



A.V.C College of Engineering

Approved by AICTE, New Delhi | Affiliated to AnnaUniversity, Chennai
| Grade 'B' Accreditation by NAAC with CGPA of 2.73/4.00 |
An ISO 9001:2008 Certified Institution



Mannampandal, Mayiladuthurai-609305

=====
==
**Department of Computer Science and Engineering
&
CSI Student Branch
Webinar on ' Cyber Security'**

Webinar on 'Cyber Security' by Mr. Mohammed Hassan Ali Tabrez, Senior Manager, Pre-Sales at Securemetric TehnologySdnBhd, Malaysia	Cyber Security	May 8, 2020 at 3.30 PM	72 Students (I, II, III and IV CSE Students + 10 IT Students)
--	----------------	------------------------	---

A.V.C. COLLEGE OF ENGINEERING
 | Approved by AICTE | Affiliated to Anna University |
 | Re-Accredited by NAAC with 'B++' Grade [2nd Cycle] |
 | An ISO 9001:2015 Certified Institution |
 Mannampandal, Mayiladuthurai - 609305.

Department of Computer Science and Engineering & CSI Student Branch
 Presents
WEBINAR on "Cyber Security"

Speaker: Mr. Mohammed Hassan Ali Tabrez
 Senior Manager, Pre-Sales at Securemetric TehnologySdnBhd, Malaysia.

Date: 10th-May-2020
Time: 10:00 a.m

20 Ways to Block Mobile Attacks

Don't let your mobile phone become your only mobile device. Be just as careful as you would on a desktop!

WiFi

Don't allow your device to auto-join unknown networks.
Always turn off WiFi when you aren't using it or don't need it.
Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

Only use apps available in your device's official app store (Google Play or the App Store).
Be wary of apps that ask for excessive permissions.
Only share sensitive information with the app's developer.
Update apps regularly to address any known security issues.

Security

Make sure you're always protected with secure and up-to-date encryption.
Use a secure VPN when connecting to public networks.
Change your PIN or password regularly.
Use a secure email provider when sending sensitive information.



Bluetooth

Disable unknown Bluetooth pairing requests.
Always turn it off when you don't need it.

Smishing (phishing via SMS)

Don't open messages that attempt to get you to send any personal information.
Be wary of links in messages that attempt to get you to send sensitive information.
Text messages are sent via your carrier's network, so they're not always secure.

Phishing (voice phishing)

Be wary of calls that attempt to get you to send any personal information.
If you're contacted, call the financial institution directly using the phone number that appears on the back of your credit card or on their website.
Never give out a PIN or an unencrypted password.
Never give out any sensitive information over the phone.
If you're contacted, call the financial institution directly using the phone number that appears on the back of your credit card or on their website.
Never give out any sensitive information over the phone.

