



Proceedings
of
National Level Webinar on
Prevention and Investigation of
PHISHING CRIMES
फिशिंग अपराध
निवारण एवं अन्वेषण की कार्यवाही

(January 18, 2022)

National Cyber Crime Research & Innovation Centre (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Promoting Good Practices & Standards



Proceedings

National Level Webinar on Prevention and Investigation of

Phishing Crimes

फिशिंग अपराध

निवारण एवं अन्वेषण की कार्यवाही

(January 18, 2022)

National Cyber Crime Research & Innovation Centre (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Promoting Good Practices & Standards

अमित शाह



गृह मंत्री एवं सहकारिता मंत्री
भारत सरकार



संदेश

मेरा यह दृढ़ विश्वास है कि कानून प्रवर्तन एजेंसियां लोकतंत्र की सुरक्षा में महत्वपूर्ण भूमिका निभाती हैं और एक चुनौतीपूर्ण कार्य करती हैं। आज राज्यों/केन्द्र शासित प्रदेशों में पुलिस बल साइबर अपराधों की रोकथाम एवं जांच का चुनौतीपूर्ण कार्य कर रहे हैं। राज्य/केन्द्र शासित प्रदेश अपने साइबर सुरक्षा तंत्र को मजबूत कर रहे हैं और अपनी कानून प्रवर्तन एजेंसियों की क्षमता निर्माण को बढ़ा रहे हैं। केन्द्र सरकार अपनी विभिन्न योजनाओं द्वारा राज्य सरकारों की पहलों को परामर्श और वित्तीय सहायता प्रदान कर उनकी क्षमता निर्माण में वृद्धि कर रही है।

NCR&IC गृह मंत्रालय की I4C योजना का एक महत्वपूर्ण विंग है जो कानून प्रवर्तन एजेंसियों को प्रौद्योगिकी का लाभ प्राप्त करने के लिए वेबिनारों का आयोजन कर रहा है जहां सुशिक्षित प्रोफेशनलों के ज्ञान और अनुभवों को राज्यों/केन्द्र शासित प्रदेशों की पुलिस और केंद्रीय पुलिस बलों के कार्मिकों के साथ साझा किया जाता है। मैं 'Prevention and Investigation of Phishing at Individual, Organization and Critical Infrastructure Levels' विषय पर वेबिनार आयोजित करने के लिए बीपीआरएंडडी के प्रयासों और कानून प्रवर्तन एजेंसियों की सुविधा के लिए इसकी कार्यवाही प्रकाशित करने की सराहना करता हूँ।

मैंने 'Prevention and Investigation of phishing at Individual, Organization and Critical Infrastructure Levels' विषय पर वेबिनार की कार्यवाही का अवलोकन किया और यह पाया कि साइबर अपराधों का सामना करने में शामिल सभी एजेंसियों के लिए यह प्रासंगिक और सूचनात्मक है।

मैं, श्री बालाजी श्रीवास्तव, महानिदेशक, पुलिस अनुसंधान एवं विकास ब्यूरो एवं उनकी टीम को इस उत्कृष्ट पुस्तक के प्रकाशन के लिए बधाई देता हूँ और आशा करता हूँ कि यह प्रकाशन साइबर अपराधों को रोकने के प्रयास में महत्वपूर्ण भूमिका प्रदान करेगा।

(अमित शाह)

कार्यालय : गृह मंत्रालय, नॉर्थ ब्लॉक, नई दिल्ली-110001

दूरभाष : 23092462, 23094686, फ़ैक्स : 23094221

ई-मेल : hm@nic.in

नित्यानन्द राय
NITYANAND RAI



सत्यमेव जयते



आज़ादी का
अमृत महोत्सव

गृह राज्य मंत्री
भारत सरकार
नार्थ ब्लॉक, नई दिल्ली – 110001

MINISTER OF STATE FOR
HOME AFFAIRS
GOVERNMENT OF INDIA
NORTH BLOCK,
NEW DELHI - 110001



संदेश

मुझे यह जानकर खुशी हो रही है कि पुलिस अनुसंधान एवं विकास ब्यूरो, नई दिल्ली में स्थापित National Cyber Crime Research and Innovation Center (NCR&IC) साइबर अपराधों कि रोकथाम, उनका पता लगाने, उनके नियंत्रण और जांच पर केन्द्रित अनुसंधान और उन्नयन के क्षेत्र में प्रमुख हितधारकों के साथ साझेदारी करने के अपने अधिदेश को पूरा करने में सक्रिय रूप से कार्य कर रहा है।

कानून प्रवर्तन एजेंसियों को नवीनतम तकनीकों का लाभ प्रदान करने के अपने अधिदेश को पूरा करने के लिए, NCR&IC कानून प्रवर्तन एजेंसियों के लाभ हेतु साइबर सुरक्षा पर प्रासंगिक विषयों पर नियमित रूप से वेबिनार आयोजित कर रहा है और इसके व्यापक प्रसार के लिए पुस्तिका के रूप में वेबिनार कि कार्यवाही प्रकाशित कर रहा है। तेज़ी से बदलते हुए साइबर अपराध के परिदृश्यों को देखते हुए NCR&IC कि यह ज़िम्मेदारी और अधिक महत्वपूर्ण हो जाती है।

मैं 'Prevention and Investigation of Phishing Frauds at Individual, Organization and Critical Infrastructural Levels' विषय पर कानून प्रवर्तन एजेंसियों के लिए वेबिनार आयोजित करने और संदर्भ के लिए एक पुस्तिका के रूप में वेबिनार की कार्यवाही प्रकाशित करने के लिए बीपीआरएंडडी में NCR&IC की सरहना करता हूँ, जो निश्चित रूप से साइबर अपराध से सामना करने में लगे पुलिस कार्मिकों को लाभान्वित करेगा।

मैं इस महत्वपूर्ण एवं उपयोगी प्रकाशन के लिए श्री बालाजी श्रीवास्तव, महानिदेशक, पुलिस अनुसंधान एवं विकास ब्यूरो और उनके सक्षम अधिकारियों की टीम को बधाई देता हूँ।

नई दिल्ली।

25 मार्च 2022

(नित्यानन्द राय)

Office Tel.: 011-23092870, 23092595, FAX No. : 011-23094896

अजय भल्ला, भा.प्र.से.
AJAY BHALLA, IAS



75
आज़ादी का
अमृत महोत्सव

गृह सचिव
Home Secretary
भारत सरकार
Government of India
नार्थ ब्लॉक / North Block
नई दिल्ली / New Delhi



MESSAGE

I congratulate the entire team of National Cyber Crime Research and Innovation Center (NCR&IC), and the enabling leadership of the Bureau of Police Research and Development (BPR&D) for conducting regular webinars on crucial topics with regard to cyber crime prevention and investigations.

2. The Ministry of Home Affairs, Government of India, has set up the Indian Cyber Crime Coordination Centre, I4C, under which seven distinct verticals are working towards crucial leads, like reporting of cyber crimes, capacity building of law enforcement agencies, cyber threat intelligence, research based solutions for investigations, etc., to bolster the fight against cyber crimes.

3. The themes of the webinar, “Prevention and Investigation of Phishing Frauds at Individual, Organization and Critical Infrastructure Levels” is one of the crucial topics in the present scenario. The proceedings of the Webinar make a very interesting and informative read. I urge the law enforcement agencies to make use of the proceedings as a ready reference to deal with cyber crime and utilize the expertise of the NCR&IC to respond effectively to this menace.

Place : New Delhi

Dated : 30.03.2022

(Ajay Bhalla)

बालाजी श्रीवास्तव, भा.पु.से.
महानिदेशक

Balaji Srivastava, IPS
Director General

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE

National Cyber Crime Research and Innovation Centre (NCR&IC) established at BPR&D is spearheading research and innovation in the area of Cyber Security in collaboration with academia, industry and Law Enforcement Agencies (LEAs) across India. NCR&IC has been striving continuously to augment the capacity of LEAs in their fight against modern day cases of Cyber Crime.

NCR&IC hosts series of webinars regularly on different emerging topics related to current trends in Cyber Crime Investigation for LEAs across India. In this sequence, the 4th webinar on the theme "Prevention and Investigation of Phishing Crimes at Individual, Organization and Critical Infrastructure Levels" organized on 18th January, 2022 at BPR&D, New Delhi was attended by several officers from State/UTs, CAPFs and CPOs. They should have benefited immensely from the deliberations.

The proceedings of the Webinar make a very informative reading. I must appreciate the hard work put in by Team NCR&IC in compiling the same.

(Balaji Srivastava)

"Promoting Good Practices and Standards"

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781344 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE


The Modernisation Division of the BPR&D has stayed true to the Bureau's tradition of keeping the flame of knowledge alit by facilitating frequent engagement with stakeholders across India. Publishing proceedings of the Webinar held earlier (January 18, 2022), deliberating issues relating to Phishing Crimes, shall further expand the reach of the wit and wisdom of domain experts who participated in the sessions.

I was reading an article sometime back where the author surmised that it was easy to get lost in cyberspace. He suggested that the cyber-world, looked different to the different people engaging with it: For a student, cyberspace could be a place to acquire knowledge and interact with peers; for a business, a place to make money, and for those working on the national security grid, cyberspace could well be a war zone-a place where the enemy reconnoiters weaknesses of the target before delivering weaponised content.

In view of its mischief potential, the world at large remains deeply concerned about a potential cyber and phishing attack. As frontline workers on the cyber front, the policing community is positioned right in the centre of the zone of response and responsibility, and cannot afford to remain ignorant, or, what's worse, make do with half-truths. Facing up to the risks, is the only way to make sure the communities we serve, realise the promise of the cyber world, and not its perils. The Modernisation Division, led by Director, Dr. Karuna Sagar, is seeking to bridge the gap by reaching out to the remotest corners of the country, through this publication.

It is in that spirit of hope and engagement that we present to our patrons and colleagues, the fruit of our deliberations on the subject, wishing that it will help sensitise and enhance, the scope and depth of understanding of professional concerns relating to phishing.

Happy Reading!



(Neeraj Sinha)

“Promoting Good Practices and Standards”

डॉ. करुणा सागर, भा.पु.से.
महानिरीक्षक / निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

EXECUTIVE SUMMARY

To deal with modern age Cyber Crime in India, in a coordinated and effective manner, Ministry of Home Affairs, Government of India has rolled out an umbrella Scheme "Indian Cyber Crime Coordination Centre (I4C). National Cyber Crime Research and Innovation Centre (NCR&IC) is one of the seven verticals under the Indian Cyber Crime Coordination Centre (I4C) which is functioning in the Bureau of Police Research and Development (BPR&D) with the aim of Innovation and Prevention of various types of Cyber Crime.

The cases of Cyber Crimes especially the Phishing Crime incidents are increasing at an alarming rate. There is a need to evolve effective strategies for prevention and investigation of cases related to Phishing Crime taking place at various levels i.e., Individual, Organizations and Critical Infrastructure Levels.

With this goal, NCR&IC organized a National level Webinar on "**Prevention and Investigation of Phishing Crimes at Individual, Organizations and Critical Infrastructure Levels**" from 11 AM to 1:15 PM on January 18, 2022 at the BPR&D Headquarters, New Delhi. More than 235 Police Officials from CAPFs, CPOs and other Police Forces from States/UTs attended the webinar.

The webinar was addressed by eminent subject matter experts from Academia, Industry and Law Enforcement Agencies. The webinar offered three different perspectives for Prevention and Investigation of Phishing Crimes at Individual, Organizations and Critical Infrastructure Levels, to the Law Enforcement Officers.

