

Assignment 14

1. Choose a fake profile on any social media platform of your preference and identify the red flags signalling its fraudulent nature.

Tracking Down Fake Social Media Accounts

Scammers, fraudsters, hackers, and just plain mean people create fake social media accounts by the thousands every day. Anyone can be a target – celebrities, influencers, businesses, and even regular people. In fact, in the first quarter of 2022, Facebook took action on **1.6 billion fake accounts**. And that is just one social media network.

You might have seen some of these imposter accounts as you scrolled through your social media feeds or checked your DMs. Fraudsters often take pictures and posts from real high-profile pages, use a similar name, and reach out to the followers of the real page with the intention of scamming them.

These accounts are extremely harmful. In turn, this activity has prompted both brands and high-profile individuals to better trace and report fake accounts that may be reputational damaging.

In this, we'll discuss:

- What fake social media accounts are
- How fake accounts affect brands
- Can fake social media accounts be traced?
- How to identify fake accounts
- How to take action against fake accounts on Instagram, Facebook, Twitter, etc.
- How to protect your brand from getting impersonated on social media

Let's dive in.

What are Fake Social Media Accounts?

Fake social media accounts are profiles that are either not associated with a real person or are created with an actual person's personal information without their consent. These accounts are usually called imposter accounts or sock puppet accounts. The latter is mainly used to describe accounts run by people to praise themselves and criticize others.

Scammers create fake social media accounts for various reasons, including:

- To impersonate you or others

- To extort money from your followers through scams (usually by pretending that the original owner of the account is in trouble and needs donations)
- To **harass people online**
- To spread false information – usually political – and hate speech
- To leave **false reviews or complaints** about brands and their products/services
- To destroy a person's reputation

Most, if not all, of the major social media platforms (i.e. Facebook, Twitter, Instagram, LinkedIn, Pinterest, YouTube, and Snapchat) are plagued with fake accounts. Even some minor platforms (Quora, Tumblr, etc.) and dating apps have fraudsters pretending to be other people.

How Do Fake Accounts Affect Your Brand?

Brands of all sizes and industries need to be wary of fake social media accounts. It's important to watch out for them on two fronts: fake accounts that impersonate your brand and fake accounts that follow your real brand account.

People who create fake accounts to impersonate your brand can trick your followers into thinking that they're your brand. This makes it easy for them to promote your products or services to people, and collect their money with zero intention of delivering the offerings.

This can destroy your reputation, reduce your followers, and ruin your brand.

On the flip side, you have fake social media accounts that follow your real brand account. At first glance, these bots merely inflate your follower count but don't actively cause trouble. This couldn't be farther from the truth.

While these bot accounts may not harass you repeatedly or leave divisive comments under your posts, they do harmful things like:

- Lower your overall engagement rate.
- Damage your credibility if a prospect looks at your follower list and finds out that a good chunk of your followers are, in fact, not people at all.
- Make it harder to segment your audience and create effective social media ad campaigns.

If you only have a few hundred followers, you can easily find, unfollow, and report these fake accounts. But if your brand has thousands of followers, this process becomes a lot trickier.

If you have a large following, we advise you to constantly scan your account(s) with the right tools like Botometer to get rid of fake followers.

Can You Trace Fake Social Media Accounts?

Our social media investigators often hear this question: Is it possible to trace online accounts? Unfortunately, the only real answer is: it depends. While we have successfully been able to trace many fake accounts, it is almost always an uphill battle. But, if it can be done, we can do it.

The people behind these types of accounts create them with the intention of **evading identification**. There are many easily available tools and techniques that can make tracking these accounts impossible. These accounts are usually set to anonymous and contain little visible information.

Even so, in this digital age, every online action leaves a digital footprint. When this digital footprint hasn't been expertly masked and/or the perpetrator gets sloppy covering their tracks, our **social media investigators** can trace this digital footprint.

How to Identify a Fake Social Media Account

Impersonators are getting smarter and they're making fake social media accounts harder to trace these days. However, if an account is fake, there's always a sign (or a few signs). If you want to be sure if a social media account is fake or not, check the following elements:

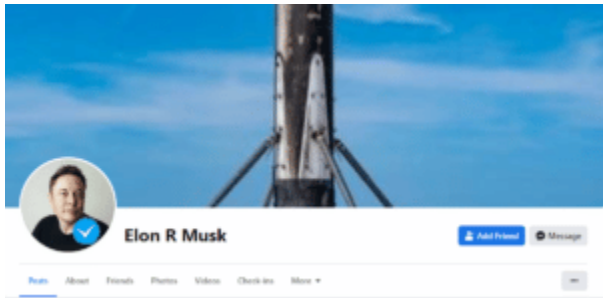
Profile Picture

Fake accounts often use avatars and symbols as their profile images, instead of photos. And when they do use actual human photos, they are usually low resolution. Low-res pictures can be a red flag when the account purportedly belongs to a public figure or celebrity.

