Information Security Education & Awareness
Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India.

CYBER CRIME AWARENESS

CYBER CRIME AWARENESS CAMPAIGN JOINTLY BY CYBERABAD POLICE AND C-DAC

సైబరాబాద్ పోలీస్ మరియు సి–డేక్ (C-DAC) ల సైబర్ క్రైమ్ అవగాహన పై ప్రచారం

مشترکہ آگاہی مہم برائے تعاون سائبرآباد پولیس اور سی ڈی۔اے۔سی کے درمیان

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Hyderabad Campus, Kukatpally, Hyderabad - 500 085. Tel: +91- 40-23150115.
Fax: +91- 40-23150117. e-mail: isea@cdac.in

About C-DAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT) for carrying out R&D in IT, Electronics and associated areas. Different areas of C-DAC, had originated at different times, many of which came out as a result of identification of opportunities.

C-DAC has today emerged as a premier third party R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities in the context of global developments in the field and responding to change in the market need in selected foundation areas. In that process, C-DAC represents a unique facet working in close junction with DeitY to realize nation's policy and pragmatic interventions and initiatives in Information Technology. As an institution for high-end Research and Development (R&D), C-DAC has been at the forefront of the Information Technology (IT) revolution, constantly building capacities in emerging/enabling technologies and innovating and leveraging its expertise, caliber, skill sets to develop and deploy IT products and solutions for different sectors of the economy, as per the mandate of its parent, the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India and other stakeholders including funding agencies, collaborators, users and the market-place.

About C-DAC Hydearabad

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

About ISEA

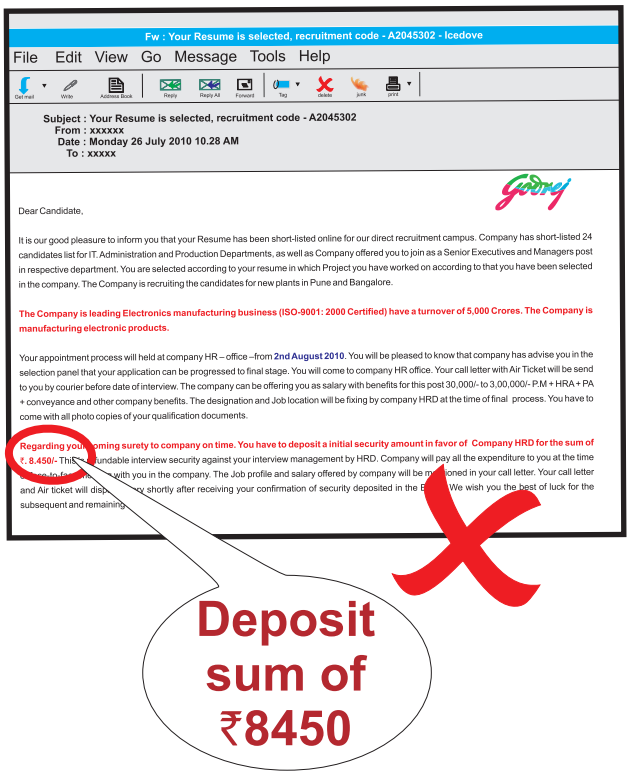
Looking at the growing importance for the Information Security, Department of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched for over a period of five years. One of the activities under this programme is to widely generate information security awareness to children, home users and non-IT professionals in a planned manner. C-DAC Hyderabad has been assigned the responsibility of executing this project by Department of Information Technology, Ministry of Communications and Information Technology, Government of India. As part of this activity, C-DAC, Hyderabad has to prepare the Information Security awareness material, coordinate with Participating Institutes (PIs) in organizing the various Information Security awareness events.

VISION

Generate Information Security Awareness among Indian citizens to enable them to participate safely in Information Society .