Sh. Neeraj Sinha, ADG, BPR&D opened the Webinar with his welcome address wherein he highlighted about the emerging challenges in cyber space for law enforcement agencies and gave examples that how the Phishing Crime is a huge challenge before LEAs and lot of scope is there for research and innovation for effective prevention and detection of Phishing Crimes.

Sh. Balaji Srivastava, DG, BPR&D delivered his inaugural address. He informed the participants that NCR&IC is one of the seven verticals of Indian Cyber Crime Coordination Center (I4C) Scheme. Due to rapid advancement of communication technology and internet, the Criminals are more focused towards the Phishing Crime now a days. Phishing attacks are not only targeted on Individuals but

"Promoting Good Practices and Standards"

also on Organization and Critical Infrastructure levels. Therefore, it is our responsibility to upskill ourselves and keep ourselves up-to-date with latest innovation and technology to deal with modern day Phishing.

Mr. Manoj Abraham, ADG, Kerala Police & Nodal Officer CyberDom, Kerala, started his talk by sensitizing the participants about the gravity of phishing crimes. He explained various categories of phishing crimes i.e., Phishing, Deceptive Phishing, Spear phishing, Vishing, Smishing, Pharming etc. He also elaborated the difference between Physical crime scene investigation and digital crime scene along with the concept of chain of custody, investigation process, Seizure memo and seizure proceedings. He emphasized on the issue of lack of integrity in the process of custody. He also suggested some forensic tools for effective Cyber Crime Investigations to LEAs.

Dr Puneet Goyal, Assistant Professor, Computer Science and Engineering, IIT Ropar, highlighted the fundamental task in cyber security and how hard AI is a new paradigm in ensuring security. He gave examples of how various types of CAPTCHA are being implemented by institutions like IRCTC to ensure security. He explained the limitations of text-based CAPTCHA methods, that may be overcome by use of Image based CAPTCHA. Further, he emphasized on the more secure CAPTCHA, i.e., handwriting CAPTCHAs (H-CAPTCHAs). Dr. Goyal also proposed various technological measures against phishing attacks, such as, Anti-Phishing Plugin/ Browser Add on, Machine-level tools, NLP techniques, Using SSL certificates, Secret images and Social Campaigns/User Education.

Sh. Sanjeev Relia, Senior Advisor Cyber Security - Tracelay, Bangalore, Alea Asia, New Delhi and SenseLearner Technologies – Noida, delivered his talk focused on various phishing attacks and threats to the Critical Information Structure. He gave examples of various incidents of Phishing attacks on Critical Information Infrastructures (CII). He briefly explained, why there is a threat to Critical Information Infrastructure. He also mentioned about the one of the important CII of India, National Critical Information Infrastructure Protection Centre (NCIIPC). The main threats to Critical Information Infrastructure includes, Espionage, Subversion and Sabotage. Sh. Relia suggested tentative solutions to deal with the Phishing attacks on the Critical Infrastructures.

The officials participating in the webinar had got a great prospect to learn and upgrade their knowledge in Prevention and Investigation of Phishing Crimes at Individual, Organizations and Critical Infrastructure Levels. They actively took part in Q&A sessions followed by each talk and enriched their awareness. Overall, it was an interactive and informative webinar about various perspectives for prevention and investigation of new age Phishing Crimes.



(Karuna Sagar)

CONTENTS

1	Webinar Agenda	2
2	Proceedings	3
3	Session – I	6
4	Session – II	13
5	Session – III	37
6	References	45
7	Contact List of BPR&D officers	46



AGENDA

Objective of Webinar: To provide an interactive session for Law Enforcement Agencies on emerging cybercrimes, new techniques and methodologies for investigation, prevention and modern-day challenges.

Time	Sessions
11:00 AM-11:05AM	Welcome Address - ADG, BPR&D
11:05 AM -11:10AM	Inaugural Address - DG, BPR&D
11:10AM-11:40AM	<i>Session 1:</i> Sh. Manoj Abraham, IPS, ADG, Kerala Police Topic – Latest Tools and Methods to Investigate Phishing Crimes
11:40 AM-11:50 AM	Q&A - Session 1
11:50 AM-12:20 PM	<i>Session 2:</i> Dr. Puneet Goyal, Assistant Professor, IIT Ropar Topic – Preventing Phishing Attacks: Hard AI Problems based Novel and Adaptive Approach
12:20 PM-12:30 PM	Q&A - Session 2
12:30 PM-01:00 PM	<i>Session 3:</i> Sh. Sanjeev Relia, Senior Advisor Cyber Security - Tracelay, Bangalore, Alea Asia, New Delhi and SenseLearner Technologies - Noida Topic – Phishing Attacks: Threat to National Critical Infrastructure
01:00 PM-01:10 PM	Q&A - Session 3
01:10 PM-01:15 PM	Vote of Thanks - IG (Mod)



PROCEEDINGS

National Cybercrime Research and Innovation Center (NCR&IC), a vertical of Indian Cybercrime Coordination Center, MHA, is deployed at Bureau of Police Research & Development, New Delhi.

In order to provide a platform where LEAs from across the country can learn about emerging cyber security and cyber crime challenges from top cyber security experts, NCR&IC has decided to organize a series of monthly webinars.

The fourth webinar on the theme "Prevention and Investigation of Phishing Crimes at Individual, Organization and Critical Infrastructure Levels" was organized on 18th Jan 2022 at BPRD HQs, New Delhi through WebEx. More than 235 participants from all States/UTs, CAPFs and CPOs participated in the webinar.

Following are three esteemed speakers one each from LEAs, industry and academia who delivered their talks:

1. **Sh. Manoj Abraham,**
ADG, Kerala Police & Nodal Officer CyberDom, Kerala
2. **Dr. Puneet Goyal,**
Assistant Professor, IIT Ropar
3. **Sh. Sanjeev Relia,**
Senior Advisor Cyber Security - Tracelay, Bangalore

Dr. Karuna Sagar, IG/Director (Mod), BPR&D started the proceedings of the webinar by welcoming Sh. Balaji Srivastava, DG, BPR&D, Sh. Neeraj Sinha, ADG, BPR&D at the event.

ADG, BPR&D delivered his welcome address by welcoming all the participants and the distinguished speakers. He expressed his compliments to the NCR&IC team, Modernisation Division and DIG (Mod) for organizing webinar on important topics of cyber crime investigation and digital forensics.

He said that according to scholars of cyber space, it is very easy for an individual to get lost in cyberspace. He further quoted an author that cyber space created by engineers and populated by masses looked different to every individual or group that interacted with it. For a student, cyber space could be a place to acquire knowledge, engage with peers, for a business a place to make money, for those working on the national security grid cyberspace could be a place where an enemy identifies the weakness of the target and launches weaponised content. He further mentioned about an essay published in a renowned foreign policy journal two authors Raj Shah and Kiran Sridhar have estimated that firms with 1000 employees spent an average of over 13 million dollars on cyber defense in the year ending 2021. These figures indicate a nearly 200 percent escalation in spending on cyber defense by private firms in a period of just two years. This indicates how much concerned the world has become about cyber crimes and phishing attacks. While emphasizing the potential damages phishing attacks can cause on organizational level, Sh. Neeraj Sinha cited the example of Dr. Reddy's, a covid-19 vaccine manufacturer



was forced by a ransomware attack to nearly shut down critical plants in nearly five countries. A cyber criminal was able to steal 6 million dollars in cryptocurrency held on the poly network exchange. This sequel had an interesting twist that the thief referred to by the company as Mr White Hat returned back all he had taken and claimed that he had done it merely to showcase its security vulnerabilities. This incident indicates that all of us who operate in cyber space should be aware about the vulnerabilities our system may be exposed to. The need to be self-aware and guard against cyber vulnerabilities has never been greater than today. The policing community cannot afford to remain ignorant.

Sh. Neeraj Sinha, ADG, BPR&D concluded his address by urging all participants to gain knowledge and wisdom from the distinguished speakers.

Sh. Balaji Srivastava, IPS, DG, BPR&D started his inaugural address by welcoming the move of NCR&IC, Modernisation Division of the Bureau to conduct this crucial webinar at the beginning of a new year.



He told the participants that NCR&IC is a crucial vertical of Indian Cyber Crime Coordination Center (I4C), an umbrella scheme of the Ministry of Home Affairs, Govt of India. In collaboration with leading academic and research institutions such as IITs, NITs and IIITs, the NCR&IC is developing many useful Technological Solutions for Central and State Police Organisations, in varied domains of Cyber Forensics, Cyber Crime Investigation and Prevention of Cyber Crime, employing cutting edge technologies. The NCR&IC also envisions harnessing the vast potential of the rapidly growing Start-up Ecosystem in the country and many bright young researchers are already part of our mission.

DG, BPR&D further told that NCR&IC has the mandate to track emerging technological developments, to proactively predict potential vulnerabilities - which can be exploited by cyber criminals and to strengthen the cybercrime handling capabilities of LEAs. He appreciated the topic of the webinar, as cyber experts point out that the first step in cybercrimes is phishing attacks. Checking Phishing attacks in the beginning itself, will definitely help the LEAs in preventing other serious cybercrimes such as cyber stalking, cyber bullying, ransomware attacks, DDoS attacks and banking frauds etc. It is therefore essential that as police officers, we equip ourselves adequately to tackle this menace.

DG, BPR&D further mentioned that NCR&IC had conducted Capture the Evidence (CTE) Contest on the theme of “Data Breach” and a grand Cyber Awareness Quiz, which was attended by more than 700



Cyber Crime investigating Police Officers in the country. He apprised the participants that NCR&IC had planned more such events in the future. He urged all the participants to attend all such events, focused on emerging technologies and concerns of cyber security.

He mentioned that in order to provide the advanced technological solutions to LEAs to augment their fight against cyber crime, NCR&IC has initiated several R&D projects in partnership with the country's premier research institutions. These ongoing projects are expected to provide research based solutions employing cutting edge technology for LEAs.

DG, BPR&D went on explaining that the technological landscape of the world is changing very rapidly. The drivers of the ongoing 4th Industrial Revolution such as Artificial Intelligence (AI), Machine Learning (ML), Cloud Computing, Internet of Things (IoT), Blockchain, Drones, Augmented Reality and Virtual Reality (AR-VR) and now the Metaverse are fast transforming our lives in every possible way. Concomitant to this sweeping metamorphosis in the cyber space are the vulnerabilities of individuals, organisations and the government establishments particularly Critical Cyber Physical/Information Infrastructure such as Power Grid, Transports, Financial System etc. According to Global Risks Report 2022, recently released by the World Economic Forum (WEF), the 'heightened cyber risks' is among top five threats being faced by the world today.

DG, BPR&D emphasized the challenges of tackling cybercrime in the present scenario. The ever growing mobile usage in our cities and rural hinterland and increasing footprints of internet users in social media have brought forth a new challenge of digital literacy. The gap in awareness of new technology and related services among the vast population is being increasingly exploited by the cyber criminals taking advantage of the anonymity available in the cyber space - particularly in the dark and deep web. With this backdrop, it is extremely challenging to protect gullible internet users from the multitude of online threats such as Cyber fraud, Social engineering, Phishing and Ransomware etc.

New chapters of technological evolution are unfolding at a breakneck speed along with their associated complexities and vulnerabilities. In this situation, even the best of the cyber security systems cannot shield us completely from the scourge of online threats. While sustained awareness is the key to any cyber security system in place, there should be emphasis on both prevention and mitigation of cyber crimes. Undoubtedly the paradigm of Sustainable Security should go hand in hand with Sustainable Development and only then, can we realize the true objectives of Atma Nirbhar Bharat and Surakshit Bharat.

