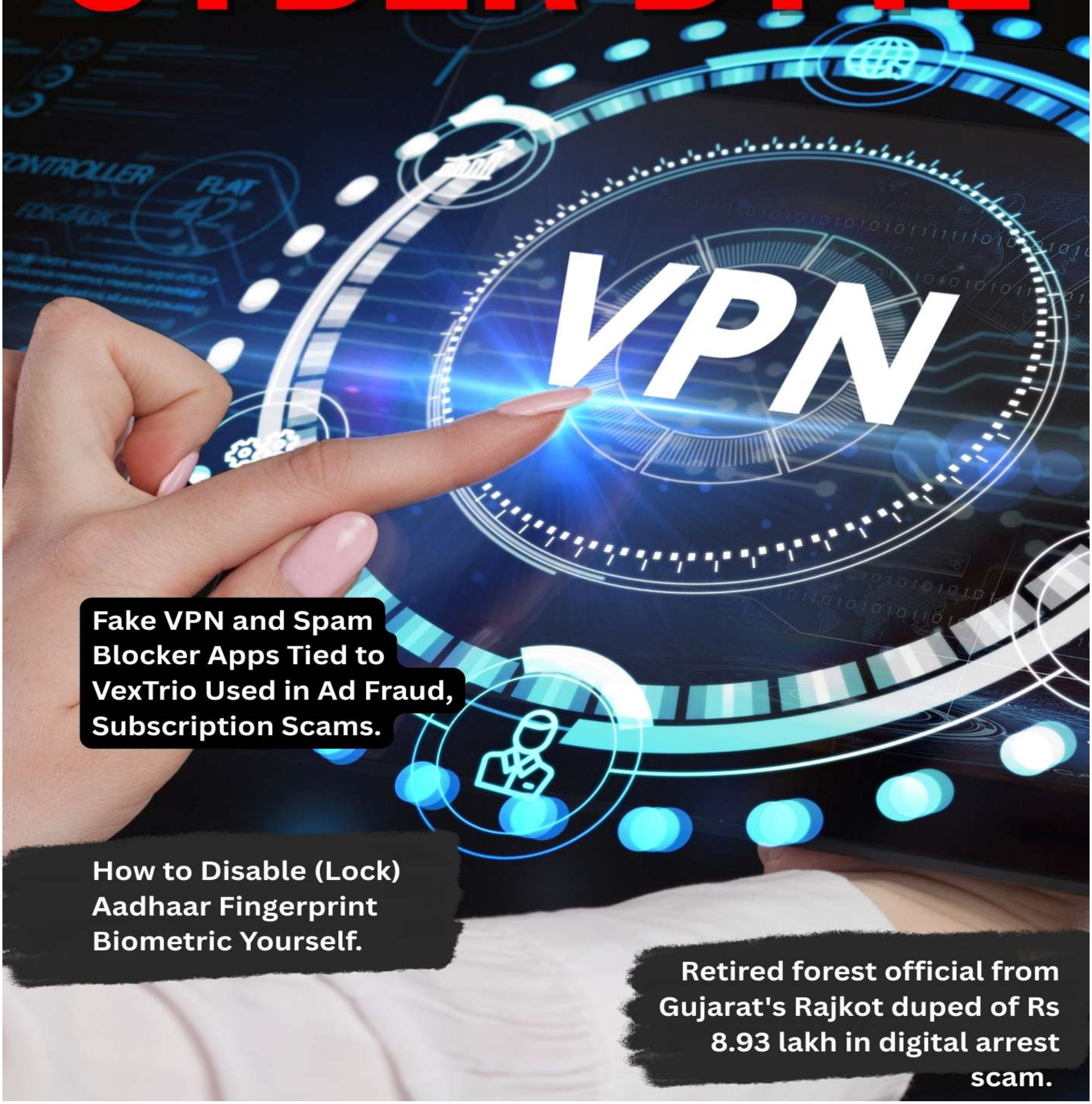
CENTRAL RESERVE POLICE FORCE

AUGUST-2025

CYBER BYTE



Fake VPN and Spam Blocker Apps Tied to VexTrio Used in Ad Fraud, Subscription Scams.

How to Disable (Lock) Aadhaar Fingerprint Biometric Yourself.

Retired forest official from Gujarat's Rajkot duped of Rs 8.93 lakh in digital arrest scam.

