Cyber Security & Awareness

E-Newsletter

December 2023

राष्ट्रीय डिज़ाइन संस्थान, असम
National Institute of Design, Assam

“Click with caution, surf with suspicion and guard your data like it's your treasure.”

Welcome to the December 2023 edition of our newsletter, where cyber safety and awareness take centre stage. As the year draws to a close, we find ourselves amidst an increasingly interconnected digital landscape. This month, we prioritize the well-being of our online community by shedding light on **Job Frauds**, **Social Media Scams**, **Matrimonial Frauds** and acquaint users with latest technological trends in cyberspace. Join us on this journey of enlightenment as we share insights, practical tips, and resources to empower you in navigating the digital world securely. Let's make this December, a month of heightened cyber awareness, ensuring a safer online experience for us all.

ONLINE JOB FRAUDS

Job frauds, also known as employment scams, occur when individuals or organizations deceive job seekers with false employment opportunities. These scams can take various forms, and scammers often use online platforms to target unsuspecting job seekers. Common job frauds include:

Fake Job Postings: Scammers create fraudulent job listings, often on reputable job boards or websites, advertising positions that don't exist. They may use enticing language and promises of high salaries to attract applicants.

Phishing Emails: Job seekers may receive phishing emails that appear to be from legitimate employers or recruitment agencies. These emails often request personal information, such as Social Security numbers or financial details, under the guise of a job application process.

Advance Fee Scams: Scammers may ask job seekers to pay upfront fees for training materials, background checks, or other services related to the job. Legitimate employers typically do not require payment from applicants.

Identity Theft: Some job scams aim to steal personal information for identity theft purposes. Applicants may be asked to provide sensitive details under the pretence of a job application.

Work-from-Home Scams: Job fraudsters may offer work-from-home opportunities that promise high earnings with minimal effort. These scams often involve fraudulent payment schemes or the distribution of counterfeit checks.

Unrealistic Promises: Scammers may make unrealistic promises about job roles, salaries, or benefits to lure individuals into applying. These promises are often too good to be true.

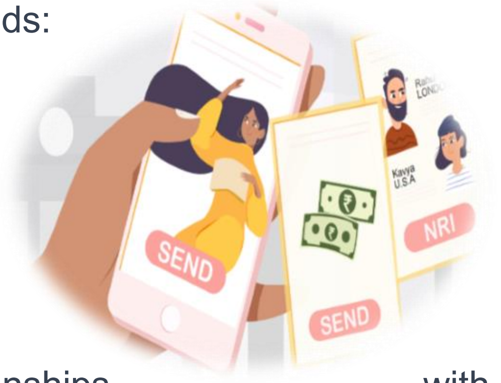
QUICK TIPS

To avoid falling victim to job frauds, it's essential for job seekers to

- Check privacy policy of job sites.
- All online interviews are not genuine. Do proper check about the organization and its representative and ask detailed question about the job and the organization.
- Never Pay for a Job offer in exchange for money. Legitimate employers typically follow standard hiring procedures and do not request payment or sensitive information upfront.
- Thoroughly research potential employers.
- Always try to check the company's website for authenticity of the job.
- Don't respond to unsolicited mails and check for spelling mistakes. Examples of suspicious addresses include info@company.net instead of info@company.com, info@companie.com, info@compaaany.com.
- Beware of fake government websites, verify before you apply or else you may end up paying to the fraudsters through a spoofing website.

Matrimonial Frauds

Matrimonial frauds encompass manipulative practices involving marriage-related matters and scams that take place in the context of matrimonial or online dating platforms. These frauds often involve individuals who pretend to be someone they are not, with the intent to deceive others for financial gain or other malicious purposes. Here are common types of matrimonial frauds:



Fake Profiles: Scammers create fictitious profiles on matrimonial websites, presenting false information about themselves, including photos, personal details, and interests.

Romance Scams: Fraudsters build romantic relationships with unsuspecting individuals, often over an extended period, and then fabricate reasons to request money or financial assistance.

Marriage-for-Green-Card Scams: Some individuals may enter relationships with the sole intention of obtaining a green card or citizenship in a specific country, rather than genuine interest in a long-term relationship.

Identity Theft: Scammers may use stolen or fake identities to create a persona that seems genuine. This can lead to serious consequences for the person whose identity has been misappropriated.

Financial Exploitation: Fraudsters may manipulate victims emotionally to gain access to their financial resources. This can involve requests for money, gifts, or other financial assistance under false pretences.

Catfishing: Catfishing occurs when someone creates a fake online identity to establish deceptive social relationships. This can be for emotional manipulation, financial gain, or other malicious purposes.