This webinar has been conceived to leverage the strength and expertise of all stakeholders, and to create strategic partnerships in the areas of research and innovation, focused on fighting cyber-crimes, cyber crime impact containment and cyber crime investigations. DG, BPR&D urged all the participants from across the country to actively interact with the BPR&D and give their valuable feedback to enable the Bureau to fully utilize the potential of NCR&IC by synergising its functioning with the requirements of Law Enforcement Agencies.

DG, BPR&D complimented the NCR&IC team in my Bureau under the guidance of the Director (Modernization) for organizing this very important webinar.

DG, BPR&D said that he was sanguine that the deliberations in this webinar will give all of you valuable insights on how to prevent and investigate Phishing crimes. This webinar should broaden your horizon with the knowledge of the latest modus operandi of such criminals and equip you with innovative tools and technologies to tackle it effectively.

Brig. Navrattan Joshi (Retd.), Principal Scientific Officer, BPR&D moderated the event.

SESSION 1

Topic: **Tools & Methods to Investigate Phishing Crimes**

Speaker: **Sh. Manoj Abraham,**

ADG, Kerala Police & Nodal Officer CyberDom, Kerala



Mr. Manoj Abraham started his talk by sensitizing the participants about the gravity of phishing crimes. He explained various categories of phishing crimes:

- Phishing
- Deceptive Phishing
- Spear phishing
- Vishing
- Smishing
- Pharming

He also elaborated the difference between Physical crime scene investigation and digital crime scene.

He discussed the process of digital forensic investigation as follows -

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

Afterwards he gave a brief about the operation falcon in which GIB helps INTERPOL identify Nigerian BEC ring members.

Sh. Abaraham discussed the crime scene investigation as follows -

- Identifying and securing the crime scene
- Documentation of the scene of offense



- Collection of evidence
 - » Gathering evidences from Switched-off Systems
 - » Gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labeling and, documenting of the evidence
- Packaging, and transportation of the evidence

After that they have described the Seizure memo and seizure proceedings. The legal provisions empowering the IOs to conduct search and seizure are provided under Section 165 Cr PC and Section 80 of the IT Act 2008.

During the crime scene investigation following points should be remembered:

- Make sure one of the technical people from the responder side along with two independent witnesses are part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.
- The notes made during the pre-investigation assessment should be used for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment at the scene of crime.

Sh. Abraham described the chain of custody in detail as Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence.

He went on to discuss the Lack of integrity in the process of custody and, absence of appropriate documentation in this regard, will not only be detrimental to the cyber crime investigation, during trial but also, expose the IOs to criminal liability under Section 72 of the ITAA 2008.

It is a very critical document and it must be maintained properly during the crime scene investigation, Investigator must ensure it.

They have talked about the forensic Artifact for analyzing the data at initial level, the cyber forensic expert should know all the relevant Artifact of the suspected computer system and also he should enhance the knowledge of the Attackers which will help to investigate the cyber crime.

He has shared his experience with LEAs. The Investigation officer should create a database of clues such as domains, nicknames, accounts on hacker forums, and phone numbers to find patterns along with the Open source intelligence (OSINT) to merge a long chain leading from the original phishing attack to a specific person or a group. Also he has suggested the Network graph analysis tools for connecting the clues with each other for better graphical representation.

He also suggested that all the connections, whatever was found during the investigation must be validated by way of following steps -

- To create a chain of links from phishing activity to specific people.
- Even if the investigation identifies a specific person, keep looking for additional independent

information to prove their involvement.

- After confirming your hypotheses with both digital and physical information, successfully identify the attacker.

After identifying the criminal as per the applicable law. If the attacker is living in the same country. If not and if the countries don't have extradition treaties, there is no way to arrest the criminal. Without effective cross-border cooperation, it is impossible to bring hackers/ criminals to justice.

He also suggested some forensic tools for the cyber crime investigators as follows -

- PALADIN
- CAINE
- X-Way Forensic
- Autopsy
- Wireshark
- NetworkMiner
- SIFT Workstation
- ProDiscover Forensic
- Volatility Framework
- Oxygen Forensic Suite
- XRY
- Xplico

Each tool has its own capability and applications. Sh. Abraham advised the investigators to read the detailed information of each tool and get hands-on.



Deceptive Phishing



Most common type
Email from recognized sender
Steals info by imitating a legitimate provider

Users should inspect URLs carefully
Check for legitimate redirection
Look out for:
Generic salutations
Grammar mistakes
Spelling errors



Spear Phishing



Most common on social media sites
Email from recognized sender
Uses personalised information

Employee security awareness training
Limit sharing sensitive personal information
Invest in automated solutions to analyze emails



CEO Fraud



Targets executives
Used to authorise fraudulent financial transfers
Obtain W-2 information on all employees

Executive training
Setting up multi-factor authentication for financial transactions



Vishing




Contacts targets by telephone
Mimics known entities to steal sensitive data / funds

Avoid calls from unknown numbers
Don't give personal information over the phone
If in doubt call entity back on a known number




Smishing




Contacts targets by SMS / text message

Mimics known entities to steal sensitive data / funds

Research unknown numbers
 If in doubt call entity back on a known number



Pharming




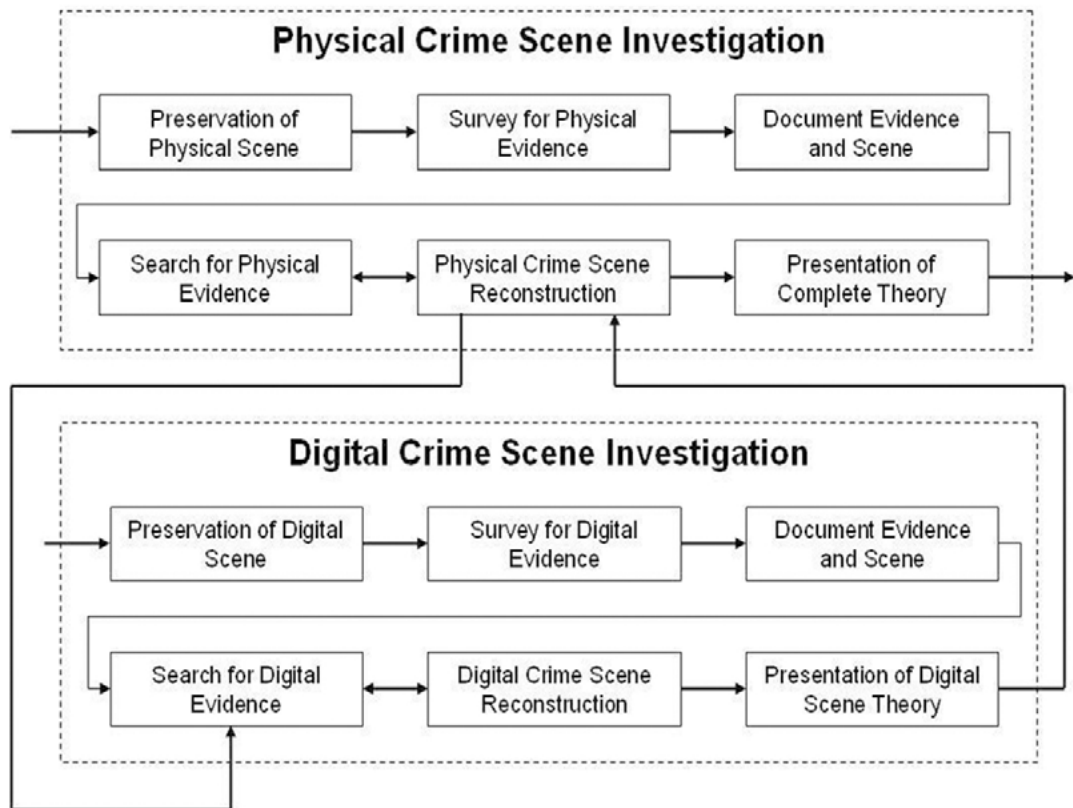
Leverages cache poisoning against DNS

Changes IP address associated with a website name

Redirects to a malicious website

Only use HTTPS protected sites
 Use regularly updated anti-virus software
 Keep security upgrades updated







Crime Scene Investigation: Search & Seizure



Steps in Crime Scene Investigation

- Identifying and securing the crime scene
- Documentation of the scene of offence
- Collection of evidence
 - Gathering evidences from Switched-off Systems
 - Gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labeling and, documenting of the evidence
- Packaging, and transportation of the evidence

Seizure Memo and Seizure Proceedings

The legal provisions empowering the IOs to conduct search and seizure are provided under Section 165 Cr PC and, Section 80 of the IT Act 2008



Make sure one of the technical people from the responder side along with two independent witnesses are part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.

The notes made during the pre-investigation assessment should be used for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment at the scene of crime.

Chain of custody

- Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence, and so on.
- Lack of integrity in the process of custody and, absence of appropriate documentation in this regard, will not only be detrimental to the cyber crime investigation, during trial but also, expose the IOs to criminal liability under Section 72 of the ITAA 2008



Sh. Manoj Abraham ended his talk with a brief session of open Q&A.

SESSION 2

Topic: **Preventing Phishing Attacks: Hard AI Problems based Novel and Adaptive Approach**

Speaker: **Dr Puneet Goyal,**

Assistant Professor, Computer Science and Engineering, IIT Ropar



Dr Goyal started his talk by explaining the fundamental task in cyber security and how Hard AI is a new paradigm in ensuring security. He gave examples of how various types of captcha are being implemented by institutions like IRCTC to ensure security.

He went on to explain that CAPTCHA, a web protection mechanism, is an automated public test employed to distinguish between humans and robots. It helps prevent automated attacks by bots. Bots may be responsible for eating up all the resources and to publish biased results.

Dr. Goyal explained the limitations of text based CAPTCHA methods and said that image based CAPTCHAS are an advanced form presently employed by software companies to ensure security. Computer vision techniques have successfully broken the text based CAPTCHAs, thus making those systems who employ it vulnerable.

Alternatively, if more noise is added to the image CAPTCHAs then it becomes even harder for humans to understand them. This prevents the accessibility of the system for human users. Natural image based CAPTCHAs are hard to attack hence they provide more security to the system. But visual CAPTCHAs has following challenges:

- Relies on recognition of non character objects.
- They are machine unsolvable to even unsolvable by both - Humans and Machines

More difficult ones are handwriting CAPTCHAs. They are called H-CAPTCHAs and the motivation behind them is that machine recognition of handwriting is more difficult than printed text. This makes the systems more secure. However, H-CAPTCHAs are unexplored by the research community.

Dr Goyal further shed some light on the new research avenues of developing advanced stage CAPTCHAs. Text detection in natural scenes is another area which may provide a robust CAPTCHA solution. Deep Learning Models have replaced the manual search and design for patterns and features. This area



carries a potential where generating distinct CAPTCHAs based on text detection in natural scene may become easier and faster. The challenges in this area as follows:

- Focus is only on English. So non-English speakers may find little or no utility.
- Robustness/Cross-dataset/Use of Synthetic Dataset
- Efficiency/Real time detection

The next topic of Dr Goyal's talk revolved around phishing attacks and the technological response to it.

He explained that phishing is a form of identity theft in which criminals build replicas of target websites and lure unsuspecting victims to disclose their credentials or sensitive information.

According to RSA Cyber crime and symantec reports 2019 phishing leads to several billion dollar losses to global organizations every year. Moreover, according to Anti-Phishing Working group (APWG) reports 2019 phishing attacks have been surging with an annual growth rate more than 97%. Losses to the US economy range from \$61 million to \$3 billion.

Very recently, SBI released a customer warning that close to 2 million users may be at risk of phishing attacks.