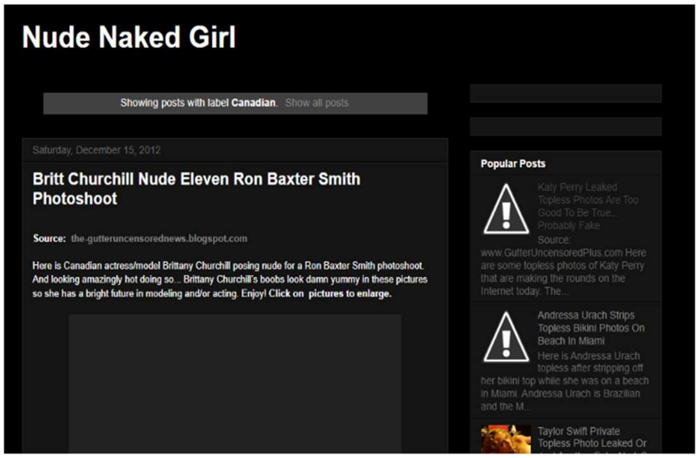
1. CYBER GEEKS NEWS

(A) Adult sites trick users into Liking Facebook posts using a clickjack Trojan.

As the use of age verification to access adult websites increases in various countries around the world, shady websites with adult content have started a timely malware-fueled campaign to promote links to their own websites.

Regularly review Facebook posts for signs of scams, particularly those that link to adult websites. Pay close attention to posts that direct users to sites hosted on blogspot[.]com, as these are often used to promote additional, similar websites in a coordinated manner. Such networks may be part of a broader scheme involving misleading or malicious content. Identify and flag these posts to help prevent the spread of potentially harmful links.

Here’s one example:



Nude Naked Girl

Showing posts with label **Canadian**. Show all posts

Saturday, December 15, 2012

Britt Churchill Nude Eleven Ron Baxter Smith Photoshoot

Source: the-gutteruncensorednews.blogspot.com

Here is Canadian actress/model Brittany Churchill posing nude for a Ron Baxter Smith photoshoot. And looking amazingly hot doing so... Brittany Churchill's boobs look damn yummy in these pictures so she has a bright future in modeling and/or acting. Enjoy! Click on pictures to enlarge.

Popular Posts

Katy Perry Leaked Topless Photos Are Too Good To Be True... Probably Fake Source: www.GutterUncensoredPlus.com Here are some topless photos of Katy Perry that are making the rounds on the Internet today. The...

Andressa Urach Strips Topless Bikini Photos On Beach In Miami Here is Andressa Urach topless after stripping off her bikini top while she was on a beach in Miami. Andressa Urach is Brazilian and the M...

Taylor Swift Private Topless Photo Leaked Or

Most of these sites promise visitors explicit pictures of celebrities, most of which will undoubtedly turn out to be generated by artificial intelligence (AI).

This, in itself, is not unusual. However, what stood out was that several of the Facebook posts had received a significant number of likes. Typically, users refrain from engaging with such content on Facebook, as the identities of those who like a post are publicly visible.

A high number of Likes for a post is great for the accounts posting these links, because when a Facebook profile or post gets more Likes it is more likely to show up in people’s feeds, which is basically more advertising for the same money.

So, how do the posts get these Likes?

It turns out that the criminals use a Trojan to promote their posts and profiles. When users click on links displayed on the adult sites, some selected visitors will download a Scalable Vector Graphics (SVG) image file. So, while navigating from one of these sites to the next, a download is sometimes—though not always—triggered.

Now, the cybercriminals are banking on the fact that SVG is not a file type that raises suspicion for most people, as it is commonly perceived as just an image file. However, SVG files are not always simple image files—they are written in XML, which allows them to contain HTML and JavaScript code. This means cybercriminals can exploit them for malicious purposes.

Here is the one provided by the adult sites:

Despite the heavy obfuscation in the second part of the script, it is fairly clear to anyone who can read the code that this file is malicious. In fact, it downloads another malicious JavaScript file, although identifying exactly which one was difficult.

Assume any SVG file using the '**hybrid JSFuck**' obfuscation technique is malicious. Analyze the more readable portions of the script to identify its behavior. If the script attempts to download and execute content from suspicious domains—such as crhammerstein[.]de—block the domain immediately and ensure endpoint protection tools like Malwarebytes are actively monitoring and responding to such threats.

JSFuck is a form of obfuscation that encodes JavaScript using only six characters: "[ ] ( ) ! +". There are several online DE obfuscators available for pure JSFuck obfuscation, but the criminals used a hybrid method by adding the String. From Char Code elements which is not that easy to unravel.

Opening the SVG file opens an empty Edge tab titled Process Monitor. This happens because SVG files on Windows are opened by Edge, even if the user has another browser set as their default.

Identify the downloaded script as JavaScript-based malware, specifically detected as Trojan.JS.Likejack. Recognize that this Trojan is designed to silently trigger 'Like' actions on Facebook pages—such as adult content posts—without the user's knowledge or consent. Ensure users are aware that the attack only works if they are logged into Facebook, which is common due to users keeping sessions open. Monitor for unauthorized Facebook activity and educate users to log out of social media accounts when not in use to reduce risk.

