SNGIST
GROUP OF INSTITUTIONS
An ISO 9001-2008 certified institution | Approved by AICTE

WAVES

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Vol 1 Issue 10 December 2021

CHRISTMAS CELEBRATION

A Christmas celebration was held on 23rd December 2021. The day was specially organized keeping in mind its sanctity and relevance. The students presented an impressive array of programs. Students added gaiety and were vibrantly dressed for the theme. The program included competitions like Crib, Christmas tree, Santa, Carol song, Christmas card, Star making and different kind of games which are conducted by various departments of SNGIST. Everyone got drowned in the happy festive vibes. The Christmas celebration became a big hit.

STUDENT'S CORNER

CYBER SECURITY

Sherin Sunny
S7 ECE

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing. The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year.

A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cyber criminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks. With the scale of the cyber threat set to continue to rise,the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices. In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources. The importance of system monitoring is echoed in the "10 steps to cyber security", guidance provided by the U.K. government's National Cyber Security Centre. In Australia, the Australian Cyber Security Centre (ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device. So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft. In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record(MBR) and are designed to encrypt or wipe data from computer's hard drive. Electronic security protocols also focus on real-time malware detection. Many uses heuristic and behavioural analysis to monitor the behaviour of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyse their behaviour and learn how to better detect new infections. Security programs continue to evolve new defences as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

Editorial Board: Ms. Nivya K Venu, Assistant Professor, ECE