गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian Cyber Crime Coordination Centre

DAILY DIGEST

14th November 2022

Prepared by

Indian Cyber Crime Coordination Centre

Ministry of Home Affairs

Indian Cyber Crime Coordination Centre (I4C)
Daily Digest – 14th November 2022

National

S. No.	News	Link	Source
1	Delhi Police arrest three of cyber criminal gang for duping patients	https://www.thestatesman.com/india/delhi-police-arrest-three-of-cyber-criminal-gang-for-duping-patients-1503130722.html	The States Man
2	Cyber Thugs withdraw Rs 1.5 lakh from PAC worker's account, sent link on WhatsApp	https://www.jagran.com/uttar-pradesh/moradabad-city-cyber-thugs-blown-one-and-half-lakh-rupees-from-pac-workr-account-by-sending-link-on-whatsapp-23200801.html	Jagran
3	Cheated in Delhi while sitting in Patna, took 50 lakhs	https://www.livehindustan.com/bihar/story-cyber-fraud-in-bihar-sitting-in-patna-cheating-in-delhi-took-away-50-lakhs-do-not-do-it-electric-scooty-7346334.html	Live Hindustan
4	Dating crime, Senior citizen duped for 17lakh rupees in Warje	https://punemirror.com/pune/crime/Dating-crime-Senior-citizen-duped-for-17lakh-rupees-in/cid9151950.htm	Pune Mirror
5	Mechanical engineer duped of Rs 80,000 by fraudster impersonating customer care executive	https://www.timesnownews.com/mirror-now/crime/online-fraud-in-mumbai-mechanical-engineer-duped-of-rs-80000-by-fraudster-impersonating-customer-care-executive-article-95489812	Times Now
6	Cyber fraudsters dupe Panchkula man	https://www.tribuneindia.com/news/chandigarh/cyber-fraudsters-dupe-panchkula-man-450676	Tribune India
7	Gurugram man loses ₹45 lakh in cryptocurrency fraud	https://www.hindustantimes.com/cities/gurugram-news/gurugram-man-loses-45-lakh-in-cryptocurrency-fraud-police-101668365699868.html	Hindustan Times

8	Man posing as kin from Canada dupes resident of Rs 6.2 lakh	https://www.tribuneindia.com/news/ludhiana/man-posing-as-kin-from-canada-dupes-resident-of-6-2-lakh-450727	Tribune India
9	Frauded 400 people by taking out a fake plot plan near Jewar Airport; Fake website was created by Yamuna Authority	https://www.livehindustan.com/ncr/story-400-people-duped-by-fake-scheme-of-residential-plots-near-jewar-airport-yamuna-authority-fake-website-also-created-on-arrested-7350616.html	Live Hindustan
10	Brothers duo dupes man of Rs 8L	https://www.lokmattimes.com/aurangabad/brothers-duo-dupes-man-of-rs-8l/	Lokmat Times

INTERNATIONAL

S. No.	News	Link	Source
1	**Black Friday and Christmas shopping scam warning issued by cops and spy chiefs after £15million nicked last year**	https://www.thesun.co.uk/money/20415596/black-friday-shopping-warning-scams/	The Sun
2	**Cyber criminals hold Asian tech workers captive in scam factories**	https://www.japantimes.co.jp/news/2022/11/14/asia-pacific/crime-legal-asia-pacific/southeast-asia-cybercrime-scams/	Japan Times
3	**Australia to ban paying of ransoms to cyber criminals?**	https://tech.hindustantimes.com/tech/news/australia-to-consider-banning-paying-of-ransoms-to-cyber-criminals-71668332209000.html	Hindustan Times
4	**Federal Government to launch international taskforce against cyber crime**	https://www.insurancenews.com.au/regulatory-government/federal-government-to-launch-international-taskforce-against-cyber-crime	Insurance News

Delhi Police arrest three of cyber criminal gang for duping patients

With the arrest of three persons, the Cyber Police team of the North Delhi has succeeded in busting a cyber criminal gang involved in duping gullible patients on the pretext of providing Ayurvedic treatment at Patanjali Yoga Gram, Haridwar.

