

The image displays three sequential screenshots of a web application used for checking if email addresses have been compromised in data breaches. Each screenshot features a blue header bar with a white input field and a dark blue button labeled 'pwned?'. Below the input field is a green section with white text.

First Screenshot:
Input: raytos.r.bsinfotech@gmail.com
Result: Good news — no pwnage found!
Subtext: No breached accounts and no pastes (subscribe to search sensitive breaches)

Second Screenshot:
Input: rlyryts02@yahoo.com
Result: Good news — no pwnage found!
Subtext: No breached accounts and no pastes (subscribe to search sensitive breaches)

Third Screenshot:
Input: rytsrly02@gmail.com
Result: Good news — no pwnage found!
Subtext: No breached accounts and no pastes (subscribe to search sensitive breaches)

5. I do not reuse passwords across different services because doing so significantly increases the risk of account compromise. If one account is breached, all others using the same password become vulnerable.

I use two-factor authentication (2FA) for important accounts to add an extra layer of security, ensuring that even if my password is compromised, unauthorized access is still prevented without the second factor.

6. Immediately change your password to a strong, unique one that you haven't used before. Avoid reusing passwords from other accounts to minimize risk. Review other accounts linked to your email for any suspicious activity. Change passwords and enable 2FA on those accounts as well, making it harder for unauthorized users to access your account even if they have your password.