10 Essential 'Be Safe' Email Checklist

everyday identity

1. Use Strong, Unique Passwords ☐

Ensure your email account has a robust, unique password to prevent unauthorized access.

2. Enable Two-Factor Authentication (2FA) ☐

Add an extra layer of security by requiring a second form of verification when logging in.

3. Be Cautious with Attachments and Links (ZTH) ☐

Avoid opening unexpected attachments or clicking on suspicious links to prevent malware infections. This ideology is known as Zero Trust Human, never click link instead go to website directly.

4. Verify Sender Authenticity ☐

Confirm the legitimacy of email senders, especially when requests involve sensitive information or urgent actions.

5. Regularly Update Security Software ☐

Keep your antivirus and anti-malware tools up to date to detect and block threats effectively.

6. Use Encrypted Connections (SSL/TLS) ☐

Ensure your email service uses encryption protocols to protect data during transmission.

7. Be Wary of Phishing Attempts ☐

Stay alert to emails that attempt to trick you into revealing personal information or login credentials.

8. Regularly Review Account Activity ☐

Monitor your email account for unauthorized access or unusual activity.

9. Educate Yourself on Email Scams ☐

Stay informed about common email scams and tactics used by cybercriminals.

10. Use Spam Filters ☐

Activate and customize spam filters to reduce unwanted and potentially harmful emails.