The accused have been identified as Harendra Kumar, 25, Ramesh Patel, 31 and Ashish Kumar, 22, all hailing from Bihar. Five laptops, ten mobiles, 19 SIM cards, Wi-Fi modem, etc, have been recovered from the accused. An amount of Rs 1,66,000 has been frozen in the bank account of the accused.

During the inquiry, it was revealed that the accused created a fake website of Patanjali Yog Gram and received calls from patients and impersonated themselves as Ayurvedic doctors for registration and booking.

Accused Ramesh and Ashish disclosed that they would purchase pre-activated SIMs of West Bengal, Assam and Orissa from various sources. They also purchased pre-activated bank accounts, which were used for transfer of payment and withdrawals.

The accused further revealed that fake websites were created so that people looking for treatment at Patanjali Yog Gram will contact them for booking as no option of online booking for stay at Patanjali Yog Gram was available on the internet.

Once the victim contacted them on their number mentioned on the website, they introduced themselves as Doctor of Patanjali Yog Gram and used to charge money in the name of booking and treatment.

Further money was withdrawn by different persons at different locations. They even sent forged payments receipts and booking vouchers to the victims to gain trust. It was even revealed that the accused Harendra created websites in the name of https://tptayurved.in/ and https://theayurvedicupchar.com/ with Ayurveda and treatment as keywords.

The accused also revealed that they keep on changing numbers on websites as their numbers get marked as spam on true-callers after making some calls. 20 fake websites in the name of Patanjali Yoga Gram and other Ayurvedic treatment centres were identified and details were sent to National Internet Exchange of India for blocking.

Deputy Commissioner of Police (North Delhi), Sagar Singh Kalsi said that a complaint on Ministry of Home Affairs (MHA) Cyber Crime Portal in the name of Nitin Sharma was received at

Cyber Police Station, North District. It was alleged that the complainant, who searched a mobile number on Google and contacted it for Ayurvedic treatment of his son, was duped of over Rs 2,40,500 in the name of registration and other booking process at Patanjali Niramayam, Haridwar.

A case was registered on the complaint and investigation was taken up. The police team started technical analysis and identified one suspect. The accused was apprehended from Patna, Bihar, who created a fake website. Subsequently, other two accused were also arrested on the information provided by the arrested accused.

Cyber Thugs withdraw Rs 1.5 lakh from PAC worker's account, sent link on WhatsApp

By sending a link on WhatsApp of 24th Corps PAC personnel based in Moradabad, cyber thugs withdrew 1.5 lakh rupees from the account. Cyber thugs had threatened him in the name of income tax. On the complaint, the Civil Lines Police has started investigation by registering an FIR.

Fraud by sending link on WhatsApp

PAC personnel Noor Alam told the police that a message came from a number on his WhatsApp. In which the accused talked about making an ID by visiting the link. In this, the thugs stole 1.5 lakh rupees from their account in the name of linking money to the wallet through UPI account in different ways by creating ID. An FIR has been lodged against the accused in the case. But, till now the police has not been able to trace him.

Cheated in Delhi while sitting in Patna, took 50 lakhs

Cyber thugs sitting in Bihar made a fake website of electric scooty and cheated the people of Delhi of about 50 lakhs.When the Cyber Cell of Delhi Police investigated the matter, it was found that the thugs were sitting in Patna. After this raids were started in Patna.Delhi Patna Police has arrested 16 accused in this case in a joint operation.The police is busy in exposing the gang.

All were produced in the court of ACJM-1 Naveen Kumar Srivastava in the Civil Court.After this, the accused were handed over to the officials from Delhi on transit remand.According to the police, the amount of forgery can increase if the fake website is scrutinized.The police are not yet able to tell the exact number of victims of the fraud.Since this gang has members from other states as

well.That's why it is estimated that hundreds of people would have been victims of the fraud.