Dr. Goyal showed some glaring examples of phishing websites. He explained the phishing information flow:

Phishing information flow has three components:

- Mail Sender: sends large volume of fraudulent emails
- Collector: collect sensitive information from users
- Cashier: use the collected sensitive information to encash

Further, Dr. Goyal explained various types of phishing attacks. One popular phishing attack is Man In The Browser/Man in The Middle Attacks. These attacks take advantage of vulnerabilities to inject code into the browser when you visit a specific site. This allows the hacker to do a variety of things including capturing information entered into fields on the website, adding fake fields to steal information or login credentials, or even gain control of the user's device.

Dr. Goyal proposed following technological measures against phishing attacks.

1. User-level Anti-phishing approaches
 - a. Anti Phishing Plugin/Browser Add on
2. AI based phishing detection approach
 - a. Applying ML tools on feature extracted from Email content/URL etc
 - b. NLP techniques
3. Enterprise level anti phishing approach
 - a. Using SSL certificates
 - b. Secret images
4. Social Campaigns/User Education



- a. User awareness seminars
- b. Simulated phishing attacks

World's renowned magazine Forbes mentioned in 2014 that even after a decade of anti phishing efforts, phishing attacks were on rise. Phishing is a “technological medium to exploit human weakness” and that technology alone cannot fully compensate for human weaknesses.

Dr. Goyal shed some light on the role of SSL in securing the website and its technological limitations.

- SSL certificates ensure data on a website is being submitted in a secure manner, but they do not guarantee the site itself is safe. Because of this, hackers are taking advantage of buying cheap SSL certificates and using them on phishing websites to appear legitimate.
- HTTPs are also not secure enough

Dr. Goyal proposed a Hard AI based enterprise level solution. Overview of Proposed Security Approach is as follows:

- Enhance security against Phishing/MitB attacks using Multimedia Content Set Particular to User (MCSPU) and user specified parameters
- For transaction confirmation, Bank would use a randomly selected image from ISPU, embedded with the critical text having properties as per User Specified Parameters.
- Banks may also intentionally respond at times with incorrect (non-user specific) image embedded with correct text that legitimate user must not confirm or else put in honeypot.

While explaining the advantage of Hard AI based solution over the normal CAPTCHA is that text appearing in the generic image is unknown to the user whereas MCSPU image shows the text provided by the user itself. So the text embedded in the proposed solution is according to the user specified parameters. Further, several CAPTCHA breaking tools are available today, making the system vulnerable to phishing attacks, whereas breaking the MCSPU based solution is harder as on date.

Dr. Goyal concluded his talk by emphasizing on the need that instead of reactive approach, the world today needs proactive approach to tackle growing menace of phishing attacks. He said that the ultimate goal is to adapt systems to an evolving threat landscape, which includes both new and known threats.



WWW

NCR&IC WEBINAR | 8-Jan-2022 BPR&D, Ministry of Home Affairs, New Delhi

Preventing Phishing Attacks: Hard AI Problems based Novel and Adaptive Approach



Puneet Goyal

Faculty, CSE, IIT Ropar

puneet@iitrpr.ac.in

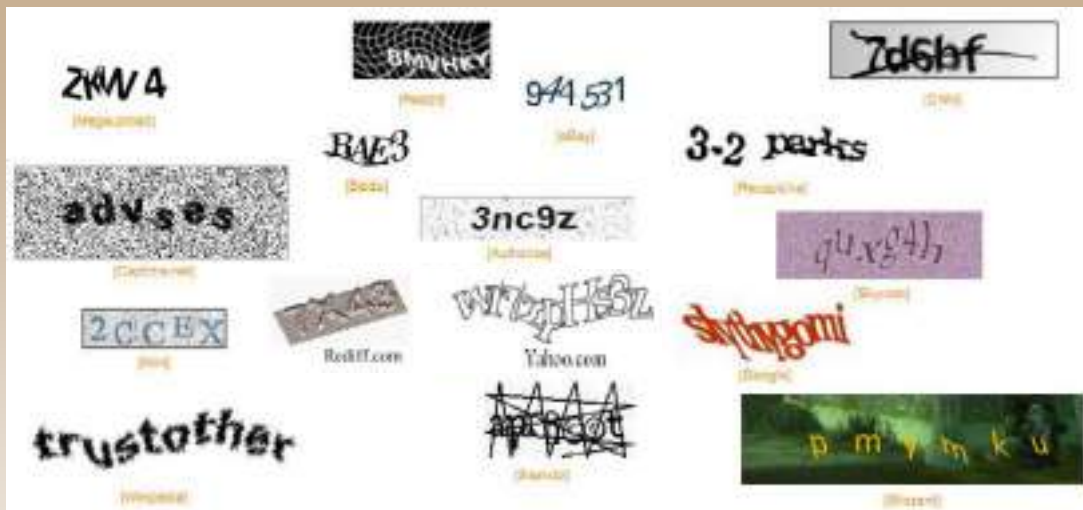
pgoyal@alumni.purdue.edu

<http://cse.iitrpr.ac.in/dr-puneet-goyal>

Introduction

- **FUNDAMENTAL TASK in Security**
 - ◆ Creating cryptographic primitives based on hard mathematical problems that are computationally intractable
 - » Example: Problem of Integer factorization in RSA
- Using **hard AI (Artificial Intelligence)** is still an exciting new paradigm
 - ◆ Most notable primitive - CAPTCHA

CAPTCHA



IRCTC uses CAPTCHAs of varying complexity at different times and at different stages

Image Recognition CAPTCHA



<http://designmodo.com/>



<http://webdevelop.com/>

Background on CAPTCHA

- **Completely Automated Public Test to Tell Computers and Humans Apart.**
- Web-based protection mechanisms
- Only humans allowed to perform certain tasks`
 - ◆ Opening E-mail accounts, Net Banking, eCommerce, etc.
- Prevent automated attacks by **bots**
 - ◆ To avoid *eating up resources*
 - ◆ To avoid biasing results, etc.

1. L. von Ahn et al., *CACM*, 2004.
2. The CAPTCHA Project – <http://www.captcha.net>

Why IMAGE based CAPTCHA

- Computer vision techniques^{1,2,3} have broken text-based CAPTCHAs
 - ◆ Over 90% accuracy
 - ◆ Makes these systems vulnerable
- Alternatives
 - ◆ More noise – harder for humans too
 - ◆ Natural image based CAPTCHAs
- Present an image to the user
 - ◆ User labels content
- Hard to attack
 - ◆ Image recognition is a hard problem
 - ◆ Hence more secure CAPTCHAs !



Image-based CAPTCHAs

(Courtesy: The Captcha Project, CMU)

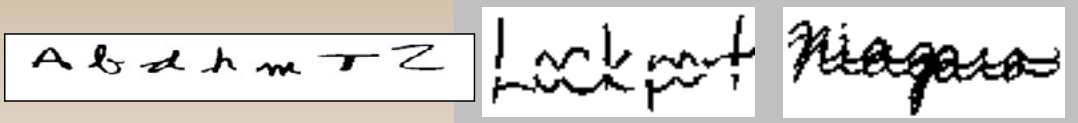
1. G. Mori et al., *CVPR*, 2003.
2. A. Thayananthan et al., *CVPR*, 2004.
3. G. Moy et al., *CVPR*, 2004.

VISUAL CAPTCHA and Challenges

- **Text CAPTCHA**
 - Relies on character recognition
- **Image Recognition CAPTCHA**
 - Relies on recognition of non-character objects
- Multi label classification problems are considered much harder than binary classification
- Machine Unsolvable to Unsolvable by both – Humans and Machines
- Relay attacks – CAPTCHA challenges are relayed to human solvers

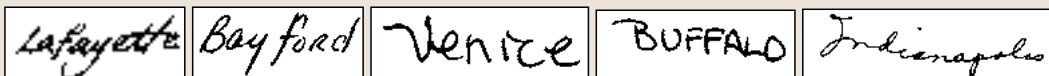
H-CAPTCHA (Rusu et al. HIP 2005) Visual CAPTCHA with Handwritten Image Analysis

Develop CAPTCHAs based on the ability gap between humans and machines in handwriting recognition using Gestalt laws of perception



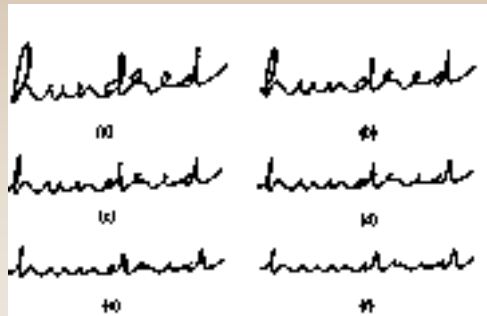
Generation of random and infinite many distinct handwritten text images

- Use handwritten word images that current recognizers cannot read
 - Handwritten US city name images available from postal applications
 - Collect new handwritten word samples



Generation of random and infinite many distinct handwritten text images

- Use handwriting distorter for generating “human-like” samples
- Models that change the trajectory/shape of the letter in a controlled fashion (e.g. Hollerbach’s oscillation model)



Original handwritten image (a). Synthetic images (b,c,d,e,f).

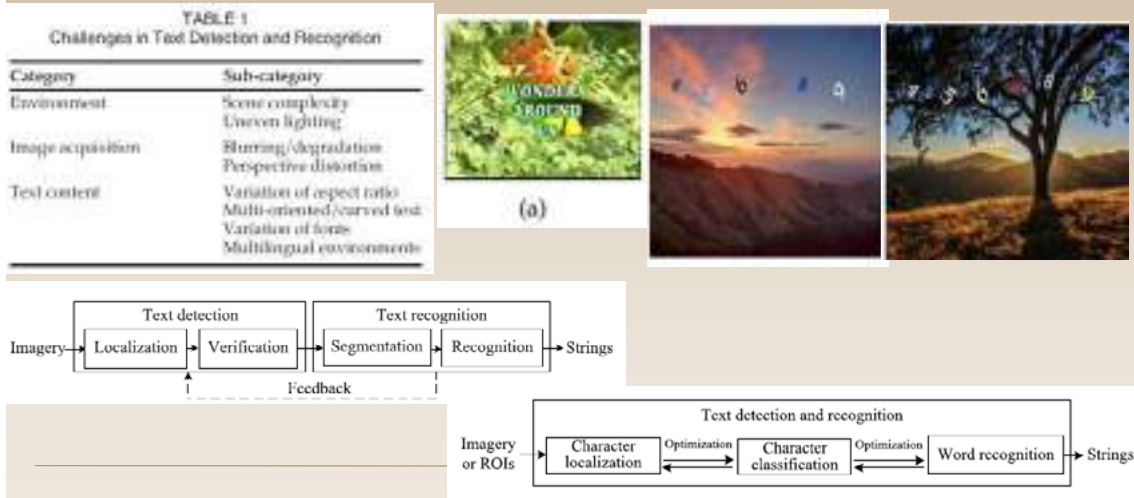
H-CAPTCHA Motivation

- **Machine recognition of handwriting is more difficult than printed text**
- **Handwriting recognition is a task that humans perform easily and reliably**
- **Several machine printed text based CAPTCHAs have been already broken**
 - Greg Mori and Jitendra Malik of the UCB have written a program that can solve Ez-Gimpy with accuracy 83%
 - Thayananthan, Stenger, Torr, and Cipolla of the Cambridge vision group have written a program that can achieve 93% correct recognition rate against Ez-Gimpy
 - Gabriel Moy, Nathan Jones, Curt Harkless, and Randy Potter of Areté Associates have written a program that can achieve 78% accuracy against Gimpy-R
- **Speech/visual features based CAPTCHAs are impractical**
- **H-CAPTCHAs thus far unexplored by the research community**
- **Challenges**
 - ♦ Controlling distortion
 - ♦ Quantifying and exploiting the weaknesses of state-of-the-art handwriting recognizers and OCR systems

Text Detection in Natural Scene Images

The gap between the technical status and the required performance indicates that text detection and recognition remain unsolved problems. While great progress has been made there are still numerous research opportunities.