(B) Fake VPN and Spam Blocker Apps Tied to VexTrio Used in Ad Fraud, Subscription Scams.

BREAKING NEWS
FAKE VPN AND SPAM BLOCKER APPS TIED TO VEXTRIO USED IN AD FRAUD, SUBSCRIPTION SCAMS
A new report exposes how seemingly legitimate apps on Google Play & App Store are linked to ad fraud, shady subscriptions, and personal data misuse

VexTrio Viper, a known malicious ad tech group, has been found distributing harmful apps disguised as legitimate utilities on both Apple's and Google's official app stores.

According to an in-depth analysis by DNS threat intelligence firm Infoblox, shared with The Hacker News, these apps pose as VPNs, device monitoring tools, RAM cleaners, dating services, and spam blockers.

Apps have been released under multiple developer aliases, including HolaCode, LocoMind, Hugmi, Klover Group, and AlphaScale Media. These applications, available on both Google Play and the Apple App Store, have collectively been downloaded millions of times.

Upon installation, these fraudulent apps manipulate users into subscribing to services that are challenging to cancel, generate excessive advertising traffic, and exfiltrate personal data such as email addresses. Notably, the developer LocoMind was previously identified by Cyjax as a component of a phishing campaign delivering deceptive ads that falsely indicated device damage.

An example of such malicious software is the Android app Spam Shield Block, which claims to function as a push notification spam blocker but covertly imposes multiple subscription charges by coercing users into enrollment.

2. CYBER FRAUDS

(A) Retired forest official from Gujarat's Rajkot duped of Rs 8.93 lakh in digital arrest scam.

In a cyber fraud mirroring the recent Rs 19 crore scam in Gandhinagar, a retired forest head clerk from Rajkot, Gujarat, fell victim to a “digital arrest” con and lost Rs 8.93 lakh. Posing as officials from TRAI and Maharashtra Cyber Crime, the scammers extorted money from the elderly man by threatening him with criminal charges and arrest.

The victim, a former Forest Head Clerk at Rajkot. He received a call from a woman identifying herself as a fraudster from the Telecom Regulatory Authority of India (TRAI). She claimed that two Jio SIM cards linked to his number were being misused and needed to be deactivated immediately.

DIGITAL ARREST
The threat of digital arrest is a cyber fraud
Don't be afraid in such a situations, approach your nearest Police Station.
Don't be a victim of Cybercrime - Stay Vigilant
Fake Police/ED CB//Crime Branch
LIVE
Cybercrime Helpline
Call 1930
www.cybercrime.gov.in

Minutes later, a second call came from someone posing as an inspector from the Maharashtra Cyber Crime Cell. The caller alleged that an HDFC Bank account had been opened using the victim’s Aadhaar-linked SIM, through which Rs 68 lakh had been fraudulently transacted. The scammer claimed the money belonged to a woman who had since died by suicide and that an arrest warrant had been issued against the retired clerk.

As the victim hesitated, the imposter escalated the pressure. Through a video call, he showed a man in police uniform seated at what appeared to be a police station and claimed the only way to avoid arrest was to provide a security bond of Rs 2 lakh. Terrified, the retired official agreed to cooperate.

(B) Retired Army Colonel Trapped in Fake Herbal Seeds Purchase Deal, Swindled of Rs 89 Lakhs by Cyber Fraudsters.

A retired army colonel has become the latest victim of cyber fraudsters, losing a whopping Rs 89 lakh. The retired colonel from Dehradun was lured into buying herbal seeds worth lakhs of rupees, which are reportedly used to treat diseases like cancer and depression.

Based on the victim's complaint, the police have registered a case against unknown accused at the cybercrime police station and are investigating the matter. Cyber fraud cases are rapidly increasing in Uttarakhand. Recently, a woman was cheated of Rs 40 lakh under the pretence of starting a gold business.

In the retired colonel's case, according to the complaint, on June 12, 2025, a girl fraudster contacted him via Facebook, claiming to be a resident of Ukraine. She said she worked as a nurse at the Royal Infirmary Hospital in Bristol, UK. The fraudster then connected the colonel with a person who claimed to be the purchasing manager of Abbott Pharmaceutical. This person proposed a purchase and sale model for rare herbal seeds, which, the colonel was told, are used to make medicines for treating cancer, depression, and other diseases.

3. TIPS OF THE MONTH

A. How to Disable (Lock) Aadhaar Fingerprint Biometric Yourself.

1. **Use UIDAI's Biometric Lock Service Online**
   UIDAI provides an official **Biometric Lock/Unlock** service that lets you temporarily disable (lock) your fingerprint and iris biometrics so they cannot be used for authentication.
2. **Steps to Lock Fingerprint Biometrics:**
   - Visit the official UIDAI Biometric Lock/Unlock page: https://myaadhaar.uidai.gov.in/
   - Enter your 12-digit Aadhaar number.
   - Verify with an OTP sent to your registered mobile number.

