

Best Practices

Title of the Practice: Muthamzh Vizha

Objectives

- To introduce students to the cultural values
- To make students understand the values of traditional culture of Tamilnadu

The Context

Increased level of diversity that happens in the society mainly propelled by globalisation and work culture the youth of India tend to forget the golden value of *Iyal*, *Isai* and *Nadagam* (prose, music and drama) which were highly useful in educating the mass. Since it is feared that the Indian youth may not grow up with values, the present programme *Muthamzh Vizha* is organised.

The Practice

The programme broadly includes conducting competition on themes mostly related to Tamil Literature. Competitions like Elocution song; drawing and debate are organised in connection with important festivals like *navarathiri vizha* and *pongal* festivals. Judges, mostly staff of the college, are appointed to identify the talented students.

Evidence of Success

There has been an overwhelming response to the programme. Students in large number participate in events organised through this forum. There has been a marked growth in skills in various fields among students who participate in the various events. In addition to this, they are able to learn the traditions of Tamil Literature as well as how the ancestors developed their skills in various forms of art.

Problems Encountered and Resources Required

Being programmes that have in built rewards- both spiritual and physical- students do not hesitate to participate. Since prize-money is extended by the college, financial crunch is not felt.

Title of the practice: Cysafe

Objectives of practice

Cysafe contest is the practice of creating awareness about the security and protection of data and information's from the digital attacks in the world around us. Cyber risk poses an alarming threat to sources of enterprise capability. The main aim of the cyber security is to achieve Confidentiality, Integrity and Availability. **Confidentiality** involves a set of rules or a promise usually executed through **confidentiality** agreements that limits access or places restrictions on certain types of data. It is respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action. It is to create a culture of cyber security that promotes safe and appropriate use of cyberspace and to cultivate national cyber security capabilities.

Context

In today's dynamic environment, cyber security has become vital for individuals and families, as well as organizations (such as military, government, business houses, educational and financial institutions, corporations and others) that collect and store a wide range of confidential data on computers and transmit that to other computers across different networks. For families, protection of children and family members from cyber crime has become substantially important. For an individual, protecting information that could impact social life as well as personal finance is essential. The internet has provided a wide array of learning opportunities, but there are risks too. Photos, videos and other personal information shared by an individual on social networking sites such as Face book, Twitter can be inappropriately used by others may lead to serious and even life-threatening incidents. Social networking sites have become the most popular medium for sharing information and connecting with other people. But these sites have created varied opportunities for cyber crimes, compromised personal identities and information leakage. Therefore, it is important for individuals to understand how to protect against cyber threats, and must also comprehend the difference between virtual and real world. One should learn how to protect computers and personal information from being hacked and should engage in appropriate online behavior in order to eliminate changes of cyber threats and thereby creating a safer online environment.

The practice

In our daily life, we probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. It's important to exercise the same caution at work. Keep in mind that cybercriminals can create email addresses and websites that look legitimate. Scammers can fake caller ID information. Hackers can even take over company social media accounts and

send seemingly legitimate messages. Phishers prey on employees in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize. With just one click, you could enable hackers to infiltrate your organization's computer network. A strong password contains at least 10 characters and includes numbers, symbols, and capital and lowercase letters. Companies also should ask you to change your passwords on a regular basis. Changing and remembering all of your passwords may be challenging. A password manager can help. Office Wi-Fi networks should be secure, encrypted, and hidden. If you're working remotely, you can help protect data by using a virtual private network, if your company has one. A VPN is essential when doing work outside of the office or on a business trip. Public Wi-Fi networks can be risky and make your data vulnerable to being intercepted. Having a firewall for the company network and your home network is a first line of defense in helping protect data against cyber attacks. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web. Smaller businesses might hesitate when considering the cost of investing in a quality security system. That usually includes protections such as strong antivirus and malware detection, external hard drives that back up data, and running regular system checks. But making that investment early could save companies and employees from the possible financial and legal costs of being breached. Cyber threats often take aim at your data. That's why it's a best practice to secure and back up files in case of a malware attack. Your company will probably have rules about how and where to back up data. Important files might be stored offline, on an external hard, drive, or in the cloud. Companies and their employees may also have to monitor third parties, such as consultants or former employees, who have temporary access to the organization's computer network. It's important to restrict third-party access to certain areas and remember to deactivate access when they finish the job.

Evidence of success

The right cyber security technology can prevent a vast majority of attacks, detect vulnerabilities quickly, mitigate cyber security risks, and enable security of strategic business initiatives like digital transformation. If done right, these business outcomes can be achieved without impeding the speed of delivery. But security threats are dynamic, fast moving, and can be highly unpredictable for legacy and manual approaches to keep up with. With an increasingly machine-based adversary, cyber security approaches that are manual, highly fragmented, and point-product-based are doomed to fail. In the digital world, success requires organizational speed and agility—more than ever before, in fact. Every organization wants, and needs, to move faster and become nimbler in spotting and taking advantage of new business opportunities. Technology plays a key role in making that goal attainable, as many of us learned over the past few decades. Fortunately, new solutions such as cloud computing, Software as a Service, and anywhere/anytime connectivity are changing the technology paradigm, delivering breakthrough capabilities faster, less expensively, and with a smaller technology footprint. Additionally,

software-based automation has laid to waste the traditional approaches of problem solving, and are significantly reducing the need for massive security operations centers (SOCs).