

Technical Details for Adjusting Campus Spam Filters

- **IP addresses of the NSSE mail-relay:** 129.79.1.58, 134.68.220.35
- **Sending account:** nsse@nssesurvey.org
- **From name:** NSSE (institutions can customize from name – see phishing section below)
- **Sending speed:** Messages are sent using a bulk email program that sends as many as 50 or more messages per minute per institution.
- **Sending window:** Between 8 a.m. and 9 p.m. local time on your scheduled delivery days. NSSE is unable to specify the exact time of day messages will be delivered.

Working with Commercial Email Providers (Microsoft, Google, etc.)

Potential Issues

It's not always easy to confirm that messages have been successfully delivered to student inboxes when using commercial email providers. For example, in a recent NSSE administration a campus contact notified NSSE with concern over low response rates. There was no evidence of technical issues; however, after several days of investigation by campus IT staff it was discovered that all emails sent to student Gmail/Umail accounts (Google) had been sent to a spam filter. IT staff made an easy adjustment and subsequent messages delivered successfully. If your campus uses such a service, NSSE recommends that you identify the person(s) on your campus that can monitor successful email delivery and ask that they check for delivery the day after a message is sent. Once NSSE sends a message we cannot see if a message delivers to the inbox or a junk mail folder; however, messages that are returned ("bounced") are tracked and displayed on the Interface for your review.

What NSSE Does

NSSE adheres to the recommended best practices as suggested by these companies, and registers our status with them as a legitimate organization so that our messages are not treated as spam. NSSE uses DomainKeys Identified Mail (DKIM) to digitally identify our messages as coming from our authorized senders. In addition we utilize a Sender Policy Framework (SPF) record which lists our authorized senders. Both of these are done to reduce the possibility of phishing attacks and spam from others using NSSE addresses and both increase deliverability of email.

During administration, we monitor response, message opening, and bounce rates for potential problems, and contact these companies if one is detected.

Preparing for Message Delivery

Campuses using Google

If your institution uses G Suite / Google for email please review the following support documentation from Google and have your campus G Suite administrator add the NSSE email server IP addresses listed above to the whitelist.

- [G Suite – Email whitelists and blacklists](#)
- [G Suite – Whitelist IP addresses in Gmail](#)

Campuses using MS Live

NSSE participates in the Junk Email Reporting Program and Sender ID services offered by Microsoft (listed at <http://mail.live.com/mail/services.aspx>). We are not eligible for participation in the Return Path Sender Score Certified Email service, however, because NSSE does not meet the criteria required by Microsoft. MS recommends the following procedures for helping NSSE emails be delivered at campuses using MS live: The mail administrator can go into PowerShell and create a transport rule to give our servers, 129.79.1.58 and 134.68.220.35, a spam confidence level of 3 or less.

Phishing

By default the “from” name matches the “from” email address in NSSE recruitment messages (see above). Historically, institutions were encouraged to customize the “from” name to reflect the message signatory (e.g., campus President or Provost) and to further personalize the message. In recent years, however, a growing number of institutions have implemented anti-phishing campaigns on campus to protect from predatory emails. Mismatched from names and email addresses are a common trait of phishing campaigns. Although institutions can still customize the “from” name, NSSE recommends against doing so as a matter of best practice.

Working with Campus Proxy Servers

To maintain our security standards for the survey, we check to see if a reported IP address changes during a survey session. If so, we then rely on the cookies used during the session. We aren't able to administer the survey if both a proxy server is used and cookies are not enabled. We recommend that institutions using proxy servers make an exception for the NSSE web survey address so that a consistent IP address is reported. Our survey support staff can work with individual students on temporarily adjusting their browser to enable cookies, but we would prefer to preempt the problem if at all possible.