

Welcome to

Identity Shield 2024

Where Pune talks Cyber Security

Anirban Mukherji

CEO, miniOrange anirban@miniOrange.com







Why have a Cyber Security Conference?



Cyber Security trends - consumers

Social Engineering attacks



People lose ₹3 crore to cybercrime across Maha daily, says DIG Shintre

Shashank, Didminhe

Pune: Burely Rs 134 errors as 10% of the total Rs 1,500 crors less to expercrime in Maharashtra since 2013 have been recovered through police investigations, deputy inspector general of police Saniay Shintre in the city saidon Saturday.

"The police force has a working system to tackle cybererimes. Bul 18 is not strong enough. The cybererime police in the state receive roughly 4,000-5,000 calls every day from the cybererime victure. The daily menetary loss to cybererimes is. Re 3 cross in Maharahira." Shintre said at an event organised by cyberiscurity solution firm Quick Heal Tochnologies.

The event was aimed at increasing eybersecurity sources and recognition efforts of students, teachers and institutions in spreading cybersecurity initiatives.

Maharushtra saw 8,249 rybercrime cases in 2022, which was 68% higher than 5,562 incidents recorded in the previous year. National

TTatal



WIDE NET: DIG Sanjay Shintre says the cybercrime police units in the state receive roughly 4,000-5,000 rails every day from victims

Crime Records Sureau (NCRS) data showed. At the national level, as many as \$5.803 cases were reported in 3022, the data revenied.

The Mahamahira powth cyberseurity project is expected to be rolled out in the counting months, Shintre said, adding that there were extreals under the project, including scenmand, security operations and network operations contras

Around 140 engineers will take complaints on a helpline under the project. These complaints will be directed to respective police stations, while a major number of case will be investigated in the central cell.

In many cases, migrant workers fall for ordine scams while looking to augment their incomes. When a fresh graduate from a rural area comes to the city in search of a job, a he realises that monthly salary is not enough to make ends meet. This is when s, he star is looking at it when s, he star is looking at

ways to make additional mones: Cybercriminals latch on to such people by using provalent baits on social media and other websites, he said.

Shintre also referred to sunk-cost fallacy. The term means that despite the victims suspecting that they are likely to be duped, they continue to engage in the "suspicious" activity as they have invested time and money into it and partly in expectation of getting something out of it. "The criminals have recognised this behaviour of the victims and they exploit it fully to their advantage," Shintre said.

Cybercriminals have even created fake online protiles of police officers and other authorities, which they use to intimidate the victims. "These criminals lure the victims to join on a video call. Criminals posing as police officers then ask them [the victims] to make newments. "Shintre said.

In India, cybercriminals target 1-2 crore people every day There are 120 crore internet users in India, 80% of these use smartphones, data available with various agencies showed.

Job Scam

- Marriage Scam
- Pension Scam
- Investment scam
- Loan fraud
- Online support scam
- Online orders scam
- Lottery scam

List is endless...



Enforcement agencies are inundated with cyber fraud

complaints

Reporting Infrastructure is inadequate



ED busts cyber scam in India on Irish complaint

Prodects.Thehar@timesgroup.com

New Delhai in a first of theirind mener laundering case, a complaint Sodgod by an Irish soman in Dungarvana, a costalown in telsand, was taken up for investigation by ED in in dia trigpering a series of sourches across Bihar and West Bengal

It resulted in busting of a syndiose of cyber criminals mustly school dropout desi beps spexific accented Relftish English — swindling people in IR and frashend by removely taaing control of their phones and computers and transferring several cross of rupous from their bank accounts into their own.

Searches in Patna, Kharagour and Kolkata unearthed a 70senter call centre operated by the crooks that had conned at least 40 victims. The Irish woman complained of receiving a call from one 'Stephanle' from Eircom Telecom, a broadband service provider of her country. Accused Stephanie, who turned out to be Nitesh Kumar, was operating from a guest house in Parna which was searched last Dec 18. He was apprehended before he could jump out of the window of his room.

Searches at three locations of crime to the bank accounts in Kolkata and one in Kharag of their foreign associates ba-

SEIZES 75 CRORE

- ➤ Searches in Kharagpur and Kolkata lend to setume of 70 PCs, 5 taptops, 16 monleys, 56 credit/withit cards and TAS crore.
- > stephanie who conned an irish woman turns out to be Nitesh Kumar from Patna > Let time an FIR abroad used as a predicate offence by ED to register PMLA case & seize proceeds of crime

purnt the premises of Sagar Yoday, the kingplin of synthiaste, led to seluture of flive laptops, it is mobile handsets, bi credit/debit certis and 69 bonk accounts along with cash of around 82 crore. Officials intre-saled II 2.8 crore in bank accounts of the accused.

The probe flarther revealed that two lilegal call custres were being operated by Sagar Yadaw in Kharagpan During the searches, 70 computers with 1P telephones and headphones were recovered. The ED arrested three persons in the case, including Yadaw and Kumar.

After taking control of the victims' bank accounts on their phone/computer remotely, the accused transferred proceeds of crime to the bank accounts of their foreign associates ba-

sed in UK Ireland, who their withdraw these amounts and transferred the screek to balls through Western Union and Moneygram platforms. After receiving the proceeded crimes in the Indian bank accounts, the same used to be will direct, in cash.

This is for the firent time than an FIR looked oversees was used as a predicate offence by the cantral agency to register a case under the Prevention of Money Laundering Act (PMLA) and seized "grounds of ceime".