1. Be aware of Job Offers Through E-mails

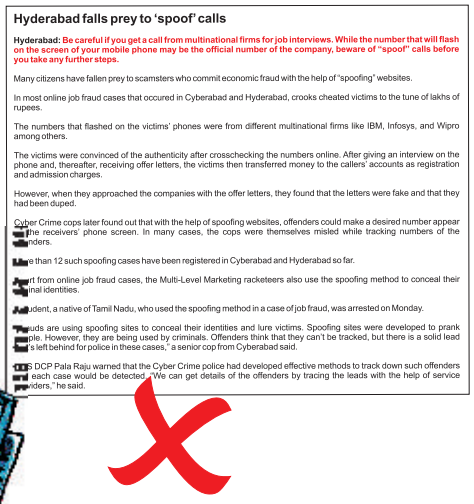
- Many of the students apply online for jobs. The accused collect the details posted in the websites and send fake e-mails.
- The e-mail looks like a mail from genuine companies through fake mailer sites and also conducts interviews.
- The victim receives a fake job offer letter. In return this fraudster ask for huge amount before and after receiving the offer letter.
- Stranger may send the offer letter using fake mailer service and make spoofing call in the name of MNC and send the offer letters and get the amounts deposited in the various places/Bank accounts and immediately withdraw the amounts and they may cheat you.



Precautions:

- Don't respond to spam mails without verification of the e-mail origin.
- Don't deposit money unless the candidate is interviewed personally by the company.
- Don't try to get job through back door methods by paying money which promises to provide employment, which will cheat you.
- Check with original company website for any job offers before proceeding.

2. Be aware of Fake Company E-mail Id's



Hyderabad falls prey to 'spoof' calls

Hyderabad: Be careful if you get a call from multinational firms for job interviews. While the number that will flash on the screen of your mobile phone may be the official number of the company, beware of "spoof" calls before you take any further steps.

Many citizens have fallen prey to scamsters who commit economic fraud with the help of "spoofing" websites.

In most online job fraud cases that occured in Cyberabad and Hyderabad, crooks cheated victims to the tune of lakhs of rupees.

The numbers that flashed on the victims' phones were from different multinational firms like IBM, Infosys, and Wipro among others.

The victims were convinced of the authenticity after crosschecking the numbers online. After giving an interview on the phone and, thereafter, receiving offer letters, the victims then transferred money to the callers' accounts as registration and admission charges.

However, when they approached the companies with the offer letters, they found that the letters were fake and that they had been duped.

Cyber Crime cops later found out that with the help of spoofing websites, offenders could make a desired number appear the receivers' phone screen. In many cases, the cops were themselves misled while tracking numbers of the nders.

e than 12 such spoofing cases have been registered in Cyberabad and Hyderabad so far.

rt from online job fraud cases, the Multi-Level Marketing racketeers also use the spoofing method to conceal their inal identities.

dent, a native of Tamil Nadu, who used the spoofing method in a case of job fraud, was arrested on Monday.

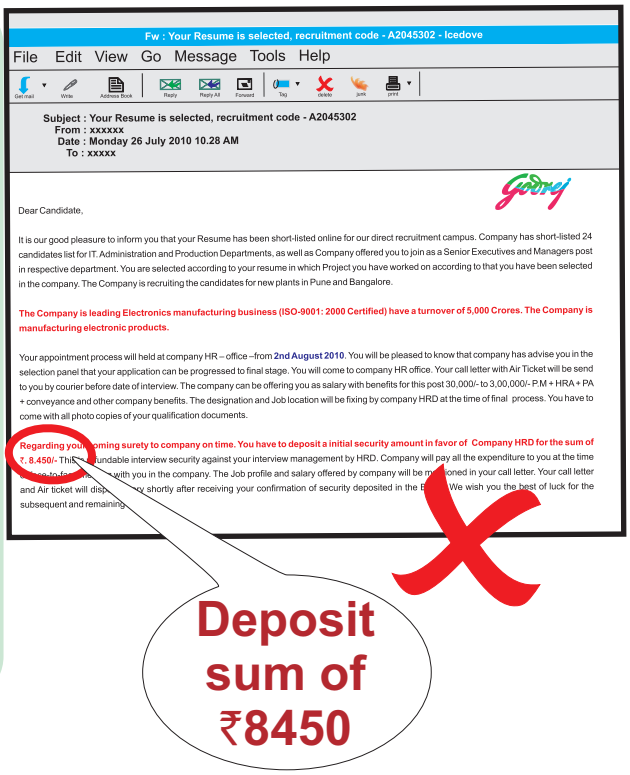
uds are using spoofing sites to conceal their identities and lure victims. Spoofing sites were developed to prank ple. However, they are being used by criminals. Offenders think that they can't be tracked, but there is a solid lead s left behind for police in these cases," a senior cop from Cyberabad said.

