

Social Engineering

Prevent

Tips To Prevent Social Engineering Attacks

◆ | Cyber Press

1. Policy and Procedure Development

Establish clear, enforceable policies and processes for data protection as well as for handling messages or actions that seem suspicious. Strict guidelines for disclosing sensitive information should be part of these regulations.

2. Email Filtering System

Advanced email filtering can aid in the identification and quarantining of suspected phishing emails, preventing their delivery to end users and lowering the danger of a social engineering assault. To protect yourself from new risks, regularly update your email filters.

3. Software and System Updates

Update your systems and software frequently. Patches for known security flaws are frequently included in software updates, which social engineers might use against you.

4. Education and Awareness

Create a culture of cybersecurity to begin with. Train your staff frequently on how to recognise potential social engineering techniques, such as phishing emails or ominous calls and texts. For improved comprehension and retention, incorporate real-world examples into your instruction. Teach staff members to stay away from exchanging critical information and to never click on links or attachments coming from untrusted sources.

5. Multi-factor Authentication (MFA)

Across your organisation, deploy MFA to strengthen your digital defences. Users of this system must give two or more verification factors, such as a passcode, a physical token, or a fingerprint, in order to access a resource. This method makes it much more difficult for social engineers to access accounts without authorization.

6. Data Encryption

Always encrypt sensitive data, whether it's being sent or being housed on corporate systems. Without the decryption key, encrypted material is useless to social engineers.

7. Implement the Principle of Least Privilege

Update your systems and software frequently. Patches for known security flaws are frequently included in software updates, which social engineers might use against you.

8. Encourage Secure Browsing Practices

Make sure your staff is aware that not all websites are secure and that some may even have been created by hackers to conduct phishing attacks. Encourage people to only access or submit sensitive information through secure, reputable websites.

From:
<https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link:
https://wiki.fortier-family.com/cybersecurity/social_engineering

Last update: 2026/09/20 14:15



