ChatGPT

Stolen Photos and Fake Persona “Sweet Baby Girl”

The scammer behind **“Sweet Baby Girl”** sent multiple personal photos to build credibility and emotional connection. These included selfies in casual settings and even one in a U.S. Army uniform with the name **“LEWIS”** visible on the name tape [1]. In chat, she referred to herself as “the beautiful Brandy Lewis” [1], suggesting the persona’s name. A reverse image search strongly indicates these pictures are **stolen** from a real individual’s social media (likely an actual woman named Brandy Lewis, who appears to be a U.S. service member). In other words, the scammer is **impersonating** someone else’s identity. This is a common tactic in romance scams – fraudsters lift photos of attractive people (sometimes in military uniform) from Facebook or Instagram and use them as their own. In fact, online scam victim communities have spotted profiles using the name *Brandy Lewis* (e.g. “Brandy Lewis Monroe”) in connection with military romance scams [2]. **None** of the pictures the scammer sent are likely original; they are **publicly-sourced images** reused to craft a fake persona. The variety of photos (including a uniformed shot, casual selfies, etc.) makes it clear the scammer had a trove of someone’s personal images, not just a single stock photo.

> **Red flags:** Romance scammers often **refuse live video chats** and stick to sending pre-existing photos. In this case, “Sweet Baby Girl” avoided video calls, making excuses (e.g. claiming poor connectivity on base) – a sign the person in the photos is not actually the person you’re talking to. The **push to move off the dating app** quickly is another warning sign: she asked the victim to delete the app and talk only on WhatsApp almost immediately [3], which isolates the victim from the safety features of the dating platform. These behaviors, combined with the too-perfect photos, suggest the persona is completely fabricated for the scam. A genuine new love interest wouldn’t mind video chatting or staying on a platform where they initially met, but a scammer needs to control the communication channel.

Military Service Claims – Inconsistencies and Red Flags

The scammer’s backstory was that she had **served 10 years in the U.S. Army** and was *“living in the barracks”* as a *“junior”* service member. At face value, parts of this story strain credulity. Typically, after a full decade in the Army, a soldier would have risen in rank and **not be considered “junior”** anymore. An enlisted soldier with ~10 years of service is likely an NCO (Non-Commissioned Officer) such as a Sergeant (E-5) or Staff Sergeant (E-6). Notably, Army regulations usually require single personnel **E-5 and below** to live in barracks, but **E-6 and above can live off base** in the U.S. [4]. If she truly had 10 years of service, it would be **unusual to still be barred to barracks housing**, unless she had never been promoted beyond E-5. That’s possible but uncommon for someone with a decade of experience. The scammer’s claim of being in the barracks thus raises an eyebrow – it’s likely a convenient lie to explain why she can’t talk freely or meet up (scammers often pretend to be deployed or on base to avoid in-person meetings).

Another flag is the way she described her military role. When asked directly **"What's your MOS?"** (military occupational specialty code), she gave an evasive answer: *"Administrative specialists assistant"* [5]. This is **not a real MOS title** in the U.S. Army – it sounds clumsy and incorrect. U.S. soldiers typically respond with a code (e.g. "42A" for Human Resources Specialist) or a specific title ("I'm a Human Resources NCO"). The scammer's vague answer and phrasing (using *"assistant"* and plural *"specialists"*) suggests she didn't actually know a legitimate MOS. When pressed again, she only repeated that she does *"paperwork for my superiors"* [6]. This kind of **non-specific description** is a hallmark of impostors. A real soldier would naturally say something like "I'm a 42-Alpha working in admin," rather than *"majorly paperwork"*. Indeed, throughout the chat her language about the military was off. For example, she referred to *"when I was in the military camp some years ago"* [7] – phrasing no actual service member would use (they might say "in basic training" or simply "when I was in the Army," not *"military camp"*). These odd terms and grammatical mistakes (e.g. *"Your more of a remote worker Yes?"* instead of "You're…right?" [8]) hint that English may not be her first language and that she's **not truly familiar with U.S. military culture**.

