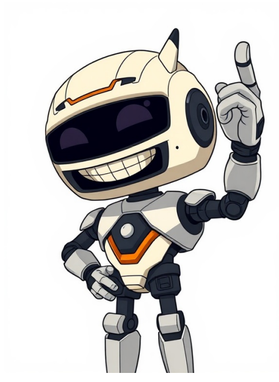
I'm not a robot



Outlook.com's Smart Network Data Services (SNDS) initiative empowers IP owners to contribute to the fight against spam, malware, and other internet evils, protecting email and the internet as a vital communications tool. By collecting and analyzing email activity data, Outlook.com provides service providers with valuable insights to react and take repair actions, preventing spam from originating within their IP space. SNDS is designed to make the Internet a better, safer place for everyone involved. SNDS Data Access: A Step-by-Step Guide Accessing and Revoking IP Access in SNDS ###ENDARTICLEDuring the activity period, users with Hotmail or Windows Live accounts can report nearly all messages as spam via the web interface. The formula, which is "# of complaints" divided by "message recipients" as outlined earlier, helps determine the complaint rate. If this rate exceeds 100%, note that SNDS records complaints on the day they are reported, not retroactively. For context, over 30% of IPs sending mail to Outlook.com maintain a complaint rate below 0.3%, a benchmark worth aiming for. To access the actual messages users reported for your IP space, refer to the Junk Mail Reporting Partner Program details on the Postmaster website. The trap message period mirrors the activity period, but instead of summary stats, it tracks exact times of messages sent to trap accounts, precise to the minute. This is especially helpful for IPs dynamically allocated to different customers, as it provides two specific timestamps to link activity to one or two IP owners. Trap hits show how many messages were sent to "trap accounts," which are Outlook.com accounts that receive no unsolicited mail. Thus, messages to these accounts are likely spam. Responsible senders rarely hit such accounts because they target valid recipients and handle NDRs. Spammers struggle to avoid them as they often neglect these practices. While sharing trap messages could aid legitimate businesses in list cleaning, the risk of spammers exploiting this data is too high. Sample messages are provided for troubleshooting and evidence, including both user junk reports and trap hits. SNDS offers one sample per IP daily for each type. To view these, click the data for the relevant day. For more complaint messages, consider joining the Junk Mail Reporting Partner Program. The sample HELO command displays an actual HELO or EHLO command sent by the IP. This command, part of the SMTP protocol, advertises the sender's identity. Spammers often hide their identity, so if this matches a customer's ID, combined with other data, it can indicate the IP isn't spamming. Similarly, the sample MAIL command shows the actual MAIL command sent, which signals the start of a message and specifies where DSNs (Non-Delivery Reports) should go. Comments provide additional IP data, such as JMR P1 Sender, JMR Block, or JMRP Spam complaint counts. The JMR P1 Sender field links complaints to the offending IP and the P1 Sender. JMR Block notes IPs blocked due to abuse complaints. JMRP subscribers can use this to identify emails marked as junk. If not enrolled, follow the steps to sign up. JMRP Spam complaint counts track spam-related complaints per IP and day, with UTC times marking the end of the report period. Shared IP users see all spam complaints regardless of the sending domain. Outlook.com scans emails for viruses, logging IPs that upload virus payloads. An IP uploading viruses will have a comment noting "1 virus(es) detected" with the timestamp. To resolve, install virus scanners or Windows Live OneCare. Microsoft also monitors websites for malware, identifying sites that exploit browser vulnerabilities to install programs on users' computers. This automated system uses proprietary software to test browsers like Internet Explorer. SNDS (Security Network Detection System) identifies web sites with browser vulnerabilities, providing IP addresses of computer systems hosting exploit code and DNS servers responsible for resolving websites to those IPs. To access the data, click the .CSV button located at the bottom of the data pages. Make sure both cookies and JavaScript are enabled, as they're necessary for the site's proper functioning. An alternative method for accessing the data is designed for automated systems to consume it, offering a simple data access URL that doesn't require Windows Live ID authentication. This feature can be optionally enabled on this page, which includes example URLs used to download the data once activated. The data provided through this mechanism is identical to the .CSV data obtained when using the Export to .CSV button on the main data page.