Police arrested Aman alias Rocky and Anish alias Golu (Mahanandpur police station Sekhupur Sarai Patna), Bittu (Bajiganj Gaya), Sunny (Katisarai Nalanda), Navlesh (Manjhawe Nawada), Aditya (Govardhan Bigha Nalanda), Vivek Kumar (Sijua police station Jokta Dhanbad). , Murari (Palauni Police Station Manpur Nalanda), Ajay Kumar (Shantinagar Chas Jhodhi Mod Dhanbad), Avinash Kumar (Ahilyachak Katrisarai), Prince Kumar Gupta (Katrisarai Nalanda), Vadithya Chinna (Mehboob Nagar Rangareddy Hyderabad), Anand Kumar (Katrisarai Nalanda), Shiva Kumar (Mahboob Nagar Rangareddy Hyderabad), Ramesh Kumar (Mahboob Nagar Rangareddy Hyderabad) Srinu S (Mahboob Nagar Rangareddy Hyderabad) have been arrested from Rupaspur police station area.

Used to cheat like this

The gang of cyber criminals had created a fake website in the name of Ola Electric City Scooty.The gang members used to talk about buying and selling by calling certain mobile numbers.Used to take a scooty worth 1 lakh 40 thousand by telling it as 70 thousand.Used to talk about ATMs, credit cards etc.After falling in the trap, they used to get the app downloaded or asked for the card number and pin code.After that, he used to withdraw money from his account.

Dating crime, Senior citizen duped for 17lakh rupees in Warje

A senior citizen (age 79 years, res Warje Malwadi) was duped of Rs 17 lakh by online fraudsters under the pretence of friendship with young ladies using a dating app. A case against a lady called Shreya has reportedly been registered at the Warje police station.

The victim is an elderly resident of Warje Malwadi. He worked as a bank officer and worked for a private corporation after retirement. A young lady named Shreya called the victim's cellphone number in December last year. She had previously sent images of several young ladies to his mobile number while luring him to friendship and enquiring if he wanted a girl for dating.

The victim transferred three thousand rupees to the accused Shreya's bank account. He occasionally sent money to the bank account Shreya had provided. The young woman responded in vain when he asked her since he wasn't friends with her. He discovered that Shreya's cellphone number was off when he tried to call

her again. The elderly citizen's son reported the scam to the Warje police as soon as he became aware of it. It has come to light that the complainant was occasionally used as bait to extort 17 lakh 10 thousand rupees. Inspector Dattaram Bagwe of the Crime Branch is conducting the inquiry.

“A case has been registered against the accused under section 419, 420 IPC and IT Act 66(c)(d) but no arrests have been made yet, we are further investigating the case, people should trust not these kinds of online apps and fall prey to the luring, and report to the police immediately,” said Police inspector Dattaram Bagwe of the Crime Branch while talking to Pune mirror.

Mechanical engineer duped of Rs 80,000 by fraudster impersonating customer care executive

In an incident of online fraud, a 49-year-old mechanical engineer was allegedly duped of Rs 80,000 by cyber fraudster on Friday. The victim works for Bombay Port Trust. A complaint was registered in the matter on Saturday.

The fraudster cheated the complainant by posing as an executive of a retail hypermarket chain, reported The Indian Express. Based on the complaint, an FIR was registered at the Wadala police station in Mumbai. The engineer held a Big Bazaar profit club card with a balance of Rs 10,000 in it.

The victim decided to withdraw Rs 10,000 from his club account as the Big Bazaar outlet in his locality had shut down. On Friday searched for customer care numbers of Big Bazaar on the internet and ended up calling a fraudster as he had posted his number as Big Bazaar helpline, reported the media outlet.

The accused asked the engineer to install the AnyDesk app on his mobile phone. The complaint followed the directions given by the fraudster. Notably, the Anydesk app makes a third party take control of others' mobile phones.

The accused asked the engineer to share his credit card details. He also got the one-time password (OTP) and used it to withdraw Rs 80,000. After the complainant saw messages about the transaction, he blocked his credit card.

Upon realising that he was cheated, the approached the police, A detailed investigation has been launched into the matter.

Cyber fraudsters dupe Panchkula man

A Panchkula resident has allegedly been duped of Rs 899 by online fraudsters on the pretext of supplying a cleansing mask.

In a complaint to the Sector 2 police post, the Sector 2 resident claimed he had placed an online order for Clayglo Green Tea Pore Control Stick Mask 1 from Gwalior-based M/s Polarity by paying Rs 899. The product was to be delivered through Shadowfax courier.