S DCP Pala Raju warned that the Cyber Crime police had developed effective methods to track down such offenders each case would be detected. "We can get details of the offenders by tracing the leads with the help of service viders," he said.

- Verify the e-mail ID thoroughly, with each and every letter of the e-mail ID before responding to any e-mails in the business transaction.
- Talk over phone with the company to ascertain, before depositing the money in their account, whether there is change of previous a/c details and name of the company.
- Maintain second step verification code to sign into account (Mobile alert).
- Whenever the fraud is noticed immediately inform to the original company.
- Don't respond to spam e-mails without verification of the e-mail origin (Header).

1. ఇ-మెయిల్స్ ద్వారా వచ్చే ఉద్యోగావకాశాలపట్ల జాగ్రత్తగా ఉండండి

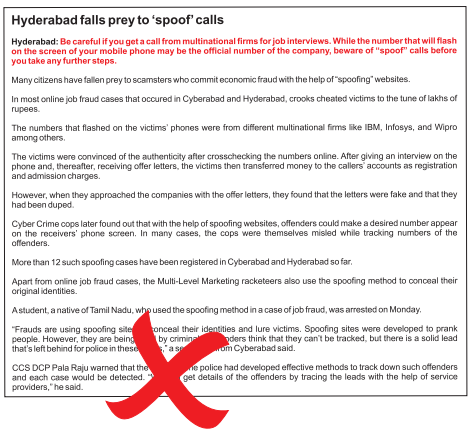
- చాలామంది విద్యార్థులు ఆన్‌లైన్‌లో ఉద్యోగాలకు దరఖాస్తు చేసుకుంటారు. వెబ్‌సైట్‌లలో నమోదైన వీరి వివరాలను మోసగాళ్ళు సేకరించి బూటకపు ఇ-మెయిల్స్ పంపుతుంటారు.
- ఈ ఇ-మెయిల్ కూడా నిజమైన కంపెనీలు పంపే మెయిల్‌లాగానే కనిపిస్తుంది. మోసగాళ్ళు బూటకపు మెయిలర్ సైట్లద్వారా ఇ-మెయిల్స్‌ను పంపి ఇజీటర్వ్యూలు కూడా నిర్వహిస్తారు.
- బాధితుడికి ఉద్యోగంలో చేరమంటూ ఒక మోసపు నియామకపత్రం అందుతుంది. ఈ లేఖ అందుకున్నవారు ఒక పెద్దమొత్తం చెల్లించాలనికూడా మోసగాళ్ళు ఆ లేఖలో సూచిస్తారు.
- మోసగాళ్ళు బూటకపు మెయిలర్ సర్వీస్ ద్వారా ఉద్యోగనియామక పత్రాన్ని పంపుతారు. బహుళజాతిసంస్థ పేరుతో ఫోన్ చేయటం, ఉద్యోగ నియామకపత్రాన్ని పంపటం చేస్తుంటారు. వారి మాటలు నమ్మి ఉద్యోగార్థులు వారి ఖాతాలలో డబ్బును జమచేస్తారు. మోసగాళ్ళు వెంటనే ఆ డబ్బును విత్‌డ్రా చేసుకుంటారు.



ముందుజాగ్రత్తలు

- స్పామ్ మెయిల్స్ ఎక్కడి నుండి వచ్చాయో సరిచూసుకోకుండా జవాబు ఇవ్వరాదు.
- అభ్యర్థుల సంస్థలతో స్వయముగా మాట్లాడనంత వరకు డబ్బులు ఖాతాలలో జమ చేయకూడదు.
- డబ్బులు చెల్లించి ఉద్యోగాలను పొందునటువంటి ప్రక్క దారులను ప్రయత్నించకండి, అవి మోసపూరితమైనవి.
- ఉద్యోగ అవకాశాలకై సంస్థలయొక్క వెబ్ సైట్లలో సరిచూసుకోండి.