To be sure whether the account is fake or not, run the profile picture through search engines like Google Image Search to see if the image is linked to another account or has appeared somewhere else on the internet.

Account Name & Profile URL

Scammers often change their Facebook or Twitter usernames after signing up on the platform. This can give you a clue as to whether an account is real or fake.



Take this Facebook account as an example. It's supposedly owned by Elon Musk.

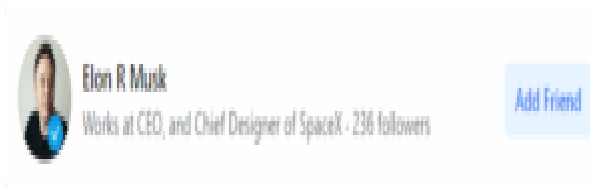
The first red flag in this profile is the use of Elon's middle initial 'R'. The account is registered at this URL (web.facebook.com/profile.php?id=100083227784922), which shows no vanity name was set for this account, making it unlikely to be Elon Musk's actual Facebook page.

To further verify the authenticity of an account like this, check if the said person is registered on other social media networks with the same name. Also check if the profile image, bios, location, and contact details match up.

If there is significant overlap, then the account is likely genuine. If not, you're probably dealing with a fake account.

Connections (Followers, Friends, & Subscribers)

How likely it is that Taylor Swift has 3,857 Twitter followers? Or that tennis superstar, Serena Williams, has a mere 126 Facebook friends? Not likely, right?



Using the fake Elon Musk example from above, that account has 236 followers—which is weird for somebody as popular and controversial as Elon Musk.

To check if this is Musk's real account or not, search for Musk's verified Twitter account and compare it to this Facebook account. On Twitter, Elon Musk has 104 million followers, which is a far cry from 236 Facebook followers.

When you spot a huge discrepancy in a person's follower count across different social media platforms, there's a good chance the account with the lower number is fake.

Another way to confirm if a public figure's account is real or not is to check if other verified accounts follow or interact with it. If yes, it's most likely real. If not, you're dealing with a fake account.

Content

Pay attention to the kinds of posts published on the social media account. Check if it matches the person or seems out of character.

Fake accounts often spread false information and extreme views, and their feeds are usually filled with memes, stock photos, and recycled images. No published posts is also a sign of a fake account.

Also, check the kinds of comments the account leaves on other people's posts. If they leave the same (or similar) comments asking people to invest money or subscribe to a sketchy channel, it's likely a fake account. This can also indicate that the account is actually a bot.

The use of slurs, curse words, or weird slang can also give away the illegitimacy of a fake account.

Verification Symbol

If you find a social media account that seems as though it's owned by a celebrity, influencer, or reputable brand, check to see if it has a blue or green checkmark next to the account name. The checkmark indicates that the account is verified.

Social media platforms give public figures this mark to protect them from being impersonated. However, not all legitimate public figures have the checkmark yet.

In this case, search other social networks for accounts with the same name. If the profile pictures, account name, location, and other details match up, the account is likely real. If they don't, it's probably fake.

What Should You Do When You Find a Fake Social Media Account?

If you suspect an account is fake, the first thing to do is check if you're following the account. If you are, unfollow it or remove it from your friends list immediately.

You can even block the fake account to restrict its access to your information.

Social media platforms like Facebook and Instagram recommend reporting any fake profiles or filling out their forms. Here's how you can report a fake account (for the major social platforms):

Note: If you plan on hiring a professional cyber investigator to track down who's behind the account, talk to them first, before reporting the account, because once it has been removed from the internet, it can be much harder to trace.

Facebook

- Go to the fake account or page and click the button with three dots at the bottom of the cover photo.
- If the fake account is for an individual, click Find support or report. If the fake account is for a Facebook page, click Report Page.
- Follow the instructions on the screen to file a report.

You can also report a fake account through Facebook Messenger by scrolling down and clicking Something's Wrong.

If you don't have a Facebook account or don't have access to your account, you can still report a fake account via [this contact form](#).

Instagram

- Visit the profile and click the three dots beside the account name.
- Click Report and follow the on-screen instructions to file a report.

Or you can report fake Instagram accounts created in your name, the name of your business, organization, or your child via [this form](#). You have to provide all the requested information, including a picture of your government-issued ID.

Twitter

- Go to the fake profile and click the three dots beside the account name.
- Click Report [@fakehandle].
- Select your reason(s) for reporting the account and submit.

You can also report fake Twitter profiles via [this form](#). You don't need a Twitter account to report a fake account.

LinkedIn

- Visit the fake profile or company page and click more under their account name and tagline.
- If it is an account for an individual, click Report/Block. If it's a company page, tap Report Abuse.
- In the what do you want to do? pop-up window, select Report content on profile.
- Then tap Profile information in the what content on this profile are you reporting? Pop-up window.
- Click Suspicious, spam or fake in the Why are you reporting the profile information on this profile? Pop-up window.