Additionally, the **scenario and timeline** she gave have inconsistencies. She claimed to be stationed at *Joint Base McGuire-Dix-Lakehurst (JBMDL)* in New Jersey (a real military base) and said she'd moved from Mexico to Ohio as a teen – details likely pulled together to make her seem authentic [9] [10]. But while she knew the base's name, she avoided any discussion of actual unit, rank or duties beyond *"paperwork."* When the conversation got more personal, she steered away from military topics, which is common for impostors once they've established that thin veneer of credibility.

> **Red flags:** The combination of **unrealistic service details** (a decade-long career still "junior" enough to be stuck in barracks), **incorrect military lingo**, and reluctance or inability to discuss her supposed Army life in depth is a strong indicator of a scam. Genuine service members take pride in their specific roles and usually don't shy away from basic questions about their job or rank. Furthermore, the scammer was **extremely quick to profess love and jealousy**, even **making the victim swear fidelity "by the Bible" within days** [11] [12]. This rapid emotional escalation is not directly about military service, but it's another hallmark of a romance scam – scammers rush intimacy to lower your guard. In this case, she went from small talk to *"I love you"* and *"you belong to me"* in essentially 48 hours, which is highly implausible in a real relationship. She also inquired unusually much about the victim's finances, asking how much money he makes per month [13] and even (before deleting a message) whether he'd buy her things *"that money can buy"* if she asked [14]. A real Army officer or enlisted member isn't going to fixate on your salary or push you to abandon a dating app immediately – those are **scammer tactics**, not the behavior of a genuine romantic partner.

HackLoop Scam Organization Profile

HackLoop is the fraudulent outfit likely pulling the strings behind this romance scam (or poised to exploit it). HackLoop is a known **scam ring** that has been active since at least **2017**, operating under aliases like **"hackloop606," "hackloopjameson,"** or sometimes **"Loophack."** Despite the name implying a hacker collective, all evidence shows it's a **criminal scam operation** [15]. HackLoop advertises itself as a kind of "hacker-for-hire" or **"cryptocurrency recovery"** service, claiming they can do everything from recovering stolen Bitcoin to hacking social media accounts or even selling counterfeit money [15] [16]. In reality, they do not deliver any legitimate services – their game is to **collect upfront fees** from victims and disappear. They

often target people who have already been victimized by other scams, a cruel practice known as a **recovery scam** (e.g. someone who lost money in a crypto scam finds HackLoop's info and, hoping to get their funds back, ends up paying HackLoop and being scammed again) [17] [18].

HackLoop's footprint across the internet is extensive and **infamous**. They use free Gmail addresses like *hackloop606@gmail.com* and *hackloopjameson@gmail.com*, and have promoted themselves on social media and forums. For instance, on a Moneylife article's comment section, a HackLoop scammer posed as a satisfied customer and wrote *"a colleague referred me to hackloop606@gmail.com, he was able to help get back my money...you can contact him for help too"*, which was a **fake testimonial** planted to lure victims [19] [20]. They've spammed tech forums and Bitcoin discussion boards with similar messages – in one case pushing *hackloop606@gmail.com* as a solution for a fake crypto exchange scam until forum users flagged it as fraud [21]. On the Nigerian forum **Nairaland**, user **"Hackloop606"** openly advertised illegal hacking services in 2019, listing capabilities like "Bitcoin hacks, bank account hacks, clearing criminal records" and providing that same Gmail and a phone number [22]. The ads boasted *"100% secure and discreet"* service with *"proof before payment,"* which is itself a huge red flag – legitimate cybersecurity professionals **never advertise on random forums** or guarantee illicit outcomes [22]. HackLoop even abused platforms like **Trustpilot**: in October 2019, an account by the name **"Hackloop606"** spam-posted a **"review"** on a spy gadget store's page, brazenly listing a menu of hacking services and their contact info (Gmail and a WhatsApp number) [23] [24]. The content of that spam review is telling – it offered *"Blank ATM cards, credit score upgrade, loans, Bitcoin hacks, counterfeit notes, clearing criminal records, social media hacks, school grade changes"*, and more, all via the **HackLoop email and WhatsApp** [16] [25]. They also provided a WhatsApp number (+1-331-276-2645 and +1-631-253-1527 have been used) in these ads [26] [27], which appear to be VoIP numbers with US area codes to seem legitimate. In reality, most actors behind this are believed to be overseas – notably, the Nairaland connection suggests **Nigerian scammers**, and the writing style and tactics align with West African scam rings. (Using a **U.S. phone number and an English name** like *"Jameson"* or *"James"* is deliberate, to instill trust in victims who might hesitate to deal with someone in Nigeria [28].) No genuine cybersecurity firm or "recovery expert" operates via an untraceable Gmail and random forum posts – **HackLoop is thoroughly fraudulent** [17] [29].

