SHAUN CONWAY *Director of Business Development, D2NA*
https://www.linkedin.com/in/shaunconway14/
www.d2na.com

Shaun has nearly fifteen years in the IT infrastructure and cyber security sector. After starting his career as a service desk engineer and progressing through several roles, Shaun now works as Director of Business Development at D2NA, a UK based Cyber Security firm that service organisations across all sizes and sectors

TIP 1. EMPLOYEE TRAINING AND AWARENESS

Educate employees about common cyber threats such as phishing, social engineering, and malware. Regular training sessions can help employees recognise and avoid potential risks. Employees can be the weakest link in the security chain, so even a little knowledge can go a long way.

TIP 2. TURN ON MULTI-FACTOR AUTHENTICATION

Implementing multi-factor authentication (MFA) for added security. If a password is compromised, enabling MFA means those credentials are useless to a potential hacker. This is such an easy step to take and can have a huge impact on securing accounts. Most online services now have the facility to turn on MFA so there is no excuse!

TIP 3. REGULAR SOFTWARE UPDATES AND PATCH MANAGEMENT

Ensure that all software, including operating systems and applications, are regularly updated with the latest security patches to address known vulnerabilities. New vulnerabilities are discovered every day and delaying updates can stop those from being patched and allow attackers an open door in.

TIP 4. FIREWALLS

Configure firewalls to restrict unauthorised access to the organisation's network and systems. Implement both network-level and host-based firewalls for comprehensive protection. Understanding the requirement for each firewall and its role in the wider network is crucial.

TIP 5. DATA ENCRYPTION

Encrypt sensitive data both in transit and at rest to protect it from unauthorised access. Use encryption protocols such as SSL/TLS for web traffic and BitLocker or FileVault for data storage If data does fall into the wrong hands, you know it will be protected with encryption and be unreadable.

TIP 6. ACCESS CONTROL

Limit access to sensitive information and systems based on the principle of least privilege. Regularly review and update user permissions to ensure that only authorised members of staff have access to necessary resources.

TIP 7. SUPPLIER RISK MANAGEMENT

Assess the cybersecurity posture of third-party vendors and partners who have access to your organisation's systems or data. Ensure that they meet your security standards and compliance requirements.

TIP 8. SECURITY POLICIES AND PROCEDURES

Develop comprehensive cybersecurity policies and procedures tailored to your organisation's specific needs and regulatory requirements. Regularly review and update these documents to reflect changes in technology and threats.

TIP 9. SECURITY MONITORING AND INCIDENT RESPONSE

Deploy intrusion detection systems (IDS) and security information and event management (SIEM) solutions to monitor for suspicious activities and respond promptly to security incidents. Our SOC service is a prime example of this.

TIP 10. REGULAR DATA BACKUPS

Implement a regular backup strategy to ensure that critical data can be restored in the event of a ransomware attack, hardware failure, or other data loss incidents. Although not strictly a cyber security improvement, having a good backup strategy will get you back online as soon as possible and is always good practice.