MIAMI INFORMATION TECHNOLOGY

Unsupported Remote Access Tools

As you may know, the use of remote access tools to dial in to on-campus computers poses a potential security risk to your and the University's sensitive information. Criminals and hackers often use these access tools to steal information or to mask the activity of computers infected by malware. **In an effort to reduce these types of security risks, UMIT will disable the ability to log in to the UM network through the use of the following unsupported tools on Wednesday, August 1, 2018:**

- AirDroid
- Alpemix
- Ammyy.Admin
- AnyDesk
- Anyplace.Control
- Apple Remote Desktop
- Back.Orifice
- Chrome.Remote.Desktop
- CrazyRemote
- Dameware
- Dameware.Remote
- DeskShare
- Doceri
- EchoWare
- EMCO.Remote.Console
- Ericom.AccessNow
- FastViewer
- FixMe.IT
- GoToAssist
- GoToMyPC
- Goverlan
- Honeywell.TotalConnect
- ISL.Light
- JSP.File.Browser
- Jump.Desktop
- LabTech.RMM
- LiveCare
- LogMeIn
- LogMeIn_Rescue
- Microsoft Remote Desktop Protocol
- MoboRobo
- Motorola.Timbuktu
- MSP.Anywhere
- MyGreenPC
- N-central
- Netop.On.Demand
- Netop.Remote.Control
- NetSupport.Manager
- Netviewer
- NTR.Cloud
- NTR.Support
- pcAnywhere
- pcAnywhere_File.Transfer
- pcAnywhere_Remote.Control
- PhoneMyPc
- Pocket.Controller
- PSExec
- Pulseway
- QQ_Remote.Control
- R.Services
- Radmin
- RDM.Plus
- RDP.over.HTTPS
- RemotelyAnywhere
- RemotePC
- Rexec
- Rlogin
- Rsh
- Rsupport.RemoteCall
- Rsupport.RemoteView
- SaltStack
- ScreenConnect
- Screenhero
- ShowMyPC
- Spy.Agent
- Supremo
- Synergy
- TeamViewer
- TeamViewer_CallReceive
- TeamViewer_CallRequest
- Telnet
- VNC
- VNC_Clipboard
- VNC_File.Transfer
- VNC.Over.HTTP
- webRDP
- Windows.Powershell
- Yoics