Non-Disclosure of Marital Status: Individuals may misrepresent their marital status on matrimonial platforms, hiding the fact that they are already married or committed.

QUICK TIPS

To protect oneself from matrimonial frauds and avoiding falling victim to these scams it's important to exercise caution

- Verify information independently,
- Be sceptical of requests for money or personal details from individuals met online. Use reputable and secure matrimonial platforms.
- Share information about the prospective match with your family.
- Fraudsters will usually call from multiple numbers. He/ She usually don’t give a number to call back. Even if he/ she give a number, they don’t pick up when you call.
- If a person is reluctant to come on video chat or to meet in person, he/she can be a fraudster as the profile picture posted on matrimonial website may not be of his/ her.
- Never share your sensitive personal photographs.
- Be cautious while dealing with NRI profiles.
- Always meet in public place.
- Conduct thorough background checks and maintain open communication.

Social Media Frauds

Social media scams and frauds are deceptive practices that exploit users on various social networking platforms. These schemes leverage the trust, personal information, and engagement of individuals for fraudulent purposes. Awareness and vigilance are crucial to protect oneself from falling victim to these scams.

Here are some prevalent types of social media scams and frauds:

Phishing Scams: Scammers create fake websites or profiles that imitate legitimate social media platforms, tricking users into providing login credentials or personal information.

Impersonation: Fraudsters impersonate individuals, celebrities, or businesses to deceive users. They may create fake accounts to extract sensitive information, money, or to damage reputations.

Fake Contests and Giveaways: Scammers organize fraudulent contests or giveaways, enticing users to participate by liking, sharing, or providing personal information. The aim is often to collect data for future scams.

Romance Scams: Fraudsters build romantic relationships with users, gaining trust before requesting money or personal information under false pretences.

Investment Scams: Scammers promote fake investment opportunities on social media, promising high returns. Once users invest, their money may disappear, and the scammer may vanish.

Tech Support Scams: Users receive unsolicited messages or pop-ups claiming their device has a virus. Scammers pose as tech support, convincing users to pay for unnecessary services or providing access to sensitive information.

Malicious Links and Downloads: Scammers share links or files that contain malware or phishing software, aiming to compromise users' devices or steal personal information.

Hacking and Account Takeovers: Cybercriminals use various methods to hack into users' accounts, gaining unauthorized access to personal information, contacts, and private messages.

QUICK TIPS

To protect against social media scams, users should be cautious

- Reporting suspicious accounts and content to the platform administrators.
- Disable profile visibility from public searches.
- Log out after each session.
- Never accept friend request from unknown persons
- Avoid mentioning home or work address in social media profiles.
- Never click on suspicious links
- Keep the privacy settings of social media profile at most restricted level especially for public viewing.
- Apply maximum caution while sharing photographs, videos, status, comments etc.
- Criminals may collect enough information about users from the posts and profile of the users.
- Never download apps received through messages.

Beware of FraudGPT Scam

FraudGPT, an AI-powered Chatbot is used by Cyber criminals to craft fraudulent content for cyber frauds and crimes.

Modus Operandi

- FraudGPT can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details, or personal data.
- It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
- It can imitate human conversation with users to share sensitive information or to perform harmful actions.
- It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.

Safety Tips

- Avoid clicking on links/ attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.

BEWARE OF MORPHING

Modus Operandi

- Morphing is altering or changing the picture of a person using sophisticated morphing tools.
- Criminals send friend requests on social media to innocent victims.
- Once the victim accepts the request, they may receive a morphed video call using images/videos of police officials.
- Criminals may blackmail the innocent victim for committing a crime, which he/she has not committed in the morphed video call.
- Fearing the loss of reputation and respect, victims pay the money to criminals.

Best Practices

- Never accept friend requests from unknown people.
- Lock profile visibility from public searches.
- Never attend to calls from strangers through social media accounts.
- Restrict the visibility of your posts, images, and videos on social media accounts.
- Keep the privacy settings of your social media profile at the most restricted levels, especially for the public and others.
- Enable multi-factor authentication with strong passwords for your social media accounts.
- Save the evidence and the screen shots for referring to the incident later.
- Don't suffer in silence; know that you are not alone. Reach out and seek help from trusted family and friends.
- If you observe your fake profile or any such objectionable posts on social media, report them the respective social media help center.
- Report cyber crimes immediately by calling 1930 or visit https://www.cybercrime.gov.in.