- Qixiang and Doermann, Text Detection and Recognition in Imagery: A Survey, IEEE Trans Patt Analy. & Mach. Intell. 2015



Scene Text Detection and Recognition: Deep Learning Era

Long, He and Yao, *International Journal of Computer Vision*, 2021

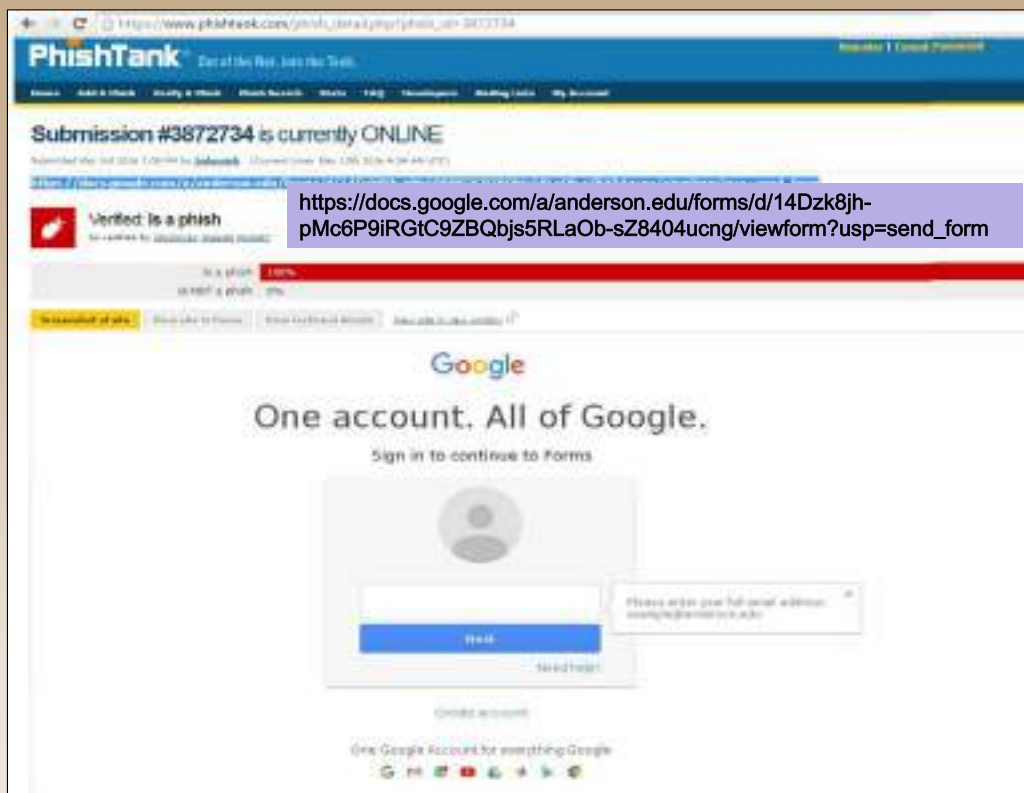
- Deep learning models have replaced the manual search and design for patterns and features.
- With the improved capability of models, research attention has been drawn to challenges such as oriented and curved text detection, and have achieved considerable progress.
- Methods adapted to more specific scenarios, e.g. bankcard, ID card, and driver's license.

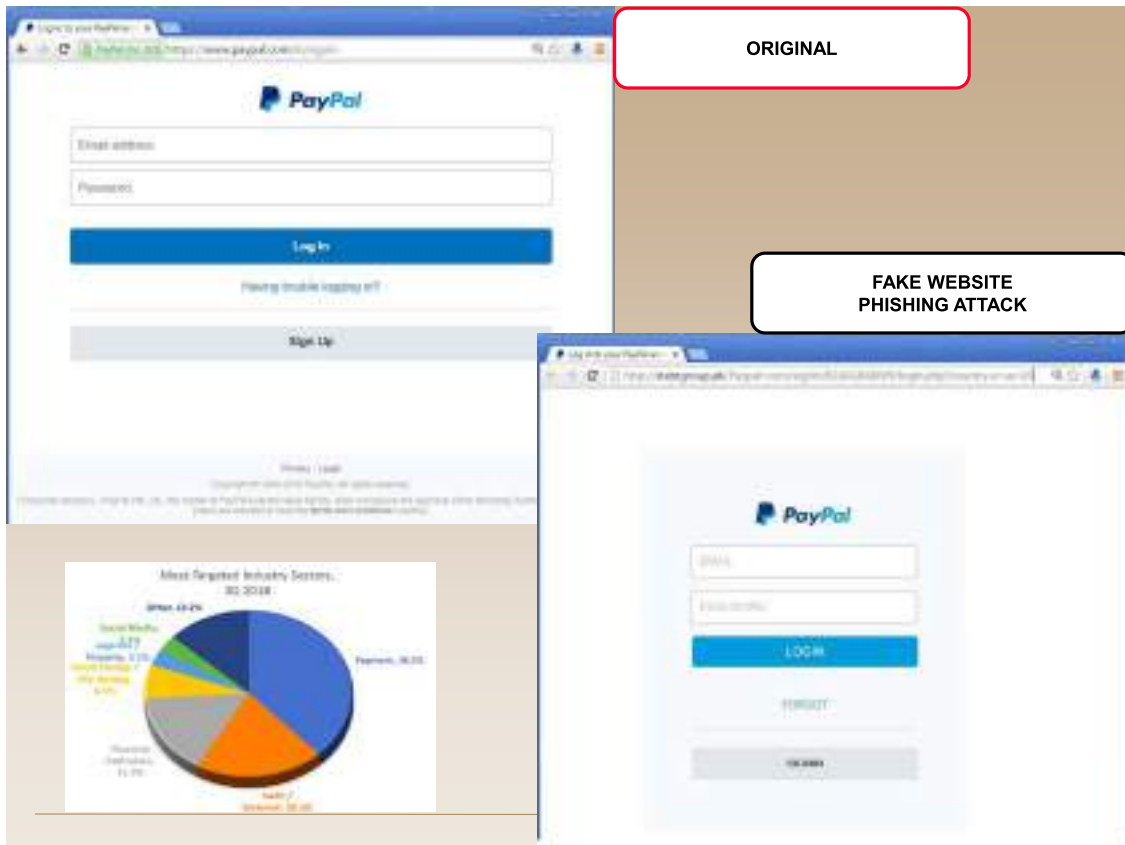
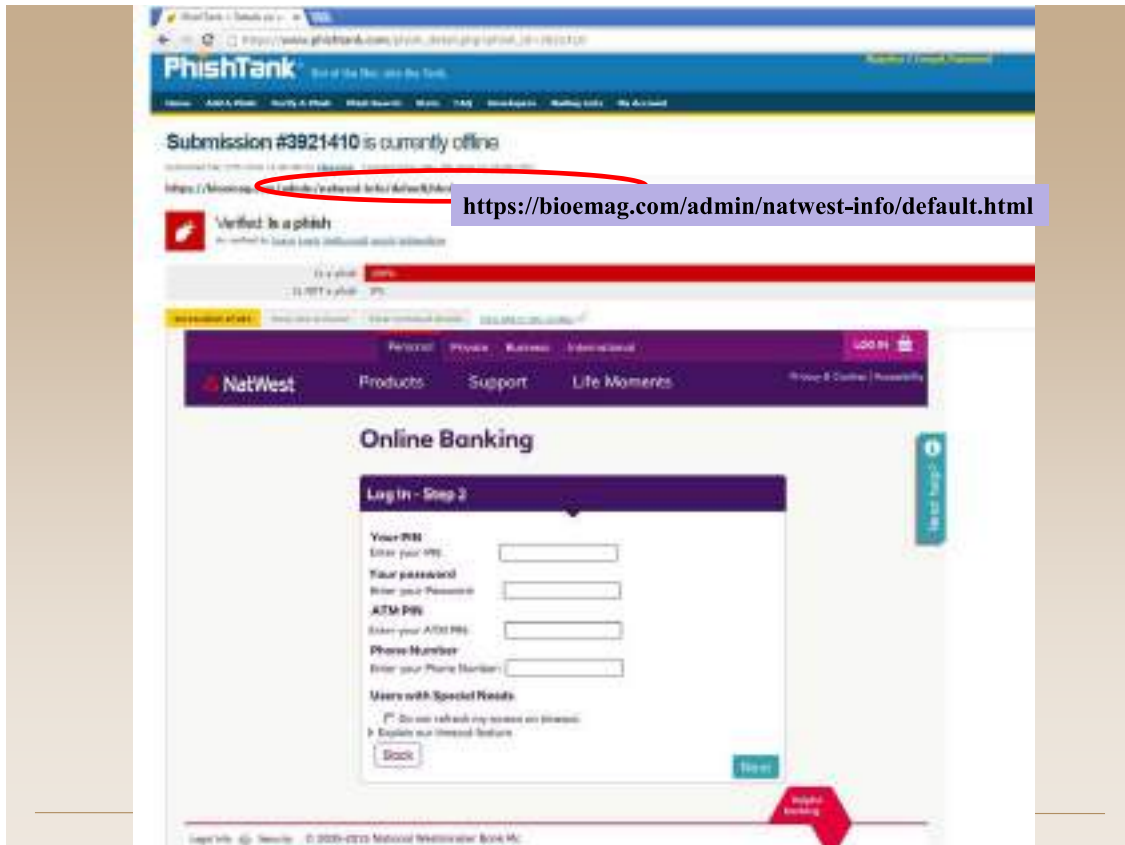
• Challenges

- ◆ Languages / Focus on English
- ◆ Robustness / Cross-dataset / Use of Synthetic dataset
- ◆ Efficiency / Real Time Detection

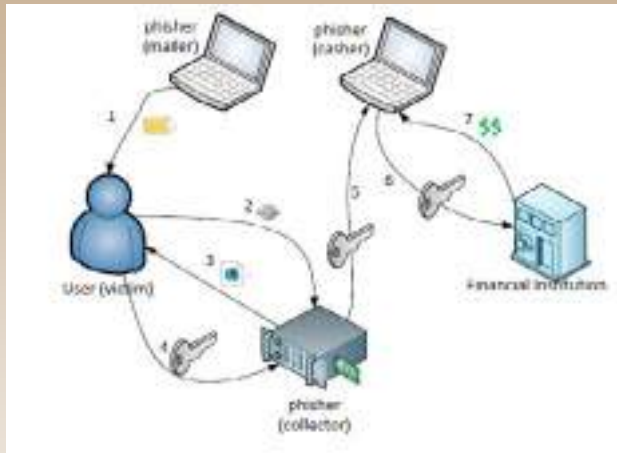
Phishing Attacks

- **Phishing** : It is a form of identity theft in which criminals build replicas of target websites and lure unsuspecting victims to disclose their credentials / sensitive information.
- **RSA Cyber-crime and Symantec reports 2019**: Phishing leads to several billion dollar losses to global organizations every year.
- **Anti-Phishing Working group (APWG) reports 2019**: Phishing attacks have been surging with annual growth rate more than 97%. Losses to US economy range from \$61 million to \$3 billion.
- **Some Recent News:**
 - SBI customer warning! 2 million users may be at risk of phishing attacks
 - UK (Action Fraud reports): More than 11,500 reports of coronavirus-themed phishing scams and £5 million worth of fraud since Feb
- Phishing attacks not only lead to financial losses but also hit down reputation of enterprises/financial organizations and also the confidence of users badly.
- The success of Digital India (Security, Education, Healthcare, eCommerce, eGovernance,...) critically depends upon usable and secure access to its remote users.





