SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with ‘A’ Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

19IT602 CRYPTOGRAPHY AND CYBER SECURITY
III Year / VI Semester

Cyber Security Vulnerabilities

Cyber Security Vulnerabilities

- Companies collect and store enormous amounts of data. From billing invoices to customers' credit card information, so much of your business focuses on private data.
- To succeed, you have to trust employees with this data.
- But, sometimes, even the most well-intentioned employee can make mistakes that leave your company vulnerable to cyberattacks.

1. Opening Emails from Unknown People

- Email is the preferred form of business communication.
- The average person receives 235 emails every single day, according to The Radicati Group.
- With that many emails, it stands to reason that some are scams
- Advise employees not to open emails from people they don't know.
- Advise employees to never open unknown attachments or links

2. Having Weak Login Credentials

- Cybercriminals have programs that mine public profiles for potential password combinations and plug in possibilities until one hits.
- Require employees to use unique passwords
- Add numbers and symbols to a password for increased security. For example, change "Seattle" to "S3att!e."
- Create rules that require employees to create unique, complex passwords of at least 12 characters; and change them if they ever have reason to believe that they have been compromised.

3. Leaving Passwords on Sticky Notes

- Have you ever wandered through the office and spotted a sticky note on a screen with passwords written on it? It happens more often than you think.
- While you want a certain level of trust inside your organization, leaving passwords visible is too trusting.
- If employees must write down passwords, ask that the paper copies are kept inside locked drawers.

4. Having Access to Everything

- In some cases, companies don't compartmentalize data.
- In other words, everyone from interns to board members can access the same company files.
- Set up tiered levels of access, giving permission only to those who need it on each level.
- Limit the number of people who can change system configurations.
- Don’t provide employees with admin privileges to their devices unless they really require such set up.
- Even employees with the admin rights should only use them as needed, not routinely.

5. Not Updating Antivirus Software

- Your company should deploy antivirus software as a protective measure, but it shouldn't be up to employees to update it.
- At some companies, employees are prompted to make updates and can decide whether or not the updates take place.
- Antivirus updates are important, should be handled promptly and shouldn't be left to employees.
- Set up all system updates to take place after work hours automatically.
- Don't let any employee, no matter what their title, opt out of this company policy.