A courier boy delivered an envelope, which was found empty when opened. On contacting the courier, the complainant learnt no such office existed. He alleged the courier firm and the company were hand in glove in duping public. The firm was luring customers through 'one plus one scheme' on Facebook, it was learnt.

Police post incharge Gurmej Singh said they had forwarded the complaint to the cyber crime cell of the Panchkula police and investigation was on.

Gurugram man loses ₹45 lakh in cryptocurrency fraud

A 44-year-old senior executive of a private firm was allegedly duped by an unidentified woman on the pretext of investing in cryptocurrency in October this year, police said on Sunday.

The victim met the woman on a social networking site. After befriending him and gaining his confidence, the woman asked him to invest in a cryptocurrency exchange platform, police added.

The victim alleged in his complaint that she made him register on a crypto trading website on October 28, and on her suggestion, he invested ₹45 lakh. The suspect used to allegedly share information regarding investments.

Police said that the victim earned huge profits after a month and his account balance soared to ₹1.30 crore, following which he tried to withdraw the money, but was asked to invest ₹25 lakh more, else there will be a 30% deduction from his account. The victim became suspicious and reported the matter to police.

"I had invested ₹45 lakh and when my amount had reached ₹1.30 crore, I tried withdrawing the money but the website restricted me. It mentioned that I must deposit ₹25 lakh first to withdraw the entire amount. This was quite alarming and when I checked the site carefully, I noticed that it was a copy of a well-known Korean cryptocurrency site," said the victim, requesting anonymity.

Police said that the victim received a message that he had to invest more money before November 14, else they would start deducting 30% of the principal amount every day from his account.

“The woman lured him to invest in cryptocurrency and sent a website link that showed huge returns on investments. We have started analysing the bank account details and other information available. We have also written to the bank to freeze the bank accounts so that the suspects cannot transfer money to any other account,” said Preet Pal Sangwan, assistant commissioner of police (crime).

The mobile number and the social media account used by the suspect have gone inactive for the last one week, police added.

On September 14 this year, a 32-year-old hearing and speech-impaired man, working with an e-commerce retail store, was arrested from Udyog Vihar for allegedly cheating people on the pretext of investing in cryptocurrency, police said.

The suspect had more than 15 crypto trading applications on his phone and used them to divert the cheated money to his associate in the United States, police added. The matter came to light after a man alleged that he was contacted by a woman named Diana on his social media platform.

ACP Sangwan said they receive at least two complaints related to cryptocurrency every week and cases of people being duped is on the rise.

Man posing as kin from Canada dupes resident of Rs 6.2 lakh

A man posing as nephew from Canada duped a resident of Rs 6.20 lakh.

The Sadar police yesterday registered a case against an unidentified person under relevant sections of the Indian Penal Code (IPC) and the Information Technology Act.

The complainant, Manmohan Singh, of Ishar Nagar told the police that on October 10 he got a call from some internatinal number and the caller posed himself as his nephew from Canada.

“I thought my nephew Jagmit Singh, who stays in Canada, might be on the line. The caller introduced himself in a way that I could not doubt his identity,” the complainant said.

He said later, the conman informed him that he got entangled in some case after a fight in a night club and he needed some money urgently to pay the legal fee.

“Since I had affection with my nephew

and I failed to gauge the intentions of the conman, I transferred Rs 6.20 lakh from my different bank accounts to him. A few days later when I got to know that my nephew had not called me for any financial help, I got a shock of my life. Afterwards, I informed the police," alleged Manmohan.

Investigating officer in the case inspector Gurpreet Singh said after registering a case, further probe had been launched by the police to identify the caller.

Frauded 400 people by taking out a fake plot plan near Jewar Airport; Fake website was created by Yamuna Authority

A case of cheating more than 1.25 crore rupees from more than 400 people has come to the fore by taking out the plan of a residential plot in the Yamuna Authority area through a fake website.The Bisrakh police of Greater Noida have arrested an accused.Preliminary investigation has revealed that this money of fraud has gone to the bank account of a firm.The police is now investigating this firm.There could be many more arrests in this case very soon.