Phishing Information Flow



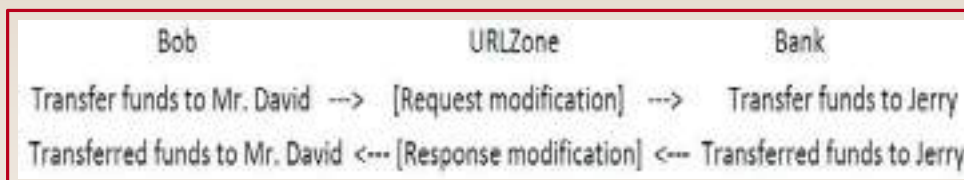
Image/Slide Courtesy: Junxiao Shi and Sara Saleem

• Three components

- ◆ Mail sender: sends large volume of fraudulent emails
- ◆ Collector: collect sensitive information from users
- ◆ Cashier: use the collected sensitive information to en-cash

Man In The Browser / Man in the Middle Attacks

- These attacks take advantage of vulnerabilities to inject code into the browser when you visit a specific site. This allows the hacker to do a variety of things including capturing information entered into fields on the website, adding fake fields to steal information or login credentials, or even gain control of the user's device.
- *Zeus Trojan attacks* responsible for around **80% of all attacks** against financial institutions today and led to **\$1 billion losses** in the last 5 years. (RSA)
- MitB : **invincible to security mechanisms** like SSL, 2-factor authentication and 3-factor authentication



Source: <http://blog.fireeye.com/research/2010/02/man-in-the-browser.html>



Improving Phishing Countermeasures: An Analysis of Expert Interviews

Sheng et al., 2009 eCrime Researchers Summit, WA, USA

A team from CMU conducted a study synthesizing the opinions of several anti-phishing experts and found that

Table 1: Phishing stakeholders. Primary victims suffer direct losses from phishing. Infrastructure providers have technical capabilities to mitigate the problem. For-Profit protectors sell solutions to primary victims and infrastructure providers. Public protectors include law enforcement officials, computer emergency response teams, and academic researchers.

Categories	Examples of key stakeholders	Roles
Consumers	--	Primary victims
Organizations	Military, Universities, Corporations	
Financial Institutions	Bank of America, Citibank, Paypal	
Merchants	Online merchants (eBay, Amazon), offline merchants	Infrastructure providers
Registrars and Registries	GoDaddy, Verisign	
Internet Service Providers	AT&T, Comcast, AOL, Universities	
Email Providers	Gmail, Yahoo!Mail, Hotmail	
Browsers	Internet Explorer, Firefox, Safari	For-profit protectors
Software Vendors	Symantec, RSA, MarkMonitor, Cyveillance	
Law Enforcement	Federal Bureau of Investigation (FBI), Secret Service state and local enforcement	Public Protectors
Computer Emergency Response Teams	CERT-CC, CSIRTs	
Academia		

Table 3: High-level findings.

Categories	Findings
Evolving threat	A. Phishing is evolving to be more organized and targeted. It is becoming part of a large crime eco-system. B. Phishing and malware are increasingly blended together.
Stakeholder incentives	A. Stakeholders have varying incentives to fight phishing. B. Sometimes stakeholder incentives are misaligned.
What stakeholders should do	A. Operating systems vendors, web application providers, browser vendors, and Internet service providers are stakeholders with key technology influence over phishing. B. Organizations are conservative about filtering and warning about phish because they are worried about false positives. C. Registries and registrars can play an important role in fighting against phishing.
Law enforcement and education	A. Law enforcement should be emphasized; but law enforcement lacks the necessary tools, personnel, and resources to catch phishers. B. Shutting down money trails is very important to defeat phishers.

Security Measures Against Phishing Attacks

- User-level Anti-phishing approaches
 - ◆ Anti-Phishing Plugins / Browser-Addons
- AI based phishing detection approaches
 - ◆ Applying ML tools on features extracted from Email content / URL etc. (NLP techniques also used)
- Enterprise-level Anti-phishing approaches
 - ◆ Using SSL certificates, secret images etc
- Social Campaigns / User Education
 - ◆ User awareness seminars / Simulated Phishing attacks

Forbes (2014): Even after a decade of anti-phishing efforts, phishing attacks on rise. Because phishing is "a technological medium to exploit human weaknesses" and that technology cannot fully compensate for human weaknesses

Using HTTPS / SSL Certificate Limitations

- SSL certificates ensure data on a website is being submitted in a secure manner, but they do not guarantee the site itself is safe. Because of this, hackers are taking advantage of buying cheap SSL certificates and using them on phishing websites to appear legitimate.
- Not many pay attention to https (or padlock symbol)
 - ♦ There is serious lack of awareness about secure practices especially India
- HTTPS not secure enough !



Using HTTPS / SSL Certificate Limitations



Using Personal Image



Using Personal Image Limitations

- Fake website developers can easily create the database of secret images by trying different usernames on the website.
 - ◆ Phishing websites can successfully mimic the authentic website and steal user credentials
- Static Approach
 - ◆ User is always presented with his/her secret image
- Not much user interaction and using same image repeatedly leads to less user-attention
 - ◆ Some research studies highlighted that majority of the participants enter their password details even when secret image and phrase were not present

A Hard AI based Enterprise Level Solution



Overview: Proposed Security Approach

- Enhance security against Phishing/MitB attacks using Multimedia Content Set Particular to User (MCSPU) and user specified parameters.
- For transaction confirmation, Bank would use a randomly selected image from ISPU, embedded with the critical text having properties as per *User Specified Parameters*.
- Bank may also intentionally respond at times with incorrect (non-user specific) image embedded with correct text that legitimate user must not confirm or else put in honeypot.
- **Attacker may change simple text response but not the text embedded on MCSPU using user specific parameters.**
 - ♦ Attacker to perform automatically text detection, text abstraction, image paintings/restoration and text insertion into the image with user known and user specified parameters.
 - ♦ Embedding fraudulent account number text within the limited time bound of Bank confirmation time limit and without showing any artifacts on the ISPU image is an extremely sophisticated task and to the best of our knowledge, there are presently no successful efficient automated algorithms for this.



Preventing Phishing with Proposed Approach

<p>Member Login</p> <input type="text"/> Random passcode to Initiate the login session <input type="text"/> <input type="button" value="LOGIN"/> ▶ Enroll Now ▶ I Lost My Password ▶ eServices Guide	<p>Member Login</p> <input type="text" value="userid ABCD"/> Random passcode to Initiate the login session <input type="text" value="456789"/> <input type="button" value="LOGIN"/> ▶ Enroll Now ▶ I Lost My Password ▶ eServices Guide
---	--

Please enter your password only after verifying your personal image below.

User ID:
userid ABCD

Random passcode to Initiate the login session:
456789

Password:

[Forgot Password](#)



MCSPU Based Proposed Approach



MCSPU based Approach



Image using japanese characters. A combination of different languages may also be used if user so requests



MCSPU based Approach



Just detecting the text contained along the curved path is very difficult, so exchanging the text within the limited time bound of Bank confirmation time limit and without leaving any artifacts on the image is even more difficult & challenging task.



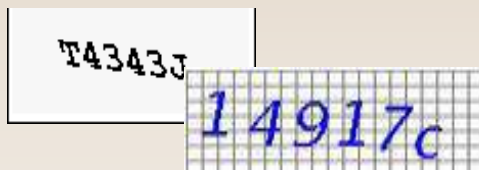
Significance of using MCSPU based Proposed Approach

- Automatic text extraction is *still a very challenging problem* especially with the variation of text due to differences in size, style, orientation & alignment.
 - ♦ Many OCR tools (like Microsoft Endnote, Abby Fine Reader etc.) - performed poorly in extracting text from natural scene images.
- This security approach involves MCSPU and User Specified embedding parameters - making it *much more complex than* just using any random image which is not specific to the user/client making transaction.
- If this approach were NOT to use *MCSPU and User Specified Text Embedding Parameters*, then adversary just need to identify the image portion within the confirmation webpage sent by Bank and modify that portion completely with some random image embedded with the user provided text information; and that will keep the user completely *UNAWARE* of the attack.

CAPTCHA Vs Proposed Method

CAPTCHA

- Text that appears in the generic image is unknown to the user
- No role of User specified embedding parameters



Proposed Method

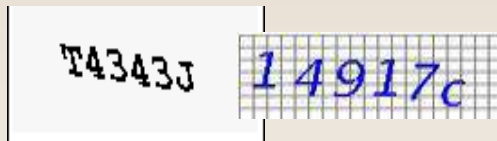
- **User only provided the text that is expected to appear in the MCSPU image**
- **Text embedded according to User specified parameters**



CAPTCHA Vs Proposed Method

CAPTCHA

- User may refresh the Captcha image to try other pass-code without having any other impact
- Several Captcha breaking tools (both automated & manual) already available.



Proposed Method

- **No option to refresh. Login Session / Complete transaction either cancelled or authenticated.**
- **No easy solution to date to break this.**



Today's Cyber Defenses are Static

- ❑ Today's approach to cyber defense is *governed by slow and deliberative processes* such as
 - ❑ Security patch deployment, testing, episodic penetration exercises, and human-in-the-loop monitoring of security events
- ❑ Adversaries can greatly benefit from this situation
 - ❑ They can *continuously and systematically probe targeted networks* with the confidence that those networks will change *slowly if at all*
 - ❑ They have the time to engineer reliable exploits and pre-plan their attacks
- ❑ Additionally, once an attack succeeds, adversaries persist for long times inside compromised networks and hosts
 - ❑ Hosts, networks, software, and services *do not reconfigure, adapt, or regenerate* except in deterministic ways to support maintenance and uptime requirements

ICISS 2014

by – Sushil Jajodia, *George Mason University*



Pro-Active Defense via Adaptation

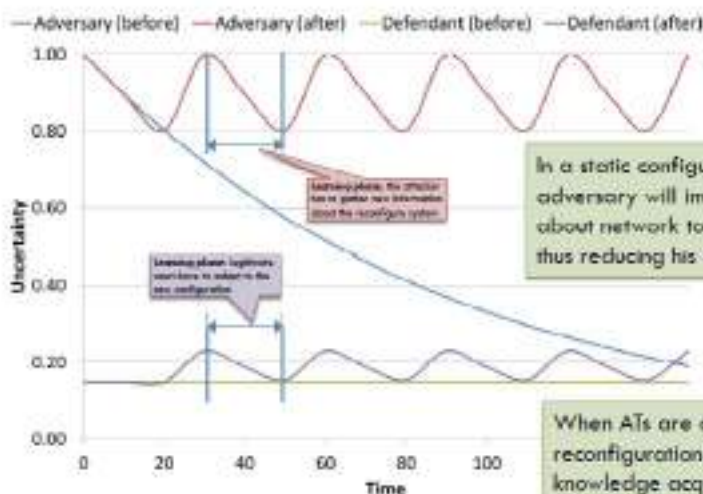
- To overcome today's limitations, we need to move from **reactive** defense to **proactive** defense
- We propose to use **adaptation** as the guiding principle enabling proactive defense
 - The ultimate goal is to **adapt** systems to an evolving threat landscape, which includes both known and new threats
 - Systems must be able to change and adapt before **such threats materialize**
 - Adaptation will provide an advantage for the defender



ICISS 2014

by – Sushil Jajodia, *George Mason University*

Adversary and Defender Uncertainty



ICISS 2014

by – Sushil Jajodia, *George Mason University*

Adaptive MCSPU based Security Approach

Presenting user with Multiple Security Images to choose from



Member Login

userid ABCD

Random passcode to initiate the login session

456789

LOGIN

▶ Enroll Now

▶ I Lost My Password

▶ eServices Guide

Adaptive MCSPU Based Approach

Select your secret image embedded with random passcode and then enter your password to login.