- Select Fake account in the How is this suspicious, spam, or fake? Pop-up window.
- Tap Submit to file the report.

Pinterest

On the Pinterest app, you can only report a profile for spam. If you notice a fake Pinterest account impersonating your brand, [contact Pinterest](#) by selecting Report harassment or exposed private information.

When you report a fake account, the support team of the social network will investigate the issue. If they determine that the reported account is, in fact, fake, they will deactivate or ban the account from the platform.

Bots & Trolls: Are They the Same?

Where there are fake social media accounts, bots and trolls are not far behind. However, bots and trolls are different from each other.

Bots

Bots, short for robots, are artificial accounts that relentlessly share content on social media, comment on posts, and initiate online debates on trending or overlooked topics.

As the name suggests, their behaviour is similar to that of automated robots. Bots are often part of a botnet—a network of bots. They are almost never singular.

There are good and bad bots on social platforms.

Good bots automatically share the news, earthquake alerts, satellite images, or weather forecasts on social media.

Bad bots, on the other hand, are designed to mimic real human activity to push an agenda or scam. Depending on its algorithm, bad bots may post content or comments on social media, follow legitimate accounts, and even send out friend requests.

How Do You Spot Bots?

Like fake social media accounts, you can detect bots by paying close attention to:

- **Account Names:** Bot usernames consist of a weird mix of words, letters, numbers, and even characters.

- **Profile Pictures:** Bot accounts usually have no profile picture. And when they do, it's usually an avatar or an image of a cartoon character/animal/object. Whenever they use a photo of a person, the image is usually low-resolution.
- **Profile Details:** Bot accounts usually have little to no profile information and a sketchy location that doesn't seem to match the person who supposedly owns the account.
- **Weird Online Behaviour:** If you notice a single social media account publishing similar and/or crude content across several platforms or underneath several posts, it's probably a bot.
- **Few to No Followers:** Bots usually follow a large number of accounts, but have a very low number of followers on their own accounts. To analyse follower counts, use tools like Botometer or Follower wonk.

Trolls

Trolls are real human beings who create social media accounts to display destructive behaviour, such as making insulting comments on posts, sending multiple disrespectful DMs, etc. Trolls are often paid to harass celebrities, public figures, or media organizations. They also often engage in this behaviour to satisfy a personal grudge.

How Do You Spot Trolls?

Troll accounts are a bit more difficult to spot than fake accounts or bots because they are controlled by real people. Identifying troll accounts becomes even harder if they were registered and in use for years as part of bigger troll networks.

Spotting troll accounts goes beyond checking profile pictures, account names, bio information, or suspicious follower counts. However, you should check those just to be sure. The best way to find troll accounts is to examine the content shared by the account.

- Does it link to websites that spread disinformation? One of the main signs of troll accounts is spreading disinformation.
- Does the user publish any personal posts at all? If they only post (or repost) third-party content, they may be a troll.
- Does the user post the exact same comment under different social posts? If they do, then you're probably dealing with a troll.
- Does the user spend a lot of time making comments on online discussions? If yes, they probably are a troll—especially if the comments are vitriolic and negative.

What are the Consequences of Creating a Fake Social Media Account?

When you report a fake social media account to the platform and the support team confirms that the account is, indeed, fake, they usually ban or deactivate the account immediately. Typically that's where it ends, unless the victim wants to push it further. If the victim wants to pursue the matter, they have to look to their local laws to see what their options are.

While creating a fake account on social media in itself usually isn't a crime, what the person does with the account might be. Most fake accounts are created for parody and satire. That is not illegal in U.S. law. Creating a fake account becomes illegal when the owner uses the account to commit one or more of the following crimes:

- **Revenge Porn:** This consists of distributing sexually explicit images without the consent of all involved parties.
- **Online Harassment:** This consists of actions like hacking, cyberbullying, cyber stalking, cyberattacks, and more.
- **Defamation/Libel:** This is the act of spreading false and harmful information to hurt a person or damage a business's reputation.
- **Impersonation of a Law Enforcement Official:** One may get away with impersonating a private citizen or celebrity. But impersonating a law enforcement official or a public servant, in general, is a crime.

If you own a fake social media account and can prove to the courts that you use the account for parodies and satire, you may be able to walk away with no criminal or civil charges. However, if you use the account to hurt people or brands, you could be charged with any number of crimes, such as a hate crime, or face any number of civil penalties.

The 7 biggest red flags you should check for when you receive an email or text.

1. Urgent or threatening language

Real emergencies don't happen over email.



Look out for:

- Pressure to respond quickly
- Threats of closing your account or taking legal action

2 .Requests for sensitive information

Anyone asking for personal information over email or text probably shouldn't be trusted with it, anyway.



Look out for:

- Links directing you to login pages
- Requests to update your account information
- Demands for your financial information, even from your bank.