On October 7, 8-10 people had filed a case in the Bisrakh police station that they had been cheated by making a fake site of Yamuna Authority.It was also told in the complaint that the thugs have made hundreds of people their victims.Bisrakh police started investigating the matter.

Police on Sunday arrested Madhur Sehgal, a resident of JP Wishtown, Sector-128, Noida, who duped citizens by creating a fake site of the Yamuna Authority.He was arrested from the shop built on the second floor of Tower-1.The accused has also maintained an office in Sector-129.Police inquiry has revealed that the thugs have deposited this money in the bank account of a firm.Now the police is probing that firm.Soon there will be other arrests in this case.

Started two months ago

Bisrakh Kotwali in-charge Umesh Bahadur Singh told that about two months ago the thugs www.Created a fake website named yerdawasiyayojna.com.The thugs started the scheme of giving cheap plots in Bhagirath Society in Dankaur area on the banks of Yamuna Expressway.People were made to deposit Rs 15000, Rs 21000 and Rs 31000 for booking plots through this website.All the money used to come into the account at once through the Rajor Pay platform.About 1.25 crore has been cheated.Applicants were

told that allotment will be done by lucky draw.

The plan comes with the permission of the authority

Greed to buy land near Jewar airport has made people a victim of fraud.In fact, the authorities bring plans of plots in the notified area.No plan comes in the notified area without the permission of the authority.If someone does this then action is taken against him.Authorities bring out plans for builders.After that the builders draw out the plan of the plot and the flat.But people got trapped in this scheme without investigation.

Such a conspiracy to cheat

The construction work of Jewar Airport is going on in Yamuna Authority area.There is a competition for those taking residential plots near the airport.In the month of September, the Yamuna Authority had come out with the scheme of residential plots.In this scheme, the number of people who filled the form had reached close to 90 thousand.In view of this, the thugs hatched a conspiracy.Started cheating people by creating fake website.

Brothers duo dupes man of Rs 8L

Two brothers duped a man of Rs 8 lakh on the lure of giving him a job in Savitribai Jyotiba Phule Hospital run by Nagari Vikas Bhuudesshiya Sanstha. The accused brothers have been identified as Avinash Manikrao Kamble (Pratapnagar) and Ajay Kamble (Bajajnagar Waluj).

According to the complaint lodged with City Chowk police station, complainant Prashant Kate (Johariwada, Gulmandi) mentioned that the Kamble brothers told him that they can get a permanent job for his brother Pranit Kate in the hospital run by the Sanstha. They asked Prashant to give Rs 4.5 lakh for the job. Rs 3 lakh was given in the office of Sachin Zaveri in cash and later Rs 35,000. Pranit worked for four months in the hospital at Ellora but did not receive any salary. Later, he was told that the hospital will be shifted to Kannad and he will have to pay for the job or the job will be given to another person. Hence, Kate brothers gave additional Rs 3.5 lakh. However, Pranit did not receive any job. When they asked Kamble brothers to give their money back, they gave only Rs 80,000 in installments. Hence, they lodge a complaint with City Chowk police. PSI Rohit Gangurde is further investigating the case.

INTERNATIONAL

Black Friday and Christmas shopping scam warning issued by cops and spy chiefs after £15million nicked last year

POLICE and spy chiefs have issued an unprecedented warning to Sun readers over online Black Friday and Christmas shopping cons.

More than £15million was nicked last year with the average loss at £1,000.

Most scams involved mobile phones, electronics, cars and designer clothes — and people aged 19 to 25 were most likely to be victims.

One buyer lost £7,000 when they tried to buy a camper van.

But officials fear scams could soar this year as the cost of living crisis forces more shoppers to hunt for rock-bottom prices.

They said criminals pose as genuine sellers on popular online marketplaces with deals that prove "too good to be true".

The warning comes jointly from the National Crime Agency, the National Cyber Security Centre and City of London Police.

The crime-fighting trio urged online shoppers to protect their accounts using two-step verification and strong passwords.

People should also check reviews from trusted sources before buying, and use a credit card to pay or platform such as PayPal, Google or Apple Pay.

The officials said: "And, if you see what you think is a scam email, text or website then reports them.