User Name - userid ABCD

Random code - 456789

Password

LOGIN





Adaptive MCSPU Approach

- **Additional Effort by the User for this enhanced security**
 - ◆ **One time Effort** – Selecting MCSPU and embedding parameters, preferably by visiting bank branch or via secure network channel
 - ◆ **Effort at the time of authentication**
 - » Providing random code based on which the information is embedded into the images (including the user-specific image) sent to the user for verification in next stage before user enters his/her password credentials, and
 - » an extra click to select the appropriate image
 - ◆ The system is designed such that ***the login button gets activated only when one radio button gets selected***. Also, this interaction will likely help user pay more attention and be more alert (at the cost of just “click”-effort) in comparison to the static case (only one image)
 - ◆ **Inappropriate image** : Either image shown is not from MCSPU, OR embedded random code OR embedding parameters - different from the user provided code / embedding parameters..

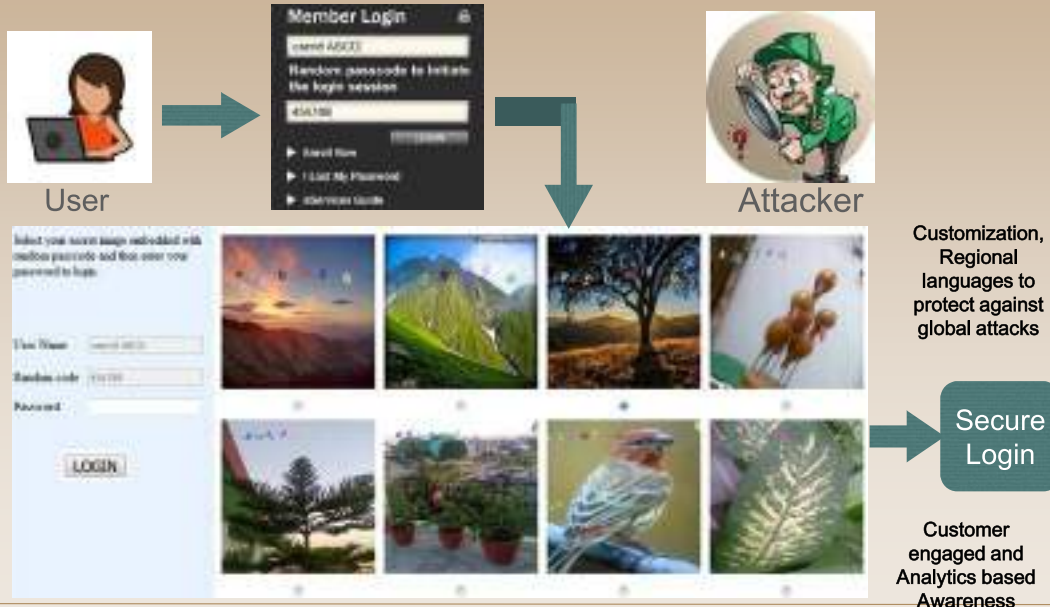
Significance of using Adaptive MCSPU Approach

- Advantages of MCSPU approach *(as discussed earlier)*
- Security enhanced by using multiple images for user to select
 - ◆ More difficult for adversary to identify user secret image
 - » Adversary cannot easily create database of images and fails to mimic original website
- Interactive platform helps user to be more attentive
- Provide means for spreading awareness and educating user
 - ◆ If one provides correct password but selected inappropriate image, not only user directed back to login page but also the user can be informed, preferably via other communication channel (email or sms), about exercising more care and alertness while logging.

Adaptive MCSPU Based Approach

Benefits of Proposed Solution MCSPU "Multimedia Content Set Particular to User":

- * Enterprise Level Solution, Easily Deployable
- * Enhanced Security -Adversary can neither modify image nor create database Interactive platform helps user to be more attentive
- * Provide means for spreading awareness & educating user (using AI / Analytics)
- * Empowers users to use regional languages / knowledge to prevent against Global Attacks



SESSION 3

Topic: **Phishing Attacks: Threat to National Critical Infrastructure**

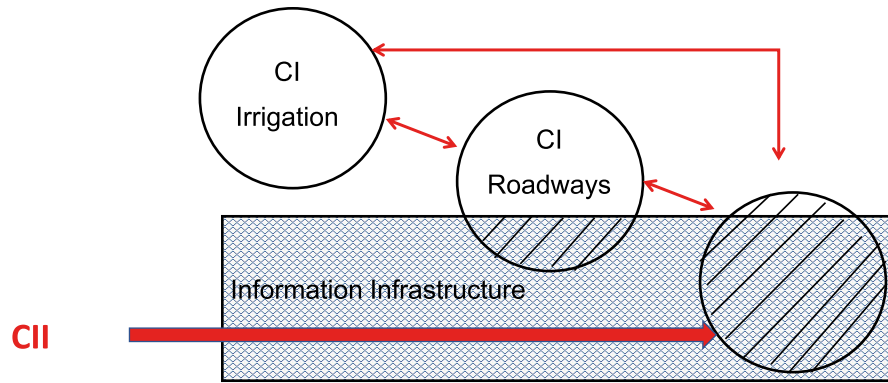
Speaker: **Sh. Sanjeev Relia,**

Senior Advisor Cyber Security - Tracelay, Bangalore, Alea Asia, New Delhi and SenseLearner Technologies – Noida



Sh. Sanjeev Relia delivered his talk focused on various phishing attacks and threats to the Critical Information Structure. He started his talk with an incident reported by ANI (dated on: Jul 11, 2021) about “Pakistan based group targets India’s critical infrastructure, cybersecurity firm warns of phishing attack”. He mentioned in brief about the incident where a suspected Pakistani group has started modern phishing attacks on India’s sensitive infrastructures such as power, telecom and finance, according to a leading cybersecurity firm. Pentapostagma reported that a cybersecurity consultant of Quick Heal Technologies said that a suspected Pakistani group has started a wave of sophisticated phishing attacks targeting India’s crucial infrastructure such as power and telecom. As per the security consultant, the initial intrusion chain begins with a spear-phishing email - an email that is designed to get the user to install a virus, trojan or other malware. (source: <https://www.aninews.in/news/world/asia/pak-group-targets-indias-critical-infrastructure-cybersecurity-firm-warns-of-phishing-attack20210711152707/>)

He discussed in brief about the Critical Information Infrastructure (CII). CII are those interconnected critical infrastructures and information infrastructures the disruption or destruction of either of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. The idea of CII can be imagined as shown in the Figure below



He also explained why there is a threat to Critical Information Infrastructure. Followings are the observations made about the same:

- Use of hi tech and networked systems.
- Use of open networking standards/ protocols such as TCP/IP.
- Use of less secure operating systems such as Windows instead of Proprietary Operating Systems.
- Mix of Legacy Systems and Modern Systems
- Convergence of networks.
- Flawed architecture – Security is not an overlay.
- CII owned by Private Sector

Moreover, he gave example of the Critical Information Infrastructure in India, i.e. National Critical Information Infrastructure Protection Centre (NCIIPC). NCIIPC is an organization of the Government of India created under the Section 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16 January 2014. Based in New Delhi, India, it is designated as the National Nodal Agency in terms of Critical Information Infrastructure Protection. It is a unit of the National Technical Research Organization (NTRO) and therefore comes under the Prime Minister's Office (PMO).

The Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as “those computer resources, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety”. NCIIPC has the vision of “To facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation.” and mission of “To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders.”

NCIIPC has broadly identified the following as ‘Critical Sectors’:

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom
- Transport
- Government

- Strategic & Public Enterprises



The main of threat to Critical Information Infrastructure includes:

- **Espionage:** Espionage or spying is the act of obtaining secret or confidential information from undisclosed sources or divulging the same without the permission of the holder of the information for a tangible benefit. A person who commits espionage is called an espionage agent or spy. Any individual or spy ring (a cooperating group of spies), in the service of a government, company, criminal organization, or independent operation, can commit espionage. The practice is clandestine, as it is by definition unwelcome. In some circumstances, it may be a legal tool of law enforcement and in others, it may be illegal and punishable by law. Espionage is often part of an institutional effort by a government or commercial concern. However, the term tends to be associated with state spying on potential or actual enemies for military purposes. Spying involving corporations is known as industrial espionage.
- **Subversion:** Subversion refers to a process by which the values and principles of a system in place are contradicted or reversed in an attempt to transform the established social order and its structures of power, authority, hierarchy, and social norms. Subversion can be described as an attack on the public morale and, “the will to resist intervention are the products of combined political and social or class loyalties which are usually attached to national symbols. Following penetration, and parallel with the forced disintegration of political and social institutions of the state, these tendencies may be detached and transferred to the political or ideological cause of the aggressor”.
Terrorist groups generally do not employ subversion as a tool to achieve their goals. Subversion is a manpower-intensive strategy and many groups lack the manpower and political and social connections to carry out subversive activities. However, actions taken by terrorists may have a subversive effect on society. Subversion can imply the use of insidious, dishonest, monetary, or violent methods to bring about such change.
- **Sabotage:** Sabotage is a deliberate action aimed at weakening a polity, effort, or organization through subversion, obstruction, disruption, or destruction. One who engages in sabotage is a saboteur. Saboteurs typically try to conceal their identities because of the consequences of their actions and to avoid invoking legal and organizational requirements for addressing

sabotage. Sabotage attack includes activities like deliberately destroying, damaging, or obstructing (something), especially for political or military advantage.

Further, he mentioned the following incidents of above attacks on Critical Information Infrastructures:

- a. Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz: (Source: <https://www.bbc.com/news/world-middle-east-56722181>). The attack caused a power blackout and damaged some of the precious machines at its site in Natanz, Iran. Iran has described this as an act of “terrorism” and pointed the finger at Israel. But there is still mystery over the cause. In Israel, some reports have suggested a cyber-attack might have been responsible but Iran has talked of “infiltrators” amid reports of an explosion linked to the power generator. An “incident” affected the power distribution network at Natanz, leading to a blackout until emergency power systems kicked in.



- b. Counterfeit Air Power: Meet China's Copycat Air Force (Source: <https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/>).

Counterfeit Air Power: Meet China's Copycat Air Force

China went from a regional to world power in record time, but it needed some "help" along the way.



BY NICK COLEMAN ON 07.07.2017



- c. Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility (Source: <https://www.wired.com/2009/11/mossad-hack/>). Agents of Israel's Mossad intelligence service hacked into the computer of a senior Syrian government official a year before Israel bombed a facility in Syria in 2007, according to Der Spiegel. The intelligence agents planted a Trojan horse on the official's computer in late 2006 while he was staying at a hotel in Kensington.

