



# FEDERAL BUREAU OF INVESTIGATION

## Public Service Announcement



### **Alert Number: I-081026-PSA | 10 August 2026 Sexual Exploitation Actors Stealing and Leaking Explicit Content**

The Federal Bureau of Investigation (FBI) warns the public about sexual exploitation (SE) actors targeting adult and underage victims<sup>1</sup> by illegally accessing their social media and personal accounts to steal and post their explicit content (also known as non-consensual intimate images, or NCII) for sale on criminal marketplaces. SE actors are using a variety of social engineering and cyber intrusion tactics to target specific individuals of interest — who may or may not be known to the actor — or general targets of opportunity. Once the sexually explicit images or videos are accessed and stolen, typically unbeknownst to the victim, SE actors are sharing or posting the content within community forums or selling them to illicit marketplaces. Personally identifiable information — such as name, date of birth, email, phone number, and social media username — is often posted along with the victim's explicit content, exposing them to continued re-victimization.

#### **How EXPLICIT CONTENT IS ACCESSED AND EXPOSED**

The FBI has observed SE actors using various tactics for illegal access to victim accounts, including:

1. **Password and PIN Targeting:** SE actors use high volume password and PIN attempts on social media and personal accounts based on curated lists obtained from a variety of sources, such as data leak sites, social media, and open source. The lists include personal information, such as date of birth or name variations, when the victims are known to them.
2. **Social Media Customer Service Impersonations:** SE actors send victims text messages stating their social media account is being disabled or locked unless they respond with a verification code. SE actors then request a password reset for the victim's social media account, which generates a code and is sent to the victim. Once the victim shares the code, the SE actor can reset the victim's password and access the account.
3. **Phishing:** SE actors create look-alike domains and email accounts emulating social media customer support to notify victims about "new logins" into their account. The impersonated emails include a malicious embedded link to "change [their] password," and once clicked, SE actors gain access to the account.

Once the sexually explicit content is stolen, SE actors post or sell it to criminal marketplaces, which often includes personal information about the victim and typically without their knowledge. As a result, victims often face re-victimization

through harassment, sextortion, stalking or other targeted attacks, such as advertising stolen content on a victim's own social media page.

### **TIPS TO PROTECT YOURSELF**

- Avoid storing sensitive images or videos on social media platforms or Internet-accessible sites.
- Use unique, complex passphrases and PINs and use multi-factor authentication methods. Avoid using information that is directly associated with your identity, such as your or a loved one's name, birthday, or other personally related information.
- Be cautious about clicking on embedded links in emails and text messages.
  - Go directly to the website to address account concerns; or
  - Consider viewing emails from a computer to hover over embedded links, verify URLs, and inspect for potential formatting inconsistencies in the email address or URL. Viewing from a mobile device could cause emails to appear legitimate at first glance.
- Use caution if you receive a temporary password, PIN reset, or access code you did not request. Do not share login information with anyone, even if the requestor claims to be associated with a platform or service with which you have an account. Go directly to the service's website or official app to change your password or PIN, if necessary.

### **REPORT IT**

If you believe you are a victim of SE actors stealing and leaking explicit content, please visit <https://ncii.ic3.gov> to provide information related to the following:

- Timeframe when your content was accessed or stolen without your permission.
  - Whether you were under the age of 18 in the images and/or videos.
- How the images and/or videos were obtained (e.g., social media, cloud storage, scam, sextortion or blackmail).
  - On which social media or cloud storage platforms your content was found.
  - The usernames or registered emails/phone numbers associated with your accounts.
- The names and links to the sites where your content was posted.
- Any further harassment, extortion, stalking, or other acts by phone, email, text, social media, or in-person targeting you may have experienced.
- Any actions you have taken since discovering your content was stolen (e.g., contacting law enforcement, etc.).

Continue to report frauds, scams, and cyber threats to [www.ic3.gov](http://www.ic3.gov) or contact your local [FBI Field Office](#). For immediate threat-to-life concerns, please call 911.

### **ADDITIONAL RESOURCES**

- National Center for Missing and Exploited Children (NCMEC) - <https://www.missingkids.org/home>
- NCMEC's NetSmartz Initiative - <https://www.missingkids.org/netsmartz/home>
- National Center for Victims of Internet and Cyber Exploitation - <https://ncvic.org/>
- Federal Trade Commission's "Take It Down" Portal - <https://takeitdown.ftc.gov/>
- On the Internet: Be Cautious When Connected — FBI: <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/on-the-internet>

DISCLAIMER: The information in this document is being provided "as is" for informational purposes only. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI.

---

<sup>1</sup>Unless otherwise stated, the use of the term "victim" in this product does not imply that the individual or entity meets the definition of "victim" in the Victims' Rights and Restitution Act (VRRRA), *34 U.S.C § 20141* or the Crime Victims' Rights Act (CVRA), *18 U.S.C § 3771*, or that the individual or entity has been identified as a victim in an FBI investigation.↩