"Last year, the public made 6.5million reports to the suspicious email reporting service, and as a result we removed 62,000 scam websites."

Cyber criminals hold Asian tech workers captive in scam factories

Indian engineer Stephen Wesley was puzzled when he was asked to take a typing test during an interview for a graphic design job in Thailand — but put it out of his mind when he got the role.

Hours after landing in Bangkok to start work in July, Wesley and seven other new recruits were instead

ferried over the border into Myanmar where their phones and passports were taken, and they were put to work on online cryptocurrency scams.

"I spent up to 18 hours a day researching, typing messages, chatting with people on social media platforms, gaining their trust and encouraging them to invest in cryptocurrency," said Wesley, 29, in a telephone interview.

Thousands of people, many with tech skills, have been lured by social media advertisements promising well-paid jobs in Cambodia, Laos and Myanmar, only to find themselves forced to defraud strangers worldwide via the internet.

Wesley spent 45 days held captive at a compound in Myanmar's southeastern border town of Myawaddy, and given a list of about 3,500 names that he had to contact via Facebook, Instagram or dating apps.

"We were trained on how to flirt, chat about hobbies, everyday routine, likes and dislikes. In roughly 15 days, the trust would be built and the client would be willing to take our advice on investing in crypto," he said.

The cybercrime rings first emerged in Cambodia, but have since moved into other countries in the region and are targeting more tech-savvy workers, including from India and Malaysia.

Authorities in these countries and the United Nations officials have said they are run by Chinese gangsters who control gambling across Southeast Asia and are making up for losses during the pandemic lockdowns.

The experts say the trafficked captives are held in large compounds in converted casinos in Cambodia, and in special economic zones in Myanmar and Laos.

"The gangs targeted skilled, tech-savvy workers who had lost jobs during the pandemic and were desperate, and fell for these bogus recruitment ads," said Phil Robertson, deputy director for Asia at Human Rights Watch. "Authorities have been slow to respond, and in many cases these people are not being treated as victims of trafficking, but as criminals because they were caught up in these scams."

Dubious tech firms

Cybercrime has surged with the rise of digital platforms that brought easy access to personal data online as well as improved translation software and artificial intelligence-generated photos that help scammers to create fake personas.

The scam that Wesley and others were forced into is known as pig butchering, where a scammer builds trust with their victims over social media, messaging and dating apps,

then pressures them to invest in bogus crypto or online trading schemes.

The term refers to the process by which scammers "feed their victims with promises of romance and riches" before cutting them off and taking their money, according to the U.S. Federal Bureau of Investigation, which traced its origins to China in 2019.

"People don't realize it, but they do share a lot of information on social media platforms," said Dhanya Menon, director of Avanzo Cyber Security Solutions in India, which advises firms on cybersecurity.

"If you follow someone's social media for just 15 days, you will glean a lot of information about them," she said, adding that cryptocurrency scams are on the rise because there is little awareness of how the virtual currency works.

India's foreign ministry in September issued an advisory warning youth with technology skills of fake job offers in Thailand from "dubious IT firms involved in call-center scam and cryptocurrency fraud."

Authorities last month said they had rescued about 130 Indians from such schemes in Laos, Cambodia and Myanmar — including Wesley and others.

Myanmar's military government — which took control of the country in a coup in February 2021 — did not respond to a request for comment.

Cambodian officials, who for months denied reports of abuses and trafficking, have taken a harder stance in recent months, and ordered a crackdown on online scam operators across the country.

Fake dating profiles

Bell, a 23-year-old Thai woman, said she was lured by the offer of an administration job with a monthly salary of about $1,000 and free food and housing at a casino in Cambodia.

But when Bell — who used a pseudonym to protect her identity — arrived at the casino in the coastal city of Sihanoukville in December, her Chinese employers took away her passport, ID and mobile phone, and locked the doors.

She was made to create a fake profile on social media and build relationships with men on the Tinder dating app, then persuade them to invest in stocks.

"I wanted to go home because it wasn't what I wanted to do, but they said I would have to pay 120,000 to 130,000 baht ($3,175-$3,440)," she said. "I had to (work) for fear of being beaten."