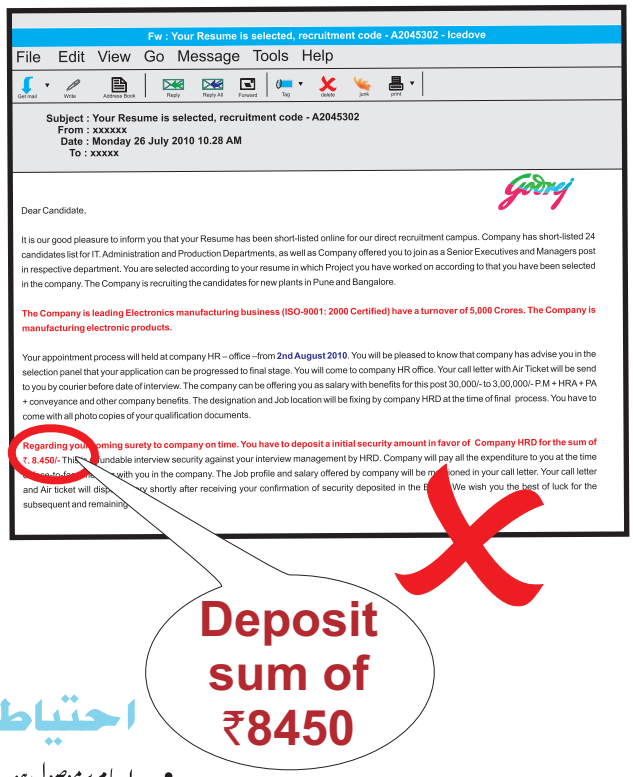
2. సంస్థల నకిలీ ఇ-మెయిల్ ఐడిలతో జాగ్రత్తగా ఉండండి.



- ఇ-మెయిల్స్ ద్వారా చేయు వ్యాపార లావాదేవీలకు ముందు ఇ-మెయిల్ ఐడి లోని ప్రతి అక్షరమును సరిచూసుకోండి.
- నగదును సంస్థల ఖాతాలలో జమచేయు ముందు వారి ఖాతా మరియు సంస్థ పేరుల వివరముల ఏమైన మార్పులు ఉన్నాయేమొ ఫోనులో అడిగి తేలుసుకోండి.
- మీ ఎకౌంటును తెరుచుటకు సెకెండ్ స్టెప్ వెరిఫికేషన్ కోడ్ (మొబైల్ ఎలర్ట్) ను నిర్వహించండి .
- ఏదైన మోసపూరితమైనవి గమనించినపుడు సంస్థలకు వెంటనే తెలియపరచండి.
- స్పామ్ ఇ-మెయిల్స్ ఎక్కడనుండి వచ్చాయో సరి చూసు కోకుండా ప్రత్యుత్తరము ఇవ్వకూడదు.

ای میل کے ذریعہ روزگار کی پیشکش پر ہوشیار باش

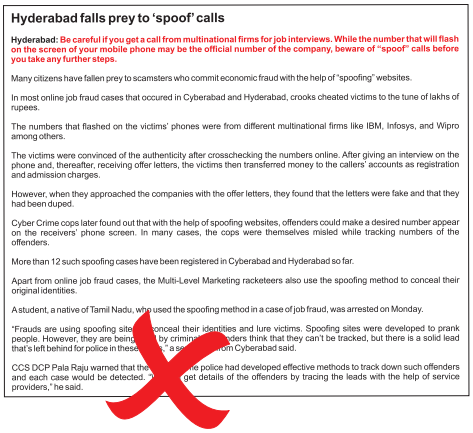
- روزگار کیلئے کئی طلبہ آن لائین درخواستیں دیتے رہتے ہیں۔جبکہ ملزمین ویب سائٹس پر بھیجی گئی ان تفصیلات کو حاصل کرتے ہوئے انہیں جعلی ای۔میلس بھیجتے ہیں۔
- جھوٹے میلر سائیٹس سے ایسے ای۔میلس بھجوائے جاتے ہیں جیسے کہ وہ حقیقی کمپنی کی جانب سے ہوں اور انٹرویوز بھی منعقد کرواتے ہیں۔
- متاثرہ شخص کو جعلی روزگار پیشکشی خط (آفر لیٹر) ملتا ہے۔اس کے بعد وہ دھوکہ باز افراد آفر لیٹر ملنے سے پہلے اور بعد ایک بھاری رقم بطورِ معاوضہ ادا کرنے کا سوال کرتے ہیں۔
- نامعلوم افراد جعلی میلر سرویس کی مدد سے آپ کو آفر لیٹر بھیج سکتے ہیں اور نقلی کال کسی ایم این سی کمپنی کے نام سے کریں گے اور آفر لیٹر بھیجیں گے اور متاثرہ شخص کی جانب سے ڈپازٹ کی گئی رقم کسی بھی مقام یا بینک کھاتہ کی مدد سے حاصل کرتے ہوئے فوری طور پر رقم نکال لیتے ہیں اور اس کے بعد دھوکہ دیتے ہیں۔