The mass falls under the categery of offerce of 'cross-border lumbication' under Phili.A as it was committed in a besign country and later the proceeds in the instant case were transferred to India, a senior official awars of the investigation revealed. The ED registered an ECIR, equivalent to a police FIR, in Oct 2023 and began toreset justing the case office it was referred to India by Irish authorities through the CBI.

Ruman's mobile phones we re solved and further investigation revesiled at least 44 hationals from the UK and Ireland had faller victim to the syndicate master minded by him along with a dozen of other associates operating from Kharagpur and Kolkata.

- Scammers are scamming foreigners sitting here in India
- Too many scams to investigate
 A large number of people are not even reporting because of different reasons
- Those that are reported, the arbitration could take months with no results
- Getting back what is lost can be tedious and is a long process
- Sometimes its more than money that is lost



Key takeaway for consumers - What is the solution to this menace?



Drop OTP? You'll still need phone

Mumbai: RBI has asked regulated entities like banks to look at alternatives to SMS-based one-time passwords for second-factor authentication. While there are alternatives, a mobile phone is central to all of them.

Bankers say that OTPs are susceptible to 'social engineering' frauds where one manages to get the customer to divulge the password or obtains the same through a SIM swap.

The most common alternative to OTP is an authenticator up that requires the user to obtain a password from another application on the phone. Service providers have develoed other options as well like kens within the mobile app. While this establishes the promance of the message, it still

RBI SEEKS ALTERNATIVES

> RBI has asked regulated entities to look at alternatives to SMS-based OTPs for twofactor authentication amid rising traud cases

The most common alternative to OTP is an authenticator app that requires the user to obtain a password from another application



➤ Service providers have also developed other options as well like tokens within the mobile app. Write this establishes the authenticity of the message, it still needs a phone

needs a phone.

Route Mobile, which provides a communication platform as a service, sends nearly four billion OTPs every mooth on behalf of various service providers "The increase in digital adoption also increases the potential for digital frauds. We are seeing a gap between

the emerging markets, which are seeing high growth without any discussion on the rising froats." Regitykumse Gupta. MD & CBO of Route Mobile. He said the rising froats have prompted the company to launch TruSense division under Route Mobile UK to thousant identity theft.

not a good standaines within tiestion option us developments in All have brought in a new risk of despthies bypasing framerics option. For the Indian market, the mobile phone is the best klendiffer as the customer must verify their identity before obtaining a connection. Straits are not as spood as it is easy to generate false false email identity. Also, asympte can conerct an email.

without KYC," said Viene

OTP-less authorization, who

re the service provider will be

us a direct data connection

OTP According to David VS

Cyber Security Education

- Site should authenticate itself to the user first
- Password less authentication
- Adaptive Authentication

Call to action - Talk to 5 people around you and make them aware that this is happening and they need to be extra assertive







What's happening in the Enterprise world?



Cyber Security trends – Enterprise

Infosys US Subsidiary Named as Source of Data Leak at BoA

Identifies IMS as source of data leak which led to Nov ransomware attack

Beena Parmar

Bengaluru: Top American lender Bank of America has named Infosys McCamish Systems (IMS), the US subsidiary of Indian software services giant Infosys, as the source of a data leak owing to a runsomware attack suffered by over 57,000 of its users in November, according to documents reviewed by ET.

"On or around November 3, 2023, IMS was impacted by a cybersecurity event when an unauthorized forming about the data breach, ET of Majne a northeastern resithird party accessed IMS systems. resulting in the non-availability of certain IMS applications. On No- America described the nature of tain-whether other bank vember 24, 2023, IMS told Bank of America that data concerning de breach (backing) that illegally ac pacted by the breach ferred compensation plans ser- cessed information of 57,028 perviced by Bank of America may sons stealing data such as 'Name



have been compromised," said a before the Office of the Ma letter sent earlier in February to torney General the chief legal Bank of America consumers in visor and prosecutor of the l has reviewed the letter.

The notification by Bank of ET could not immedi the incident as "External system tomers of Infosys were also

or other personal identifier in comhination with: Social Security Number" Bank of America's systems were not compromised to

This is as per a recent disclosure.



- Access is gained through 3rd party vendors where security is not top notch
- Phishing attacks are carried out on non technical staff
- Sophisticated attacks DOS, Ransomware

Denial of Service attacks

Insider threat



Key takeaway for enterprises





- Background checks
- **→** 3rd party access control
- > Privilege access management
- Cyber Security education to prevent phishing attacks
- ➤ Keeping systems upto date with patches, not keeping un-necessary ports open, restricting access, sophisticated security systems in place
- > SSO, MFA







It is all about Identity and Access



Identity Shield has something for your unique Cyber Security needs.



IdentityShield 2024 Consumer section

- 1. Posters for Cyber Security Education To spread awareness. Different types of fraud happening in our society and how to prevent them.
- 2. Sessions on protecting your online identity Basic track

IdentityShield 2024 - Enterprise section

- 1. Posters for Cyber Security Education for enterprises
- 2. Sessions on advanced topics related to Identity, Access, Single Sign on, Multi Factor Authentication
- 3. Booths showcasing different Cyber security products that are being used by our 20000 customers worldwide

IdentityShield 2024 – For students

1. To have a career in CyberSecurity, its very important to know how to create Security products rather than knowing how to use them!

Welcome to... IdentityShield 2024!





Cyber Security is all about protecting your identity!

Let's explore IdentityShield 2024

Anirban Mukherji

CEO, miniOrange anirban@miniOrange.com

