects all body AND all p elemnts\*/*

**body**, **p**

{

}

*/\*Actual css for HW1 pages\*/*

**p**

{

**text-align**: **left**;

}

**li**

{

**text-align**: **left**;

}

**h1**

{

**text-align**: **center**;

**font-weight**: **bold**

}

*/\*add a litte indent to the body on the main page\*/*

**.bodyClass**

{

**text-indent**: 10;

}

**.starter-template**

{

**padding**: 40px 15px;

*/\*text-align: center;\*/*

}