احتیاطی تدابیر

- اسپام پر موصول ہونے والے میلس کا جواب ان ای میلس کی تصدیق کے بغیر جواب نہ دیں۔
- جب تک کہ امیدوار کمپنی میں سیدھا شخصی انٹرویو نہ دے کوئی بھی رقم نہ دیں۔
- روزگار حاصل کرنے بھاری رقم ادا کر کے پیچھے کا دروازہ والے طریقے پر چلنے کی کوشش نہ کریں جس میں تو روزگار دلانے کی قسم کھائی جاتی ہے لیکن اصلیت میں دھوکہ ہوتا ہے ۔
- کسی بھی روزگار کی پیشکش پر اس کی جانب پیش قدمی کرنے سے پہلے اصل ویب سائٹ کا ملاحظہ ضرور کریں۔

کمپنیوں کے جھوٹے ای میل آئی ڈیس سے ہوشیار رہئیے



Hyderabad falls prey to 'spoof' calls

Hyderabad: Be careful if you get a call from multinational firms for job interviews. While the number that will flash on the screen of your mobile phone may be the official number of the company, beware of "spoof" calls before you take any further steps.

Many citizens have fallen prey to scamsters who commit economic fraud with the help of "spoofing" websites.

In most online job fraud cases that occured in Cyberabad and Hyderabad, crooks cheated victims to the tune of lakhs of rupees.

The numbers that flashed on the victims' phones were from different multinational firms like IBM, Infosys, and Wipro among others.

The victims were convinced of the authenticity after crosschecking the numbers online. After giving an interview on the phone and, thereafter, receiving offer letters, the victims then transferred money to the callers' accounts as registration and admission charges.

However, when they approached the companies with the offer letters, they found that the letters were fake and that they had been duped.

Cyber Crime cops later found out that with the help of spoofing websites, offenders could make a desired number appear on the receivers' phone screen. In many cases, the cops were themselves misled while tracking numbers of the offenders.

More than 12 such spoofing cases have been registered in Cyberabad and Hyderabad so far.

Apart from online job fraud cases, the Multi-Level Marketing racketeers also use the spoofing method to conceal their original identities.

A student, a native of Tamil Nadu, who used the spoofing method in a case of job fraud, was arrested on Monday.

"Frauds are using spoofing site[illegible] conceal their identities and lure victims. Spoofing sites were developed to prank people. However, they are being [illegible] by criminal[illegible]nders think that they can't be tracked, but there is a solid lead that's left behind for police in these[illegible] a s[illegible]m Cyberabad said.

CCS DCP Pala Raju warned that the[illegible]e police had developed effective methods to track down such offenders and each case would be detected. "[illegible] get details of the offenders by tracing the leads with the help of service providers," he said.

- تجارتی معاملات میں کسی بھی ای میل کا جواب دینے سے قبل اس ای میل ائی ڈی کو اچھی طرح سے ایک ایک حرف کے ساتھ اچھی طرح جانچ لیں۔
- پیسے ادا کرنے سے قبل یقین دہانی کیلئے راست کمپنی سے فون پر بات کریں کہ کہیں کمپنی اکاؤنٹ کی پرانی تفصیلات اور کمپنی کے نام میں کوئی تبدیلی تو نہیں؟
- اکاؤنٹ کھولنے میں ہمیشہ ثانوی تصدیقی کوڈ کا استعمال کریں (یعنی موبائیل الرٹ)
- جب کبھی دھوکہ دہی کا اندازہ ہو جاۓ فوری طور پر اصل کمپنی کو اس کی اطلاع دے دیں۔
- اسپام میں آنے والے ای۔میلس کا جواب نہ دیں جب تک کہ اس ای۔میل (عنوان) کی اصلیت کی تصدیق نہ ہو جائے