3 .Anything too good to be true

Winning a lottery is unlikely. Winning a lottery you didn't enter is **impossible!**



Look out for:

- Winnings from contests you've never entered
- Prizes you have to pay to receive
- Inheritance from long-lost relatives

4 .Unexpected emails

Except the unexpected, and then send it right to the **trash.**



Look out for:

- Receipts for items you didn't purchase
- Updates on deliveries for things you didn't order

5. Information mismatches

Searching for clues in phishing email puts your love of true crime podcasts to good use.



Look out for:

- Incorrect (but maybe similar) sender email addresses
- Links that don't go to official websites
- Spelling or grammar errors, beyond the odd typo, that a legitimate organization wouldn't miss

6 .Suspicious attachments

Attachments might seem like gifts for your inbox. But just like real gifts, they're not always good...



Look out for:

- Attachments you didn't ask for
- Weird file names

- Uncommon file types

7. Unprofessional design

For some reason, hiring a graphic designer isn't on a cyber criminal's priority list.



Look out for:

- Incorrect or blurry logos
- Company emails with little, poor or no formatting
- Image-only emails (no highlightable text)

If you spot any of these red flags in a message:

- don't click any links
- don't reply or forward
- don't open attachments

Delete the **email or text**, or reach out to the sender through a different channel if you're not sure

How to Prevent Being Impersonated on Social Media

If you are an individual, below are some ways to prevent being impersonated on social media.

- Set your social media profiles to private – This ensures that your profile can only be viewed by people you personally approved.
- Don't put any sensitive information on your profile – This includes your bank details, social security number, home address, and phone numbers, amongst other things. Many times people don't intentionally put this information on their profiles, but it can

be found in the background (such as statements left on the counter while taking a selfie).

- Be careful of the things you post – Fraudsters often use people’s posts to create a convincing fake account.
- Only accept friend (or follow) requests from people you know.
- If you receive a friend (or follow) request from someone you have already connected with – reach out to them directly to confirm that it’s really them that sent the request.

If you are a brand, here are some things you can do to protect your followers from fake accounts that may seek to scam them in your name.

- Always share your official profiles across all of your social platforms/channels, email, newsletters, SMS messaging, etc.
- Openly – and frequently – communicate with your customers via your official social media accounts. This way, if you’re being impersonated, they’ll figure it out in no time and report the fake account before it scams your followers.
- Consider verifying your social accounts. Not only does this increase your credibility, it also makes it easier for copycat accounts to be removed if they are impersonating you.
- Monitor social platforms for potential accounts that are impersonating your brand.
- Look for accounts with alternate variations, misspellings, alphanumeric combinations, separations, etc. of your brand name.
- Monitor branded hashtags used by your official account(s).

Find & Get Rid of Fake Social Media Accounts

Given the billions of fake accounts that exist across several social media platforms, it can be difficult to find and get rid of all the accounts that are impersonating you. If you suspect that someone is impersonating and spreading false information about you or your brand, your best bet is to hire a company that can investigate the situation for you.

[Section 230 of the Communications Decency Act](#) protects search engines and other internet service providers from liability for negative content posted on their platforms. Though many providers will voluntarily remove negative content, you may have to jump through hoops to get there. Below, we answer common questions about fake accounts and what victims can do about them.

How Can You Find Someone Who Has Made a Fake Account?

Our private investigators use advanced investigation tools, techniques, and software to locate and identify anonymous accounts online. Every case is different and not every

technique can or should be used in each case. Even so, a few of the techniques we regularly utilize include:

- Advanced search tools
- Advanced link analysis
- Metadata tracing
- Engaging the offending party using subterfuge
- Setting up a “honey pot” or “tripwire” to catch the account off guard
- Subpoenas ordering a website or search engine to provide IP address information

How Can One Deal with Online Harassment?

Until you learn the identity of the person behind the harassment, nothing can be done. Once they are identified, your legal options will depend on the unique circumstances of your situation. We recommend you speak to a lawyer specializing in internet/cyber issues about your situation to get a full view of your options.

Your options could include:

- Removing the damaging content from search-engine indexing
- Removing the damaging content from the website or internet
- Restraining orders against the bad actor
- Pursuing compensatory damages against the individual behind the fake account
- Criminal charges when warranted.

Before taking any action, you need to gather and preserve online and [social media evidence](#). This evidence must prove that harassment and damages exist. Our online and social media investigators explore our clients’ situations and gather the necessary evidence needed for their claims as well as identify the individual behind the harassment.

How Can I Prove Authenticity & Authorship?

As [social media case law](#) continues to evolve, we are seeing more and more that you cannot only count on printouts for evidence. You have to show proof of account authorship and authenticity.

In order to [prove authorship and authenticity](#), there are a couple of steps we take. First, we need to preserve the content as it was found. This includes capturing the images you see on the screen, but also the preservation of associated metadata. After that, we hash the data.