Bell and 20 other Thai detainees were rescued in June by Thai police, who have freed more than 1,200 of their citizens from compounds in

Cambodia since late last year, said Surachet Hakphan, assistant commissioner general of the Thai police.

More than 3,000 Thais are still trapped in Sihanoukville and Phnom Penh, Surachet estimated.

Wesley, who was also told to pay a large ransom if he wished to leave the compound in Myanmar, had to create a fake persona of a young female Brunei-born graphic designer who was working in Monaco and was fond of posting selfies.

He targeted 50 people daily in Europe, Australia, Britain and India, asking each to invest $20,000 to begin with.

Now back in India, Wesley is struggling to find work.

"When I look back ... I keep wondering if there were any signs that I missed or anything I could have done differently," he said from Chennai, where he was interviewing for a job. "But I didn't suspect anything.

Australia to ban paying of ransoms to cyber criminals?

Australia's Home Affairs Minister Clare O'Neil on Sunday said the government would consider making illegal the paying of ransoms to cyber hackers, following recent cyber attacks affecting millions of Australians.

Australia's biggest health insurer, Medibank Private Ltd, last month suffered a massive cyber attack, as Australia grapples with a rise in hacks.

Singapore Telecommunications-owned telecoms company Optus, Australia's second largest telco, along with at least eight other companies, have been breached since September.

Asked on ABC television on Sunday whether the government planned to look at outlawing ransom payments to cyber criminals, O'Neil said "that's correct".

"We will do that in the context of ... cyber strategy," she said.

The comments come after O'Neil, on Saturday, formalised a new cyber-policing model between the Australian Federal Police (AFP) and the Australian Signals Directorate - which intercepts electronic communications from foreign countries - to do "new tough policing" on cybercrime.

Around 100 officers would be part of the new partnership between the two federal agencies, which would act as a joint standing operation against cyber criminals.

The taskforce would "day in, day out, hunt down the scumbags who are responsible for these malicious crimes", she said.

The AFP earlier this week said Russia-based hackers were behind the attack on Medibank, which compromised data from around 10 million current and former customers.

Attorney General Mark Dreyfus on Saturday refused to be drawn on whether the Russia-based ransomware group REvil was responsible for recent cyber attacks on Australians, but said it was a "very organised criminal gang" located in Russia.

Prime Minister Anthony Albanese has previously said the government was doing all it could to limit the impact of the Medibank hack and had set up a phone service for affected customers to seek help from both the government and Medibank.

Federal Government to launch international taskforce against cyber crime

The Federal Government says it will launch a “standing operation” to investigate and disrupt the practices of cyber crime syndicates, with a focus on ransomware threat groups in the light of the Optus and Medibank data breaches.

The Office of Home Affairs announced that the Australian Federal Police (AFP) and the Australian Signals Directorate (ASD) will coordinate with international partners to shut down online criminal operations “regardless of where they are”.

“The recent Optus and Medibank data breaches have shown the extent of the damage that can be done by malicious actors,” Minister of Home Affairs Clare O’Neil said.

“This new joint campaign will ensure the full powers of the AFP and ASD are brought to bear to stop such incidents before they start.

“Where incidents do take place, it means that cyber criminals will be hunted down and their networks disrupted. It sends an important message to criminals and hackers intending to do harm – Australia will fight back.”

Ms O’Neil described ransomware as a “global scourge” which requires “coordinated international action to combat”. The effort comes after recent data breaches of major Australian companies, including Optus and Medibank, exposed millions of Australians’ private data and information to hackers.

The Department of Home Affairs

Cyber and Critical Technology Coordination Centre will host the taskforce and international government stakeholders to discuss effective solutions against cyber crime.

"The international counter-ransomware task force will drive international cooperation and joint efforts to tackle ransomware including through information and intelligence exchanges, sharing best practice policy and legal authority frameworks, and collaboration between law enforcement and cyber authorities to conduct counter-ransomware activities," Ms O'Neil said.

The government has also aimed to pass stricter privacy laws that will increase penalties for data breaches to at least $50 million.

It says the proposed changes will help to act as an incentive for companies and large organisations to have adequately installed security to prevent the risk of similar exposures of customer data.