Known aliases and infrastructure: The group uses various names that play off the "hack" theme. **Hackloop606** was an early moniker (the number might be arbitrary or signify something to them), and more recently **HackloopJameson** (or sometimes **LoopHack**). The "Jameson" persona is likely fictitious – there's no real individual by that name fronting a company; it's just a handle to make it sound like a single *"expert"* [29]. They've created at least one Facebook page (titled *"Hackloop Crypto Recovery"*) advertising since 2017 that they recover lost Bitcoin, etc. [30]. Emails associated with them include the @gmail.com addresses mentioned, and they often solicit contact via **WhatsApp chats** (one number they gave, 331-276-2645, is an Illinois number [26], and another 631-253-1527 is New York-based [27]; both likely virtual). **No legitimate business hides exclusively behind anonymous Gmail/WhatsApp**. This lack of transparency and the absence of any verifiable identity or physical address is a giant warning sign noted by consumer protection agencies [31] [32]. The U.S. Federal Trade Commission explicitly warns that **"recovery service"** offers asking for upfront payment are almost always scams [33] [34] – HackLoop fits this pattern to a T.

Scam repertoire: HackLoop is versatile in the scams it runs or facilitates. Primarily, it's known for **"refund/recovery" scams** [35] [36] – scamming people who were already scammed elsewhere (like online shopping fraud, crypto investment fraud, etc.) by promising to recover lost funds for a fee. They have also promoted **hacker-for-hire scams**, where they lure customers who want illegal services (hacking someone's Facebook, changing grades, making fake money). In those cases, the "customer" is actually trying to engage in

wrongdoing, so when HackLoop takes their money and vanishes, the victims are often too embarrassed or afraid to report it. Additionally, there are indications HackLoop (or affiliates of it) might engage in **romance or bait scams** as well. The persona "Sweet Baby Girl" could be one way to **bait a victim into trust**, and then either directly extort money or funnel the victim into another scam (for example, the scammer could at some point say, *"I have a problem with my bank/crypto account, but I know a trusted hacker who can help – his name is Jameson from HackLoop"*, thereby roping the victim into contacting HackLoop for "help"). This kind of **cross-connected scam** isn't unusual; the scammers will maximize any angle to get paid. Even if the romance itself was heading toward asking the victim for money (for a fake emergency, "leave papers fee," etc.), HackLoop could be the backend team to receive those funds (they often ask for payment in hard-to-recover forms like cryptocurrency or wire transfers). It's also possible that **HackLoop provided the fraudulent documents or playbook** for the romance scam – large scam rings share resources. For example, the intense love proclamations, the scripted lines about *"you belong to me"*, and the sudden mention of material needs are all part of a known **romance scam script** [37]. HackLoop, being active on many scam fronts, likely has a hand in crafting such scripts or training scammers.

