RTI REQUEST DETAILS

Registration No. :	PGCIL/R/2019/80114	**Date of Receipt :**	01/10/2019
Transferred From :	Ministry of Power on 01/10/2019 With Reference Number : POWER/R/2019/50682/5		
Remarks :	**Hard copy already sent vide letter No.25-19/31/2019-PG dated 19.09.2019**		
Type of Receipt :	Electronically Transferred from Other Public Authority	**Language of Request :**	English
Name :	Ankit Kumar Lal	**Gender :**	Male
Address :	A 89, LGF, Defence Colony, Pin:110024		
State :	Delhi	**Country :**	India
Phone No. :	+91-9871896117	**Mobile No. :**	+91-9871896117
Email :	ankitkumarlal@gmail.com		
Status(Rural/Urban) :	Urban	**Education Status :**	
Letter No. :	Details not provided	**Letter Date :**	Details not provided
Is Requester Below Poverty Line ? :	No	**Citizenship Status**	Indian
Amount Paid :	0 (RTI fee is received by **Ministry of Power (original recipient))**	**Mode of Payment**	Payment Gateway
Request Pertains to :			
Information Sought :	Please provide a list of the cyberattacks faced by the energy infrastructure across India in 2018, and if the data are available in 2019, complete with location and date for each event. Each item should briefly describe the nature of the attack and, where identifiable, the place of origin (India or foreign country). Infrastructure will include power plants such as dams, solar and wind farms, and coal power plants as well as any other plants with a capacity of more than 7MW. The list should also include discoms websites, breaches of the commercial billing software used by discoms, and any other relevant software infrastructure that may have been targeted by cybercriminals.		
Original RTI Text :	Please provide a list of the cyberattacks faced by the energy infrastructure across India in 2018, and if the data are available in 2019, complete with location and date for each event. Each item should briefly describe the nature of the attack and, where identifiable, the place of origin (India or foreign country). Infrastructure will include power plants such as dams, solar and wind farms, and coal power plants as well as any other plants with a capacity of more than 7MW. The list should also include discoms websites, breaches of the commercial billing software used by discoms, and any other relevant software infrastructure that may have been targeted by cybercriminals.		

Print Save Close