Ans: Various types of prevent technique for email attracts.

1. PGP:

* It is integrity, authenticity and confidentiality encryption method using cryptographic.
* This system is using a public encryption key method. It uses a pair key they are public key using for encryption and private key using decryption.
* Sender sent an email using a privet key while receiver use a privet key for public key.
* PGP also give a digitally sign which is give more squares.

2. S/MIME :

* It is integrity, confidentiality and authenticity encryption method for cryptographic for email messaging.
* It gives trusted authorities certificate and identify both recipients and senders.
* It is similar to PGP cryptography.
* It gives an own certificate authority for digital integrity .

3. Email Authentication:

* SPF verify the incoming message form the sender and check the authorized server.
* DKIM verify the authentication of this mail sender and detract it.
* It’s authentication system is domain base system and handle authentication

4. Email Encryption:

* It is a common technique PGP encryption technique. it is use private and public key. For message encryption and decryption.
* Secure system for email transduction because of it is end to end encryption method.

5. Anti-Spam Filters:

* Bayesian filters: For this technique using algorithm and pattern for detect spam message
* Content based filters: Analyze the content of including text, attachments, email, metadata, identify spam messages.

6. Malware Protection :

* Anti Malware Software: for this technique use anti malware software.
* Sandboxing: It gives a secure environment . it allow the human environment to prevent spam message.

7. User Awareness and Training:

* This technique is use awareness which is Phishing and which is not.
* Social Awareness this method is training the user to protect this attects.

8. Email Filtering and Whitelisting:

* This technique is use for set up a machine for filtering spam email.
* Email will trusted are detected otherwise give it spam box

9. Two-Factor Authentication :

* This use for two factor one is mobile device and another is password.
* When anyone try to break the password mobile device sent a otp.

10. Incident Response and Monitoring:

* Mentoring the system for sending minimum number of email sending.
* When any email sends continuously then it can became block.

11. Regular Software Updates and Patch Management:

* Client software, server and ensure security up-to-date every day.

12. Email Backup and Recovery:

* It is a technique when any email loss then recovers from where he stores it.
* This is a most secure because one lost he became fine aging.

- Regularly backing up emails ensures that in the event of an attack or data loss, emails can be restored, minimizing the impact and ensuring continuity of communication.

Conclusion:

All of the technique is use for prevent email attracts.