Geographic patterns: Many clues point to West Africa (particularly Nigeria) as the base of operations for HackLoop. The open advertisements on **Nairaland (a Nigerian forum)** [22], the style of English in their posts, and the trend of Nigerian scam rings running both romance and recovery scams support this. However, they obscure their true location by using U.S. contact info and claiming to be *"100% discreet."* Victims have reported that once they pay HackLoop (often via Bitcoin or Western Union), the communication goes dark or they're strung along with excuses – classic of scam operations that are likely offshore. Law enforcement and scam trackers are aware of HackLoop; its name surfaces in anti-scam forums and even in an FTC consumer advisory [33] [34]. Unfortunately, because they operate online through aliases, shutting them down is challenging – as soon as one email/number is reported, they pop up with a variation (e.g. Hackloop**607** or different Gmail).

Public warnings: In summary, any encounter with **"HackLoop"** in any form (be it hackloop606@gmail.com, hackloopjameson, or a supposed hacker named Jameson offering services) should be treated as **highly suspect** and almost certainly fraudulent. Numerous community posts and reports have flagged HackLoop as a scam over the years [38] [17]. No legitimate professional recovers stolen money by asking for a fee via Gmail, and no honest hacker advertises in blog comments and forums. If someone claiming to be a **soldier or romantic interest** ever refers you to a service like this – or if you find HackLoop by googling a way to get your lost money back – **know that it's a con**. The best course is to cease contact immediately. In this case, the persona "Sweet Baby Girl" displayed many of these red flags, and the likely involvement of HackLoop means any money sent to them would have disappeared. It's a tangled web, but recognizing these signs – stolen photos, inconsistent personal details, and the shadow of an organization like HackLoop in the background – can help others avoid falling victim to such **romance bait and recovery scams**.

Sources: The analysis above is supported by connected investigations and reports. For example, a detailed investigation into **hackloopjameson@gmail.com** confirms that *"Hackloop"* is a scam operation using aliases like Hackloop606, posting fake testimonials, and advertising illegal hacking services on forums [19] [22]. Scam warning communities on Reddit and Facebook have similarly identified **HackLoop contacts as frauds**, often tied to recovery scam attempts [17] [29]. The **Trustpilot spam review** by *Hackloop606* (Oct 2019) explicitly lists their outrageous service menu and WhatsApp, which is a public record of their scam advertising [24] [39]. Additionally, U.S. Army housing policy documents note that by **10 years in service** (often E-6 rank), a soldier wouldn't typically be forced to live on-base [4] – contradicting the scammer's claims. All these sources reinforce the conclusion that *"Sweet Baby Girl"* was a crafted persona in a broader

fraud scheme, and that **HackLoop** (whether as the scammer group or later “recovery” pitch) is a known scam entity to be avoided. [1] [5] [20] [24]

---

[1] [3] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] WhatsApp Chat with Sweet Baby Girl.txt
file://file-Kb424ioEKunfzwGhymUXrQ

[2] Fake profile, created 4 days ago! | Facebook
https://www.facebook.com/groups/461638187343012/posts/3011543465685792/

[4] BASE HOUSING | Housing | Benefits Handbook - Military Times
https://ec.militarytimes.com/benefits-handbook/housing/base-housing/

[15] [17] [18] [19] [21] [22] [23] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [38] Investigation of __hackloopjameson@gmail.com__.pdf
file://file-QZJ25mgYZXzYHtE8whoNHM

[16] [24] [25] [26] [39] Spy World Reviews | Read Customer Service Reviews of www.spyworldmiami.com
https://www.trustpilot.com/review/www.spyworldmiami.com

[20] Cheated in online shopping? Here is how you can get justice
https://www.moneylife.in/article/cheated-in-online-shopping-here-is-how-you-can-get-justice/33172/66119.html

[37] The Nigerian Scammer's Playbook - Paladin Risk Solutions
https://paladinrisksolutions.com/bluesky/the-nigerian-scammers-playbook/