

July 25, 2024

CYBER SECURITY AWARENESS – PROTECT FROM SPAM E-MAILS

As you know, spam emails are a constant presence in our inboxes. While most get filtered out, some can slip through. These emails can be a nuisance but they can also be dangerous attempts to steal your personal information or infect your devices with malware.

To help keep us all safe online, here is a quick reminder on how to identify and handle spam emails:

RED FLAGS OF SPAM:

- ✓ **Suspicious Sender:** Beware of emails from unknown senders or addresses with misspellings or unusual formatting (e.g., Office of The Commissioner of Police police.cbe-in.gov84@vigoire.de).
- ✓ **Urgent or Threatening Language:** Scammers often use urgency or fear tactics to pressure you into clicking on links or opening attachments.
- ✓ **Unbelievable Offers:** Promises of "get rich quick" schemes or free gifts are usually too good to be true.
- ✓ **Poor Grammar and Spelling:** Legitimate companies typically have good email formatting and avoid grammatical errors.

WHAT TO DO WITH SPAM:

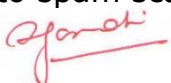
- ✓ **Don't Click on Links or Attachments:** These are common entry points for malware.
- ✓ **Don't Reply:** Engaging with spam can confirm your email address as active and lead to more spam.
- ✓ **Mark as Spam:** Select the suspicious email and "Report as Spam." This helps our email provider improve its filtering and protects others.

FOR EXTRA PROTECTION:

- ✓ **Beware of Phishing** (Phishing is a process of stealing confidential information by various types Lures, Spoofing, Masquerading): Spam emails can be used for phishing attacks. Never be lured or give out personal information or login credentials.
- ✓ **Use Strong Passwords:** Ensure your email account is protected with a strong, unique password, and enable Two-Factor Authentication(2FA) if you are in a possession of responsibility handling sensitive and confidential information of the institutions. Your school IT Administrator is trained to help you enable 2FA.

If you are ever unsure about an email's legitimacy, it is always best to err on the side of caution.

By following these tips, we can all help keep school data secure and avoid falling victim to spam scams.



PRINCIPAL



BAL BHARATI PUBLIC SCHOOL DWARKA

SCHOOL CYBER POLICY ON SPAM E-MAIL

JULY 2024



At BBPS Dwarka, we are committed to maintaining a safe and secure digital environment for all our stakeholders, including students, parents, teachers, and staff. This policy outlines the procedures and best practices for handling spam emails to protect our community from potential threats such as phishing, malware, and identity theft.

"Spam emails are the weeds in our digital garden; it's up to us to keep them from taking over."



What are Spam Emails?

Spam emails are unsolicited messages sent in bulk, often containing irrelevant or inappropriate content. These emails may also include malicious links, attachments, or fraudulent requests for personal information.

How can we identifying Spam Emails?

Spam emails often exhibit the following characteristics:

1. Every spam email is a potential threat. Stay vigilant and protect your digital identity.
 2. A well-informed community is the strongest shield against the dangers of spam emails.
 3. Protecting ourselves from it is essential for our digital well-being.
- Unfamiliar sender addresses.
 - Suspicious or misleading subject lines.
 - Requests for personal, financial, or login information.
 - Spelling and grammatical errors.
 - Unsolicited attachments or links.
 - Urgent or threatening language.



How to report a Spam Emails?

If you receive a suspicious email, follow these steps:

- 1. Do not open any attachments** or click on any links within the email.
- 2. Don't Reply:** Engaging with spam can confirm your email address as active and lead to more spam.
- 3. Mark as Spam:** Select the suspicious email and "Report as Spam." This helps our email provider improve its filtering and protects others.



What are the preventive measures for safe guarding from spam?

To minimize the risk of spam emails, adhere to the following guidelines:

- **Be Cautious with Email Addresses:** Avoid sharing your email address publicly or with untrusted sources.
- **Regularly Update Software:** Ensure your email client and antivirus software are up to date.
- **Educate Yourself:** Stay informed about common email scams and phishing tactics.
- **Use Strong Passwords:** Create complex passwords and change them regularly.
- **Enable Two-Factor Authentication:** Add an extra layer of security to your accounts.

Response to Spam email

In the event of a spam incident:

- **Immediate Action:** Inform the IT department immediately to take action and mitigate the threat.
- **Notification:** Affected individuals shall be notified promptly with instructions on how to secure their accounts.
- **Investigation:** A thorough investigation shall be conducted to determine the source and extent of the incident.
- **Reporting:** Relevant authorities (such as Cyber Cell) shall be informed if necessary.

By following this policy and staying vigilant, we can collectively protect our digital environment from the threats posed by spam emails.

Thank you for your cooperation and commitment to maintaining a secure institution.

IT Team
Bal Bharati Public School Dwarka