

Phishing

Six Protective Measures Against Phishing



Six Steps to Shield Your Business from Phishing Attacks

1. Email Safety

- Set up advanced spam filters and email monitoring
- Flag external emails and unknown senders
- Implement domain-based message authentication (DMARC, DKIM, SPF)

2. Employee Training

- Run quarterly phishing simulations
- Educate staff on social engineering tactics like urgency and authority
- Make security awareness part of onboarding and regular meetings

3. Access Controls

- Use the principle of least privilege (PoLP)
- Regularly audit access rights and remove unused accounts
- Apply role-based access permissions and network segmentation

4. Incident Response Plan

- Have a documented and practiced response plan
- Include a clear reporting structure and recovery timeline
- Assign roles for internal response, communication, and legal obligations

5. Multi-Factor Authentication (MFA)

- Require MFA for all remote access and critical systems
- Use app-based MFA over SMS where possible
- Regularly test and update MFA configurations

6. Security Reviews

- Conduct regular audits of systems and policies
- Keep software and security tools up to date
- Include physical security and password hygiene checks

Bonus Tip

Encourage a culture of “Stop and Think.” If something seems odd, employees should feel safe to question and report it—without fear of blame.

Ready to build a stronger human firewall? Schedule a [free consultation](#) with our cyber security team and take the next step toward protecting your people and your business.