Metadata is the code behind the content. It can show important information such as location, time published, and user ID. The hash value acts as a digital fingerprint, which

can be replicated by the opposing side's expert to verify it wasn't altered, which is essential for the [admissibility of social media evidence if your case goes to court](#). Check out our article "[Authenticating Social Media Evidence: Verifying the Source](#)" to learn more about verifying evidence pulled from a social account.

How Much Does it Cost to Track a Fake Account?

Conducting an investigation to track down the person behind a fake account is neither easy nor inexpensive. Our work is usually billed hourly. Doing the investigation and gathering the evidence will usually cost between \$5,000-\$10,000, but it can sometimes be more.

As the case progresses, we will be transparent about whether or not the continued investigation will likely lead to a successful outcome. As a general rule, using our most common methods, we have about a 75% shot (depending on the specifics of the case) of tracking down who is behind a fake account.

Keep in mind that our objective is to track down the culprit and gather the necessary evidence. In order to take legal action, you will need to retain an attorney, which would incur attorney fees and court fees. Typically, attorney costs start between \$5,000-\$10,000 depending on which attorney you hire. In about 65% of cases we handle, hiring an attorney is a necessary step to unmask the identity of the bad actor.

Can I Sue for Online Defamation to Recover My Costs?

This is a complicated question. You could have a viable claim to recover compensation for damages, but it depends on exactly what was posted and the facts surrounding the situation. Again, you should speak with a lawyer about the best options for your case.

Keep in mind that states have statutes of limitation, or time limits on how long you have to make a claim. For example, in California, you only have one year from the date of the defamatory statement to bring a defamation claim against someone. There are exceptions to this statute, but generally, you want to save yourself plenty of time.

2. Outline the objectives and demographics of Interpol's International Child Sexual Exploitation Database.

What is child sexual exploitation?

Child sexual exploitation (CSE) is a type of [sexual abuse](#). It happens when a child or young person is coerced, manipulated or deceived into sexual activity in exchange for

things that they may need or want like gifts, drugs, money, status and affection. Children and young people are often tricked into believing they're in a loving and consensual relationship so the sexual activity may appear consensual. This is called **grooming** and is a type of abuse. They may trust their abuser and not understand that they're being abused. CSE does not always involve physical contact, and can also occur through the use of technology.

Children and young people can be **trafficked** into or within the UK for sexual exploitation. They're moved around the country and abused by being forced to take part in sexual activities, often with more than one person. Young people in gangs can also be sexually exploited.

Sometimes abusers use violence and intimidation to frighten or force a child or young person, making them feel as if they've no choice. They may lend them large sums of money they know can't be repaid or use financial abuse or blackmail to control them.

Anybody can be a perpetrator of CSE, no matter their age, gender or race. The relationship could be framed or viewed as friendship, someone to look up to or romantic. Children and young people who are exploited may also be made to 'find' or coerce others to join groups.

It's important to recognise that although the age of consent is 16 years old, children and young people over 16 can be exploited. Child sexual exploitation is a very complex form of abuse. It can be difficult for parents and carers to understand and hard for the young person to acknowledge that they are being exploited.

What is Online Child Sexual Abuse and Exploitation?

A Child is anyone under the **age of 18**.

Child Sexual Abuse (CSA) involves forcing or enticing a child to take part in sexual activity, whether or not the child is aware of what is happening. This may include activities such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse.

Child Sexual Exploitation (CSE) is a form of CSA. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) the financial advantage or increased status of the

perpetrator or facilitator. The victim may have been sexually exploited even if the activity appears consensual.

Online Child Sexual Abuse and Exploitation (CSAE) is used throughout this information resource to capture all types of offence. Online CSAE Offending can take a number of different forms which include:

Online Grooming - The act of developing a relationship with a child to enable their abuse and exploitation both online and offline. Online platforms, such as social media, messaging and live streaming, can be used to facilitate this offending.

Live Streaming – Live streaming services can be used by Child Sex Offenders (CSOs) to incite victims to commit or watch sexual acts via webcam. CSOs also stream or watch live contact sexual abuse or indecent images of children with other offenders. In some instances CSOs will pay facilitators to stream live contact abuse, with the offender directing what sexual acts are perpetrated against the victim.

Online coercion and blackmail – The coercion or blackmail of a child by technological means, using sexual images and/or videos depicting that child, for the purposes of sexual gain (e.g. to obtain new IIOC or bring about a sexual encounter), financial gain or other personal gain.

Possession, production and sharing of IIOC and Prohibited Images– CSOs can use online platforms to store and share IIOC and prohibited images. Online platforms can also be used to facilitate the production of IIOC, for example screen-recording of CSEA perpetrated over live streaming.

Indecent Images of Children (IIOC) are images of, or depicting, a child or part of a child which are judged to be in breach of recognised standards of propriety. Examples of images considered to be indecent are those depicting a child engaging in sexual activity or in a sexual manner, through posing, actions, clothing etc. IIOC includes photographs, videos, pseudo-photographs and tracings.