- Select the option to **lock** your biometric data (fingerprint + iris).
- Submit the request.

3. **What Happens After Locking?** Once locked, your fingerprint and iris cannot be used for authentication (e.g., at banks, services requiring Aadhaar biometric). Instead, you'll have to authenticate using OTP or other means.
4. **You Can Unlock Anytime** If you need to use biometrics again, you can unlock them anytime using the same website and OTP verification.
5. **Important Tips:**
   - **Use your registered mobile number** to receive OTP, since locking/unlocking requires mobile verification.
   - **Do not share your OTP** with anyone.
   - Only use the **official UIDAI website** to lock/unlock biometrics. Avoid third-party apps or websites.
   - Keep your **Aadhaar number and mobile secure** to prevent unauthorized locking or unlocking.
6. **If You Don't Have Access to Registered Mobile** Visit the nearest Aadhaar Enrollment Center to update your mobile number first, as OTP-based verification requires the registered mobile.
7. **Regularly Monitor Aadhaar Authentication History** Check your Aadhaar usage history at https://uidai.gov.in to spot any unauthorized biometric authentication attempts.

Important Security Advisory for All Users

Do NOT install any mobile application from the Google Play Store or Apple App Store that has not been officially prescribed or approved by the IT Wing Directorate for official use.

Unauthorized or unverified apps may contain malicious code and pose a serious threat to personal and organizational data.

Additionally, never share official or sensitive personal details such as:

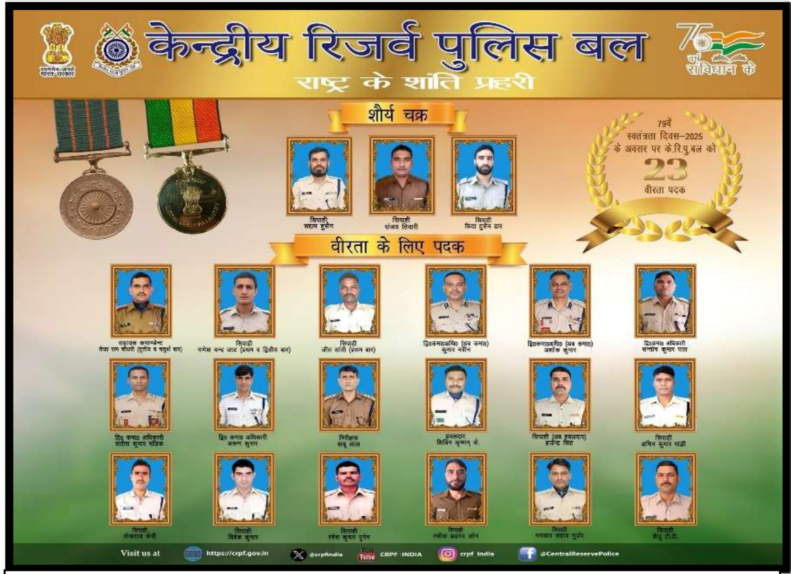
- Force Number / IRLA Number
- Full Name
- Date of Birth
- Place of Posting
- Salary or Financial Information
- Any internal communication or access credentials

Such information can be misused by cybercriminals for impersonation, identity theft, or targeted attacks.

Beware of fraudulent apps and social engineering attempts. Stay alert. Stay secure.

The Mega Blood Donation Campaign 5.0 by AIIMS New Delhi, 555 CRPF personnel donated blood, with Shri G.P. Singh, DG CRPF.

Inspired by PM Modi, CRPF launched a BMI campaign. The DG recorded his BMI at NS Hospital.


केन्द्रीय रिजर्व पुलिस बल
राष्ट्र के शांति प्रहरी
75 वर्ष संविधान के
शौर्य चक्र
सिपाही सद्दाम हुसैन
सिपाही संजय तिवारी
सिपाही फिदा हुसैन डार
79वें स्वतंत्रता दिवस–2025 के अवसर पर के.रि.पु.बल को 23 वीरता पदक
वीरता के लिए पदक
Visit us at https://crpf.gov.in @crpfindia CRPF-INDIA crpf_india @CentralReservePolice

On the 79th Independence Day, 23 gallantry medals, including 3 Shaurya Chakras, were awarded for bravery.

During his visit to 136 Bn RAF, DG CRPF met martyrs’ families, celebrated a Veer Putri’s birthday, and felicitated all present.

Shri Praveen Vashishtha, Special Secretary (Internal Security), MHA, was the Chief Guest at the CRPF Officers Institute, New Delhi.

Srinagar Sector CRPF held a Tiranga Rally at Dal Lake for the Har Ghar Tiranga campaign.