In News Cybersecurity, Attacks, Scams

- **Online job aspirant defrauded of Rs 27.56 lac.**

  A case of online job scam in which the victim lost Rs 27.56 lac has come to light here. An individual received a message on telegram app on June 19 that money can be earned by completing the task of rating hotel and home stay. The complainant who trusted it, had completed 30 tasks from Aditi MMT Guru Group. The unidentified person had paid Rs 900 profit. He had made the complainant invest Rs 11,000 on the same day and paid Rs 20,000 and Rs 70,000 profit. He lured the complainant that more profit will be earned if he continues to invest and made the victim transfer Rs 27,56,129 to various accounts between June 19 and August 26 in stages and cheated by not paying any profit later.

- **Two men have been arrested in connection with a cyber fraud conducted under the guise of a part-time job opportunity.**

  Ankit Gupta (33), a BTech graduate, utilised his technical expertise to orchestrate the scam involving over Rs 1 crore, allegedly in association with Bharat Bhushan (35) and two others based in Bangalore. The investigation began after receiving a victim's complaint on November 1. "The complainant, seeking a part-time job, fell victim to the scam where she paid Rs 1000 for a task upon which she had received a small return only to be lured into investing Rs 198,000. The accused then ceased communication after receiving the funds,".

- **How a man hacked into a company's bank account, and stole Rs 18.74 lakh**

  Navi Mumbai police have unearthed a cyber theft case where a man allegedly hacked into the bank account of a company and stole Rs 18.74 lakh. According to a report by news agency, the man used SIM card fraud to hack into the account. The man using the genuine mobile phone number had received an SMS saying his SIM card had been deactivated, but he failed to notice. The same SIM card was found active in the mobile phone of the accused person. (SIM card fraud, also known as SIM swapping or SIM hijacking, is a type of account takeover fraud that allows criminals to gain access to your phone number and potentially your online accounts.)

- **Pratibimb app helps nab 78 cybercriminals in a month.**

  The Pratibimb App launched by the state CID is proving to be a boon for investigating agencies in nabbing cyber criminals operating from different districts of the Santhal Pargana division.

  A total of 78 cybercriminals have so far been arrested from different districts of Santhal Pargana since the app was launched on November 7. Police also recovered hundreds of mobile phones, SIM cards and other incriminating items from their possession. "So far, 78 cyber criminals have been arrested from different districts of Santhal Pargana in 25 days since the CID launched the app," DIG said, adding many arrests were made even before the crime could be committed.

  With 41, Deoghar top the list in terms of arrests, followed by 27 from Jamtara, which is infamous for cyber-crimes. Other arrests were made from Dumka, Godda and Pakur districts. Seizures include 255 mobile phones, 385 SIM cards, two laptops, 26 ATM cards, 14 passbooks, and two cheque books. "The Pratibimb App enables the cyber police to locate the geographical location of the criminals resulting in their arrests instantly,"

- **83-year-old man gets 'KYC call', loses Rs 2.5 lakh**

  An 83-year-old man who visits the bank for all transactions was duped out of Rs 2.5 lakh after he received a call from a man who said he was calling from "table number 3" of the branch where the victim has his pension account. The caller had said he was calling to verify the KYC (know your customer) of the octogenarian, S.P. Sinha. The aged man failed to follow the caller's instructions to "update his KYC online" and handed the phone to his 11-year-old grandson so he could take instructions from the caller and "update the KYC". The boy unknowingly answered to all the queries and after the call ended, the old man was poorer by a few lakhs of rupees.

- **IT Professional Duped of Rs 27.9 Lakh in “Drug-in-Parcel” Scam**
  A 37-year-old IT professional from Pune has fallen victim to a sophisticated online fraud, losing a staggering Rs 27.9 lakh to cybercriminals posing as Mumbai police officers. The incident, which highlights the growing threat of “drug-in-parcel” scams, underscores the importance of online vigilance and awareness.

- **Jamtara cyber police unveils interstate cyber gang: 12 arrested in raid operation.**
  In a significant breakthrough, the Jamtara cyber police station has successfully exposed and apprehended an interstate cyber gang. SP Animesh Naithani, in a press conference on Sunday, announced that a total of 12 cybercriminals were arrested in coordinated raids conducted in the villages of Sindarjori, Sheetalpur, and Siatand, among others, within the Karmatand police station area.

