

I.K. Gujral Punjab Technical University Jalandhar
(I.T. Services)

CIRCULAR

No: - IKGPTU/ITS/2017/5615

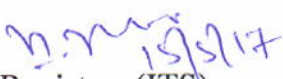
Dated: - 15.05.2017

It is hereby informed that, there is a critical vulnerability (Microsoft Security Bulletin MS17-010) in Various Versions of Microsoft Windows (Client as well as server) which is being used to spread ransomware across the globe. The ransomware is spreading like wild fire infecting critical installations like healthcare globally.

So, it is requested to kindly follow the following steps below to ensure safety of your data and machines.

1. Patch all the Microsoft Windows (Client and Server) for the Vulnerability mentioned in the Microsoft Security Bulletin MS17-010.
2. Always have backup of your important data at your own end.
3. Don't open any email attachment from unknown senders.
4. Don't open these extension files in your systems (taskche.exe, .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .js, .crypto, .cring, .r5a, .pzdc, .good, .LOL!, .R16M01D05, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .Lechiffre, .keybtc@inboxcom, .0x0, .bleep, .1999, .vault, .HA3, .toxencrypt, .magic, .Supercrypt, .CTBP, .CTB2, .locky or 6-7 length extensions consisting of random characters.
5. Be careful while opening and downloading from any unknowing third party websites.
6. Upgrade your traditional Antivirus Solutions to Endpoint Protection Solutions
7. Upgrade your Operating System XP/2003, as 70% attack will happen on these OS.
8. Make sure that ports TCP/UDP 445 are blocked on all perimeter devices and internal access control devices and also on all clients and servers using host firewalls through host antiviruses and HIPS.

Please ensure all the steps carried out immediately to avoid data loss and vulnerability.


Dy. Registrar (ITS)

Copy to Information to: -

- All HoD's of IKGPTU and its Campuses.
- All Faculty/ Officers/ Staff (Teaching and Non-Teaching).
- Officials handling Server's.
- Office File.