NEA Cybersecurity Awareness Month

Cybersecurity Awareness Month, observed every October, is a critical initiative for the Nepal Electricity Authority (NEA) as it underscores the importance of safeguarding our digital infrastructure. This month-long campaign, endorsed globally and locally, aims to educate and empower all NEA employees to adopt robust cybersecurity practices. Given the increasing reliance on digital systems for efficient energy management, it is imperative for us to stay vigilant against cyber threats. Throughout this month, we will engage in various activities and training sessions designed to enhance our understanding of cybersecurity risks and the measures we can take to mitigate them. By fostering a culture of security awareness, we ensure the resilience and reliability of our power systems, ultimately protecting our nation's critical infrastructure.

Ten practical actions users should take to enhance their cybersecurity awareness and protect themselves online

1. **Use Strong, Unique Passwords**: Create complex passwords using a mix of letters, numbers, and special characters, and avoid reusing passwords across different accounts.
2. **Enable Multi-Factor Authentication (MFA)**: Add an extra layer of security to your accounts by enabling MFA, which requires a second form of verification beyond just a password.
3. **Be Wary of Phishing Scams**: Be cautious of unsolicited emails, messages, or links, especially those asking for personal information. Verify the sender's authenticity before responding or clicking on links.
4. **Keep Software Updated**: Regularly update your operating system, software, and applications to patch vulnerabilities and protect against malware.
5. **Secure Your Wi-Fi Network**: Use strong passwords for your home and office Wi-Fi networks to prevent unauthorized access.
6. **Back Up Your Data**: Regularly back up important files to an external hard drive or a cloud service to ensure data recovery in case of a cyber-attack or hardware failure.
7. **Use Antivirus and Anti-Malware Software**: Install and maintain reputable antivirus and anti-malware software to detect and prevent threats.

8. **Practice Safe Browsing**: Avoid visiting suspicious websites and downloading files from untrusted sources. Use secure, HTTPS-encrypted websites whenever possible.
9. **Monitor Your Accounts Regularly**: Frequently check your financial and online accounts for any unauthorized transactions or changes and report any suspicious activity immediately.
10. **Educate Yourself Continuously**: Stay informed about the latest cybersecurity threats and best practices by participating in training sessions, reading articles, and following cybersecurity news.

IT Department
Nepal Electricity Authority