Prohibited Images of Children are non-photographic images, for example CGI, cartoons etc., which portray a child engaging in sexual activity, a sexual act being performed in the presence of a child or focus on the child's genital or anal region.

International Child Sexual Exploitation Initiative

India's Central Bureau of Investigation (CBI) has joined the Interpol's International Child Sexual Exploitation (ICSE) initiative and gained access to its image and video database.

- The International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool.

- It allows specialized investigators to share data on cases of child sexual abuse.
- The ICSE database uses video and image comparison to analyse Child Sex Exploitation Material (CSEM) and make connections between victims, abusers and places.
- India is the 68th country to have access to this database and software.
- The initiative will allow the CBI to collaborate with investigators in other countries for
 1. Detecting child sex abuse online and
 2. Identifying abusers, victims, and crime scenes from audio-visual clips using specialised software.

On average, the database of the ICSE initiative helps identify 7 child victims everyday globally.

- Using the image and video comparison software, the investigators attempt to identify locations of markers visible in a piece of media.
- The detectives in all 68 countries of the grouping can further exchange information across the world.

India's Actions to combat Online Child Sex Abuse

- **Interpol data** - According to Interpol data, India reported over 24 lakh instances of online child sexual abuse from 2017 to 2020, with 80% victims being girls below the age of 14 years.
- More than 60% unidentified victims were prepubescent, including infants and toddlers.
- Around 65% of unidentified victims were girls, but severe abuse images were more likely to have boys, the Interpol said on its website.
- **OCSAE** - In 2019, the CBI set up a special unit called the 'Online Child Sexual Abuse and Exploitation Prevention/Investigation (OCSAE)'.
- This special unit was set up for tracking and monitoring posting, circulation and downloads of CSEM online.
- Based on intelligence developed by the unit, the CBI started a country-wide operation against the alleged peddlers of online CSEM in 2021.
- In 2019, the National Centre for Missing and Exploited Children, a US-based non-profit organisation, had started sharing tip-offs about child sex abuse with Indian agencies.
- Received by the National Crime Records Bureau (NCRB), this information was passed on to the states where the incidents took place, to boost detection of those sharing such

Imagine you are the victim of a crime committed by someone from another country. How can police catch the person?

Our full name is the International Criminal Police Organization and we are an inter-governmental organization. We have 196 member countries, and we help police in all of them to work together to make the world a safer place.

To do this, we enable them to share and access data on crimes and criminals, and we offer a range of technical and operational support.

Who makes up INTERPOL?

The **General Secretariat** coordinates our day-to-day activities to fight a range of crimes. Run by the **Secretary General**, it is staffed by both police and civilians and comprises a headquarters in Lyon, a global complex for innovation in Singapore and several satellite offices in different regions.

In each country, an INTERPOL **National Central Bureau (NCB)** provides the central point of contact for the General Secretariat and other NCBs. An NCB is run by national police officials and usually sits in the government ministry responsible for policing. The **General Assembly** is our governing body and it brings all countries together once a year to take decisions.

The infographic features a dark blue background with a top section showing a row of national flags. On the left, the INTERPOL logo is displayed with the text '100 YEARS AND COUNTING' and 'INTERPOL'. The main heading reads 'OUR EXPERTISE TO SUPPORT MEMBER COUNTRY INVESTIGATIONS'. Below this, eight circular icons represent different support services: Fugitive Investigative Support, Police Data Management, Forensic Support, Capacity Building and Training, Command and Coordination Centre, and Special Projects. Two additional services, Criminal Analysis and Innovation, are shown in a separate row of two circles.

Connecting police

We connect all our countries via a communications system called I-24/7. Countries use this secure network to contact each other, and the General Secretariat. It also allows them to access our databases and services in real-time, from both central and remote locations.

We also coordinate networks of police and experts in different crime areas, who come together through working groups and at conferences to share experiences and ideas.



What INTERPOL do

The General Secretariat provides a range of expertise and services to their member countries. It manage 19 police databases with information on crimes and criminals (from names and fingerprints to stolen passports), accessible in real-time to countries.

It offer investigative support such as forensics, analysis, and assistance in locating fugitives around the world. Training is an important part of what Interpol do in many areas so that officials know how to work efficiently with their services.

This expertise supports national efforts in combating crimes across four global areas it consider the most pressing today: terrorism; cybercrime; organized crime; and financial crime and anti-corruption.

Officials working in each specialized crime area run a variety of different activities alongside member countries. This can be investigative support, field operations, training and networking.

Importantly, since crimes evolve, we keep an eye on the future through research and development in international crime and trends.



A global platform

Today's crimes are increasingly international. It is crucial that there is coordination among all the different players in maintaining a global security architecture.

Since INTERPOL is a global organization, it can provide this platform for cooperation; we enable police to work directly with their counterparts, even between countries which do not have diplomatic relations.