Feeds / Images References

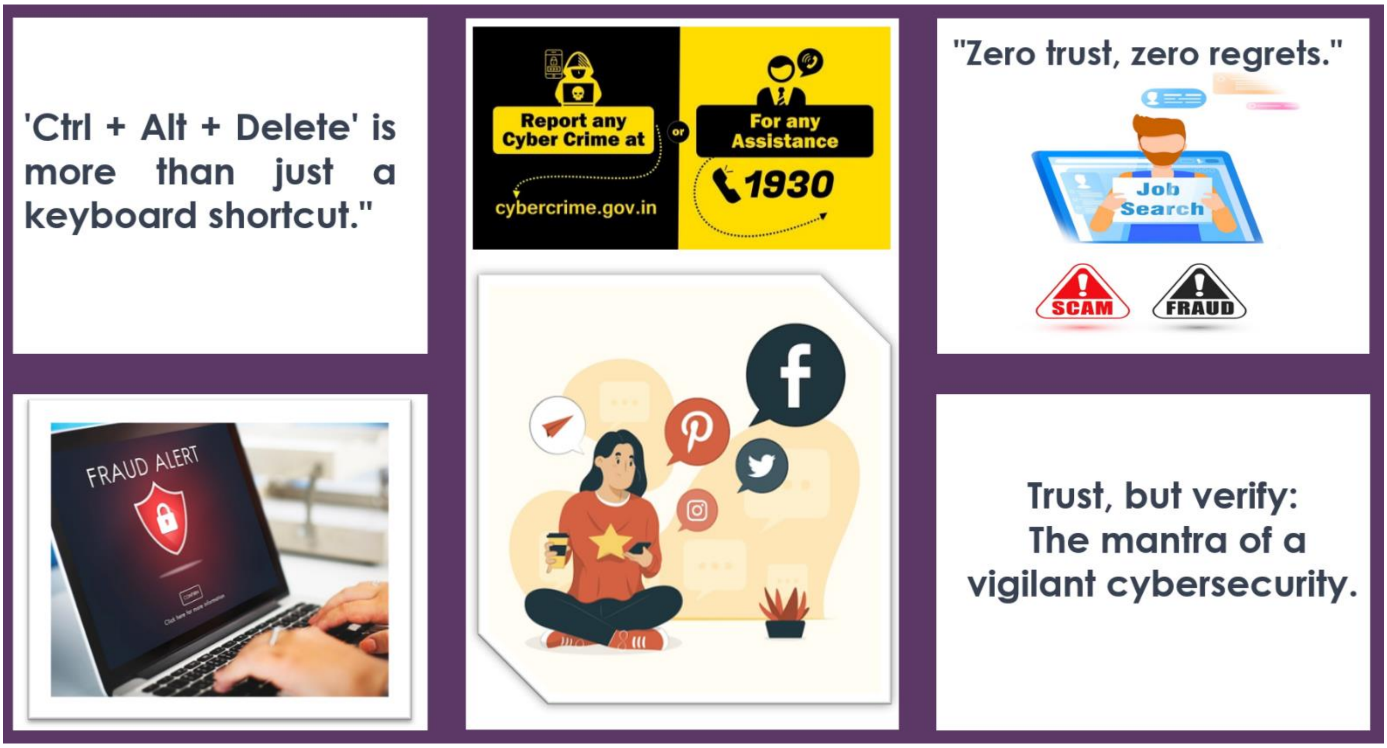
- https://timesofindia.indiatimes.com/city/delhi/two-arrested-for-1cr-cyber-fraud-in-delhi/articleshow/105768029.cms
- https://timesofindia.indiatimes.com/city/ranchi/pratibimb-app-helps-nab-78-cybercriminals-in-a-month/articleshow/105797050.cms
- https://www.freepik.com/
- https://cybercrime.gov.in/
- https://www.infosecawareness.in/
- https://timesofindia.indiatimes.com/gadgets-news/how-a-man-hacked-into-a-companys-bank-account-and-stole-rs-18-74-lakh/articleshow/105762957.cms
- https://www.telegraphindia.com/my-kolkata/news/online-fraud-83-year-old-man-gets-know-your-customer-call-loses-rs-2-5-lakh/cid/1984849
- https://www.the420.in/pune-it-professional-duped-of-rs-27-9-lakh-in-drug-in-parcel-scam/
- https://avenuemail.in/jamtara-cyber-police-unveils-interstate-cyber-gang-12-arrested-in-raid-operation/

As we wrap up the month of December, it's essential to take a moment to contemplate the significance of being mindful about cybersecurity. Cyber security is not a one-time effort but an ongoing commitment. The year 2023 has witnessed several digital scams, frauds, leaking of personal and sensitive information and bankrupt thousands of users using digital media. As we step into 2024, let's carry forward the lessons learned this year. Remember, each one of us plays a role in the collective defence against cyber threats.

Stay watchful, stay updated.

Let's make cyber security a priority throughout the coming year.

We'll be back next year with more tips and updates.


'Ctrl + Alt + Delete' is more than just a keyboard shortcut."
Report any Cyber Crime at
cybercrime.gov.in
or
For any Assistance
1930
"Zero trust, zero regrets."
Job Search
SCAM
FRAUD
FRAUD ALERT
Trust, but verify: The mantra of a vigilant cybersecurity.

THANK YOU