NOV 2009 SECURITY 11.03.2009 02.35 PM

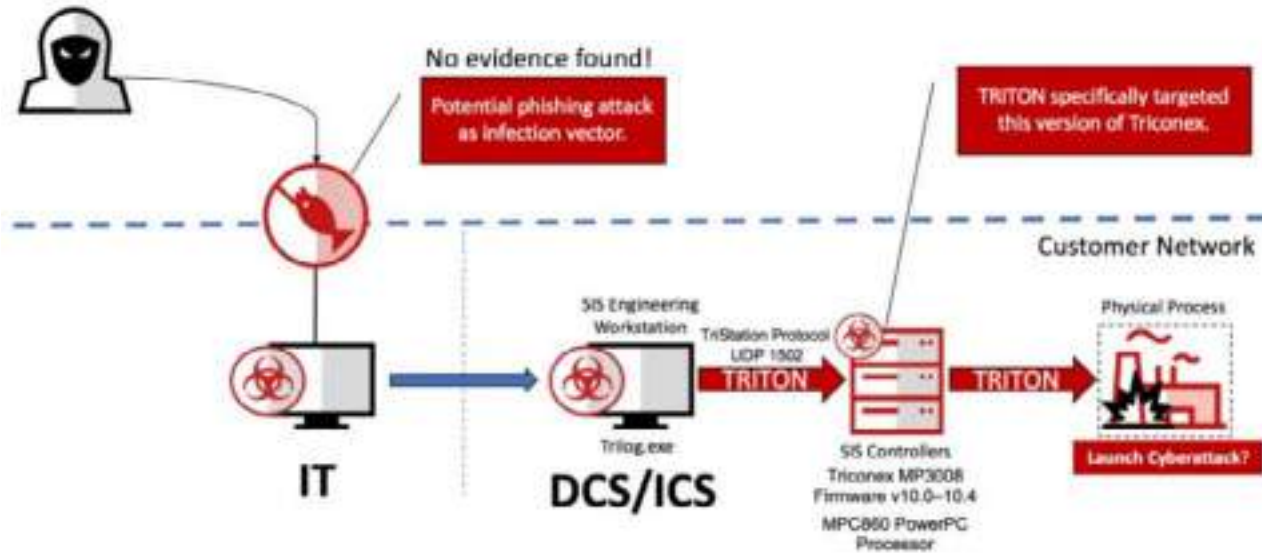
Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility

Agents of Israel's Mossad intelligence service hacked into the computer of a senior Syrian government official a year before Israel bombed a facility in Syria in 2007, according to Der Spiegel. The intelligence agents planted a Trojan horse on the official's computer in late 2006 while he was staying at a hotel in the Kensington [...]

Sh. Sanjeev Relia, further described in detail about a Phishing Attack Targeting an Industry: Triton Malware Attack in 2017, with following information:

- Potentially most destructive and dangerous cyber attacks on Industrial Control Systems.
- This malicious code could have led to an explosion or release of toxic gas in a Saudi petrochemical plant.
- First time an attack was purposefully designed to cause loss of life.
- Spear phishing was the initial attack vector used to access the plant's internal network.

Safety Instrumented System (SIS) Controllers, specifically a component named "Tricon", manufactured by Schneider Electric SE and commonly used in several industry sectors was targeted. The hackers deployed TRITON attack framework in an attempt to reprogram the facility's SIS controllers, as shown in the Figure below:

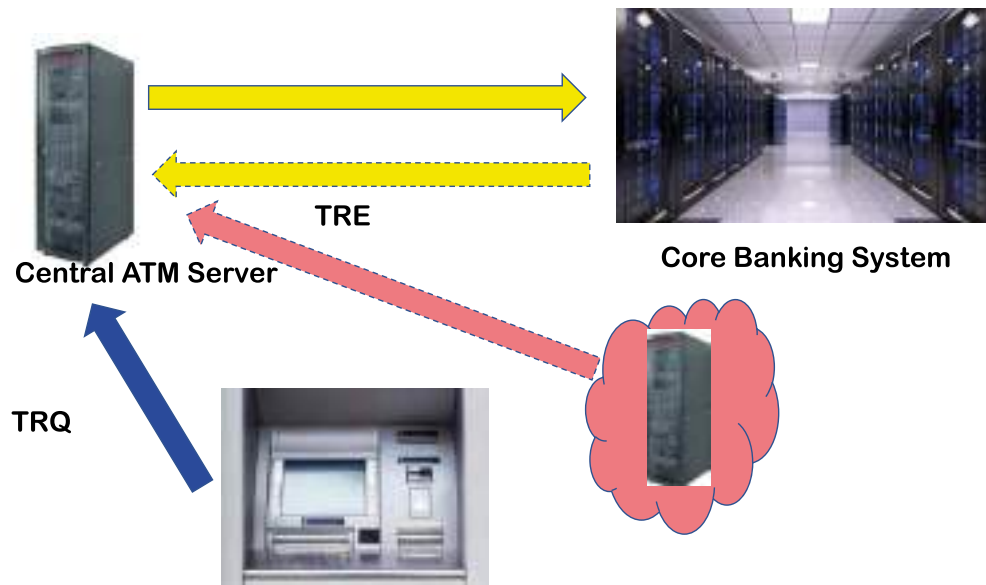


He also mentioned an incident of attack on Cosmos Bank, Pune. Cyber attack in August 2018 on Cosmos Bank's Pune branch which saw nearly 94 Crore rupees being siphoned off. Hackers wiped out money and transferred it to a Hong Kong situated bank by hacking the server of Cosmos Bank. Hackers hacked into the ATM server of the bank, installed a proxy server and with stolen details of many visa and rupay debit cards took money out using mules.

<p>WHAT HAPPENED</p> <ul style="list-style-type: none"> Fraudsters launched a malware attack and siphoned off ₹94.42 crore from Cosmos Bank on August 11 and 13 	<p>IS THE ACCOUNT HOLDERS' MONEY SAFE?</p> <ul style="list-style-type: none"> The account holders' money is safe now and in the future, says the bank, as the proxy switch was operative on the payment gateway, not the 'Core Banking System'
<p>HOW IT HAPPENED</p> <ul style="list-style-type: none"> The fraudsters created a proxy switch to interact with the VISA and Rupay payment gateway They used the fake switch to approve 12,000 transactions at ATMs in 28 countries, and 2,800 transactions in India 	<p>WHO'S BEHIND IT?</p> <ul style="list-style-type: none"> Experts suspect the hand of Lazarus, a group linked to the \$81 million heist in Bangladesh and the 2014 attack on Sony Pictures <p>WHAT'S NEXT?</p> <ul style="list-style-type: none"> The bank has appointed a professional forensic agency to investigate the attack The servers, internet banking, mobile banking and ATMs have been suspended The bank said it will take 3-4 days for the alternative switch to become operational

(Source: <https://timesofindia.indiatimes.com/city/pune/cosmos-bank-hit-by-cyber-hack-loses-rs-94-crore-in-2-days/articleshow/65409441.cms>)

The attack vector of Cyber Attack on Cosmos Bank, Pune, can be depicted as shown in the Figure below:

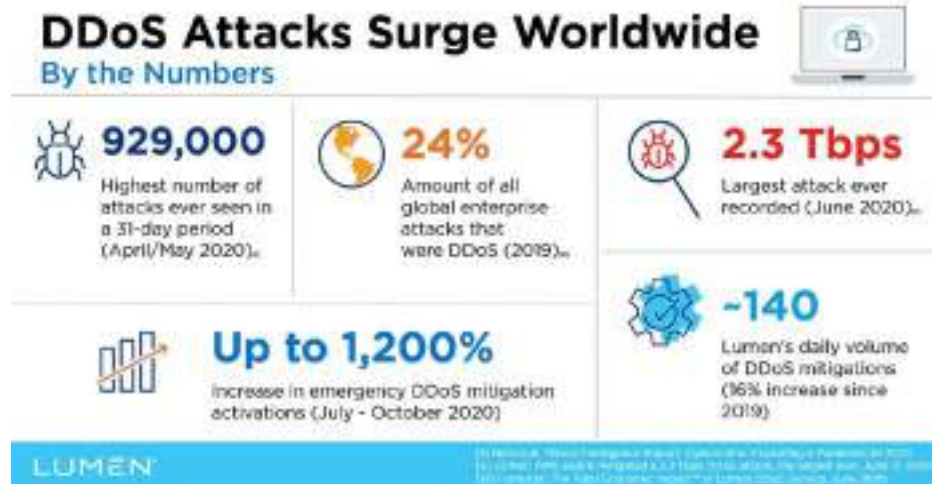


Following are the details of Details of Cosmos Bank Heist:

- Multiple targeted malware infections were used to compromise the bank's internal and ATM infrastructure.
- The malware was used in tandem with an infected central ATM or POS switch.
- When the first stage of the attack was implemented, the malware severed the connection between Central Systems and the backend Core Banking System (CBS) to prevent transaction verification.
- Once this connection was compromised, a central malicious switch was used to tamper with target account balances to enable unauthorized ATM withdrawals.
- Attackers were able to send fake Transaction Reply (TRE) messages in response to Transaction Request (TRQ) messages from cardholders and terminals.

He also explained about the Phishing Attack Threat by DDoS Attacks. As we know, botnets are created by Luring users into making a drive-by download - Phishing, Exploiting web browser vulnerabilities, Tricking the user into running a Trojan.

As per the Google's Threat Analysis Group (TAG) Blog (dated on 16th Oct 2020): "In 2020, our security reliability engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453 and 9394), which remains the largest bandwidth attack of which we are aware."



According to Sh. Relia, followings are the tentative solutions to above scenarios:

- Creation of a secure cyber ecosystem
- » CEA under the provision of Section 3(10) on Cyber Security in the “Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019” has framed Guideline on Cyber Security in Power Sector to be adhered by all Power Sector utilities to create cyber secure eco system.
- Cyber security an integral part of R&D of a system
- User Awareness
- Air Gapping of Networks

Sh. Sanjeev Relia’s talk ended with a brief session of open Q&A.

In the end, Dr. Karuna Sagar, IG/Director (Mod), BPR&D proposed a Vote of Thanks to the Chair and other Dignitaries. He mentioned that the knowledge shared by respected experts/speakers on the topic “**Prevention and Investigation of Phishing Crimes at Individual, Organizations and Critical Infrastructure Levels**” will definitely help all the Law Enforcement Officers to deal with the day to day Cyber Security Challenges especially related to Phishing Crime on various levels.



REFERENCES

1. Telling Humans and Computers Apart Automatically, Luis von Ahn, Manuel Blum, John Langford, Communications of the ACM, February 2004, Vol. 47 No. 2, Pages 56-60
10.1145/966389.966390
2. The CAPTCHA Project – <http://www.captcha.net>
3. G. Mori and J. Malik. Recognizing objects in adversarial clutter – breaking a visual captcha. Proceedings of the Conference on Computer Vision and Pattern Recognition, vol. 1, Madison, USA, pp. 134-141, June 2003.
4. A. Thayananthan, B. Stenger, P. H. S. Torr, and R. Cipolla. Shape Context and Chamfer Matching in Cluttered Scenes. Proceedings of the Conference on Computer Vision and Pattern Recognition, vol. 1, Madison, USA, pp. 127-133, June 2003.
5. Distortion estimation techniques in solving visual CAPTCHAs, Proceedings / CVPR, IEEE Computer Society Conference on Computer Vision and Pattern Recognition. IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2:II-23- II-28 Vol.2, January 2004
6. <http://blog.fireeye.com/research/2010/02/man-in-the-browser.html>
7. Improving phishing countermeasures: An analysis of expert interviews, DOI:10.1109/ECRIME.2009.5342608, November 2009
8. Why phishing still works: User strategies for combating phishing attacks, Mohamed Alsharnouby, Furkan Alaca, Sonia Chiasson, International Journal of Human-Computer Studies, Volume 82, Pp- 69-82, Oct 2015



CONTACT LIST OF BPR&D OFFICERS

Name of the Officer	Ph. No.
Sh. Balaji Srivastava Director General	011-26781312
Sh. Neeraj Sinha Addl. Director General	011-26781341
Dr. Karuna Sagar IG / Director (Mod)	011- 26782023
Brig. Navrattan Joshi (Retd.) PSO (Electronics)	011-26732185
Dr. Ajit Mukherjee, PSO (LS)	011- 26734938
Dr. Raveesh Kumar, PSO (W)	011- 26785451
Sh. Sushil Kumar PSO (B&E)	011-26734931
Dr. M.M. Gosal, SSO (T)	011- 26734815
Lt. Col. Ashwani Kumar AD (Mod)	011- 26782183

 officialBPRDIndia


 BPRDIndia

 Bureau of Police Research & Development India

 bprdIndia

 www.bprd.nic.in

 Cyberdost

 www.cybercrime.gov.in



NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037