It also provide a voice for police on the world stage, engaging with governments at the highest level to encourage this cooperation and use of our services.

All their actions are politically neutral and taken within the limits of existing laws in different countries. It help specialized units work across borders and sectors to ensure criminals don't exploit children.

INTERPOL's main activity is to help police to **identify victims** of child sexual exploitation, by analysing photos and videos found on the Internet or on seized devices.

Our **database** of images is available to specialized experts, and supports traditional police investigations.

It also provide opportunities for experts to boost their skills and networks, leading to more effective investigations.

Victim identification

The **identification** of young victims portrayed in sexual abuse material is a top priority for law enforcement, as it can also help locate the perpetrators.

Crucial to our work is the **International Child Sexual Exploitation image database**, which uses sophisticated image comparison software to make connections between victims and places.

8 steps to identifying victims of child sexual abuse



Preventing the distribution of child sexual abuse material

Prevention of access to child material online is complementary to investigative work, and stops re-victimization of the children abused. We work closely with Internet service providers to block access to child abuse material online.

Appropriate terminology

Along with international experts, we recommend using **appropriate terminology** describing child sexual abuse or sexual exploitation. The Luxembourg Guidelines have been established as the reference for such terminology.

Training

A core function of our specialized experts in this area is to help police in our member countries to build their capacity to investigate child sexual exploitation. Interpol organizes training courses in all regions of the world and covering the entire scope of child sexual abuse investigations:

Conducting investigations in the online environment;

The use of INTERPOL's **International Child Sexual Exploitation database**;

Victim identification methods;

Victim and offender interview techniques;

Categorization and triage of child sexual abuse material.

While many countries have child protection and special victims units, few have specialized staff able to investigate online child sexual abuse cases or perform victim identification. Our specialized officers can advise countries on how to set up victim identification units and can provide tailored support to national authorities.

Specialists Group on Crimes against Children

The INTERPOL Specialists Group on Crimes against Children meets annually to facilitate and enhance the investigation of sexual crimes against children. Gathering law enforcement, regional and international organizations, NGOs, the private sector and academia, the group identifies new trends and techniques and develops best practice.

The SGCAC draws attention to emerging issues and helps drive innovative responses. In the case of end-to-end encryption (used by criminals to conceal their illicit online activities), the SGCAC provided leadership to draft a resolution on safeguarding children against online sexual exploitation, which was unanimously adopted at the 89th session of the INTERPOL General Assembly in 2021.

At the most recent SGCAC 38th operational meeting in March 2022, specialists from law enforcement units and partners from around the world gathered at INTERPOL to enhance the collective global response.

Some 100 participants from 54 countries discussed global efforts and technical solutions to assist investigation of online child sexual abuse, identify victims and their attackers, and disrupt criminal networks involved in producing and circulating abusive content.

Travelling sex offenders

Some sex offenders will cross borders to abuse children, allowing them to stay out of sight of their home authorities and gain unsupervised access to children.

INTERPOL can issue a **Green Notice** to warn about a person's criminal activities, where the person is considered a threat to children, or a **Blue Notice** to collect information on a person's identity, location or activities in relation to a crime.

Missing, abducted and trafficked children

At the request of a member country, it can issue a **Yellow Notice** to help locate missing persons, especially minors. These notices are circulated on an international basis and recorded in their database of missing and abducted children.

Interpol also work closely with our member countries and partners to protect minors from being **trafficked** and exploited for labour.

Partners

We nurture relationships with a number of cross-sector partners in order to cast the widest possible net against sex offenders.

ECPAT

Human Dignity Foundation

INHOPE

International Justice Mission

Internet Watch Foundation

We Protect Global Alliance

Virtual Global Taskforce

National Centre for Missing and Exploited Children

Regional law enforcement organizations

THORN

Private sector partners such as financial institutions, internet service providers and software developers also play a crucial role in tracking child sexual abuse material and shutting down illegal distribution channels. Their input is highly valued and a key part of our coordinated approach.

Victim identification involves the detailed analysis of images and videos to locate and rescue child sexual abuse victims.

Online child sexual abuse is one of the rare crime areas where police officers start with the evidence and work their way back to the crime scene.

The images can either be discovered through:

Child exploitation investigations;

Proactive monitoring of online platforms;

Forensic analysis of seized mobiles, laptops, digital storage units, etc.

Once images are found, victim identification specialists take over. They go through the images with a fine-toothed comb with the objective of removing the child from harm and arresting the abuser.

Evidence of a serious crime

Contrary to common beliefs about sexual abuse, the abuser is most often a person known to the child, such as a family member, neighbour or childcare professional. The vast majority of child sexual abuse cases are not documented, mostly taking place behind closed doors in private settings.

When the abuse is recorded or photographed, however, what is really being documented is evidence of a serious crime. Abusers often use the images for future sexual gratification, or to be traded and shared with other abusers.

Photos and videos of child sexual abuse found on the web are not virtual; they are evidence of a real crime involving real children and real suffering.

