TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

AWARENESS KEY TO PROTECTION AGAINST CYBER ATTACKS

#CyberSecurityAwarenessMonth

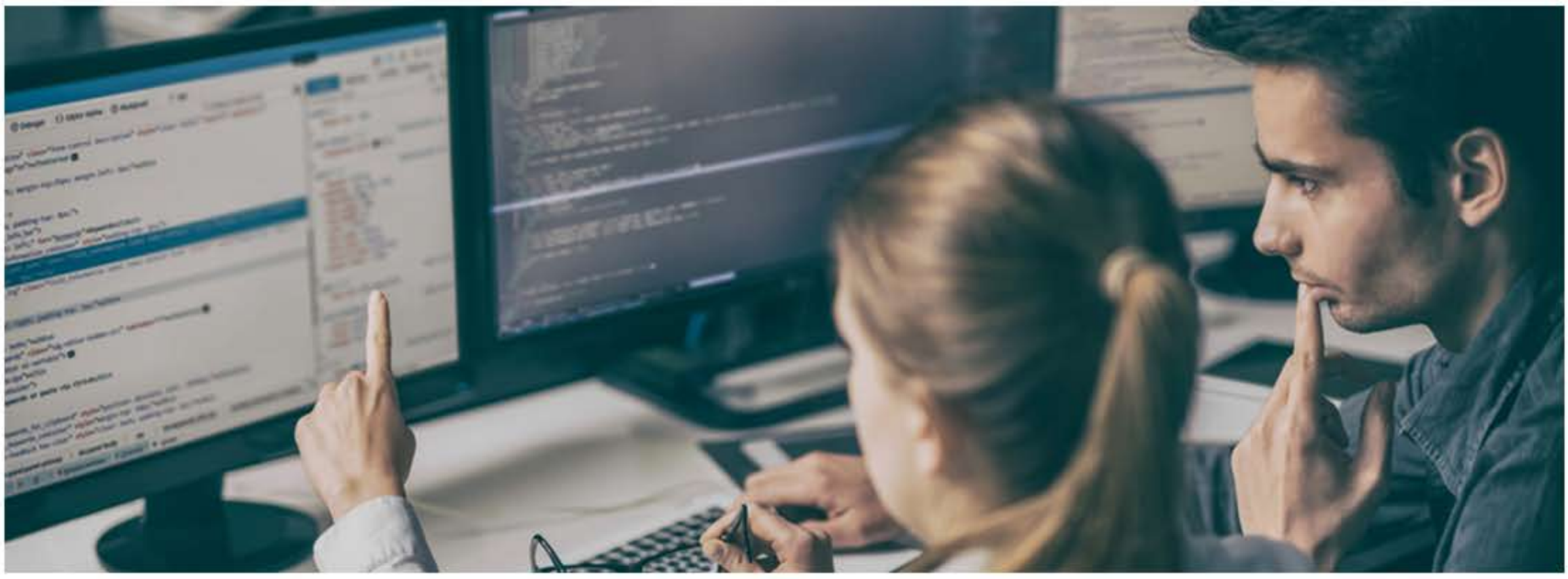
TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Are you aware that 99% of cyber-attacks require human interaction?

Nearly, all cybersecurity incidents start with the exploitation of the human tendency to make errors. Phishing and Social Engineering are the most common methods used by cybercriminals to lure victims and gain a foothold in the targeted system, network or infrastructure. As per the Phishing Activity Trends Report 2020, around 146,994 phishing sites were detected in the Q2 of the current year. This study is quite sufficient to explain the ever-evolving nature and techniques of cybercrimes. A people-centric cybersecurity approach encompassing effective Security Awareness Training is the need of the hour to overturn the growing spike of such cyber-attacks and make organizations more resilient than ever before.

IMPORTANCE OF CYBERSECURITY AWARENESS PROGRAM FOR BUSINESSES



While being an important asset for an organization, humans are one of the most vulnerable resources as well. Threat actors target people, rather than systems because of the low levels of security awareness among them. As per the Cyber Risk Survey 2019, less than one-third (31%) of employees receive annual, companywide training from their organizations. Lack of knowledge and awareness concerning cybersecurity among the workforce could result in a major breach or cyber-attack. Cybersecurity Ventures has also predicted that the cost of cybercrimes will exceed $6 trillion annually by 2021. So, the best way to contain the cost and strengthen the defence is to create awareness among employees.

Cybersecurity awareness training helps organizations to inform their employees about how to maintain good cyber hygiene. This may include (but not limited to) propagating knowledge regarding the evolving cyber threat landscape, best practices to identify potential threats like malware and phishing emails, and adherence to applicable compliance and data protection regulations.

Creating such a culture reduces the possibility of a successful cybersecurity incident to a great extent. Also, it helps employees to understand the potential impact that a cyber-attack can make on the organization.

Recommendations for organizations to increase cybersecurity:

- Perform a thorough audit and identify your valuable assets, which may include critical data like PII, financial information, intellectual property, etc. Figure out who has access to them and what functions they can perform.
- Focus on high-risk users with escalated privileges. For example, CISO, CIO, CFO and CEO as they have access to high-value data.
- Review the efficacy of existing security solutions and identify areas of weakness.
- Automate repetitive tasks to reduce manual efforts, which minimizes the chances of errors.
- Implement a data recovery strategy to back up data in case of a successful security incident.
- Establish an incident response plan to take appropriate actions when security is breached.
- Disseminate strong password policy to all the employees.

BENEFITS OF IMPLEMENTING SECURITY AWARENESS TRAINING

Security awareness training is one of the most preferred methods to tackle the growing concern of cyber-attacks. It yields multiple advantages for an organization, including:

- Reduces the percentage of human errors & minimizes the likelihood of data breaches and cyber-attacks
- Encourages employees' to work in a security-focused atmosphere
- Improves brand reputation and trustworthiness among clients and partners
- Prevents downtime, which badly affects an organization's workflow and targets
- Demonstrates compliance with industry regulations

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

HOW INDIVIDUAL USERS CAN ENSURE CYBER SAFETY?

Some useful security practices recommended for users to remain guarded against malicious activities include:

- Keep systems and applications up-to-date as updates are designed to patch the existing vulnerabilities.
- Pay sufficient attention while accessing emails from unidentified sources. Look for red flags and do not click on suspicious URLs, as well as download attachments from such emails.
- Avoid using identical passwords for different applications.
- Implement multi-factor authentication as it adds an additional layer of protection.
- Always enable firewall protection to protect the network against incoming malicious web traffic.
- Avoid using public wi-fi for internet banking, accessing corporate data, sending critical information, etc.
- Always prepare a backup of your data at regular intervals to avoid data loss in case of a cyber-attack.

Remember, ensuring cybersecurity is not a one-time process. It is a continual activity that must be maintained and followed by each individual associated with the organization. Cyber awareness helps people to take accurate decisions while confronting an adverse situation, which ultimately strengthens the cyber defence of the company. Always engage yourself in safe online behaviour by implementing recommended security practices.