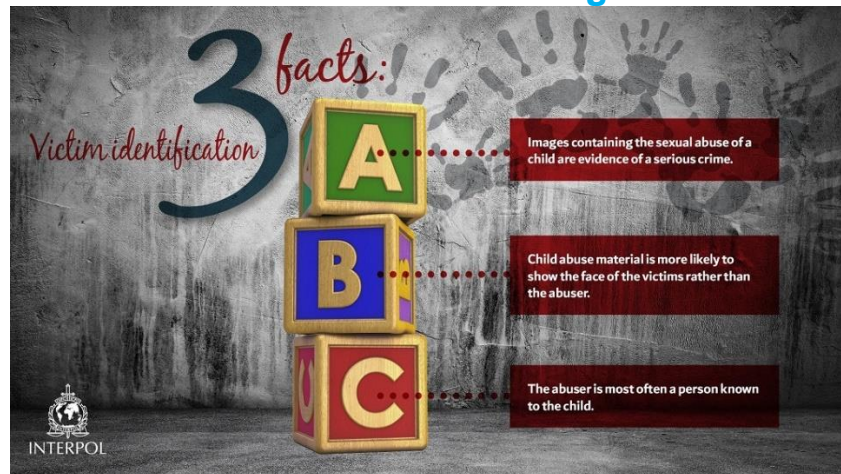
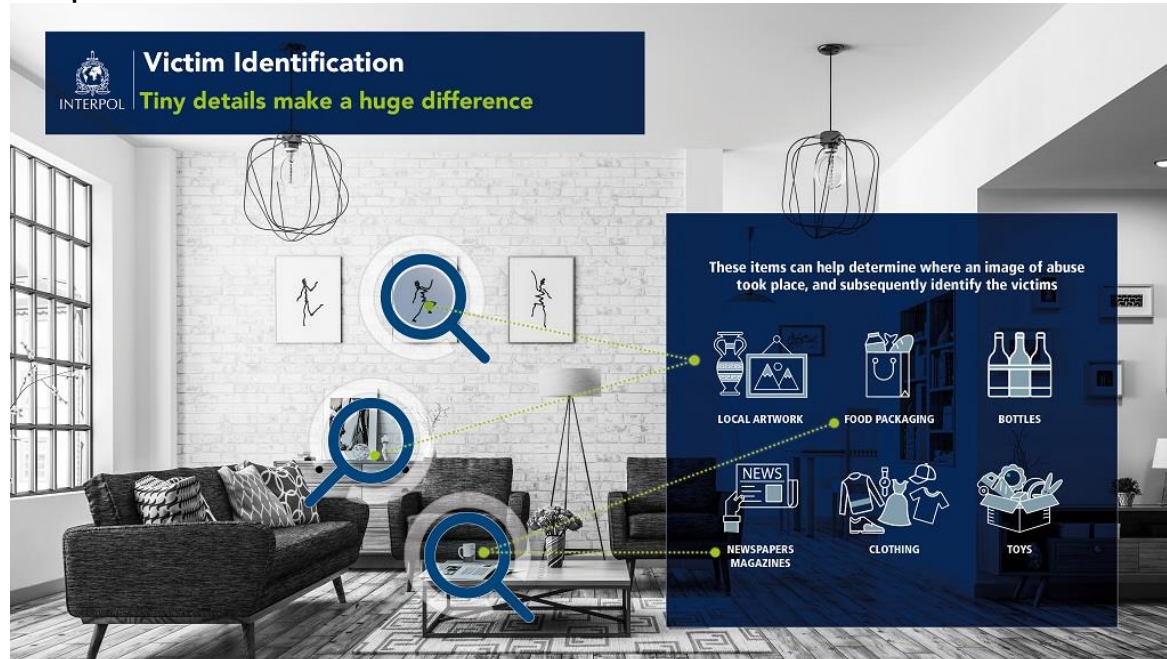


Image analysis

Victim identification combines detailed image analysis and traditional investigative methods.

By examining the digital, visual and audio content of photographs and films, officers can find clues identifying the location or victim. Clues can come from many places and in many forms – it is up to the victim identification specialists to piece them together using a range of specialized tools.



The results of this analysis of the virtual world will be crucial to the investigation that can then take place in the physical world.

A key tool in this is our International Child Sexual Exploitation Database, which includes image comparison software that helps victim identification specialists compare and exchange information on material and active investigations.

Specialized investigators

Due to its very nature, victim identification is difficult work, which requires specialists from all different fields. Often, law enforcement officers will work closely with authorized civilian analysts to determine the origin of a series of images or video.

Victim identification specialists work closely with their counterparts all over the world to ensure that clues that are unique, typical or easily recognizable in one country are not overlooked by another country.

We are always just one clue away from a break in a case. All it takes is the right person with the right tools and skills to make that connection.

This database helps victim identification specialists worldwide analyse and compare child sexual abuse images.

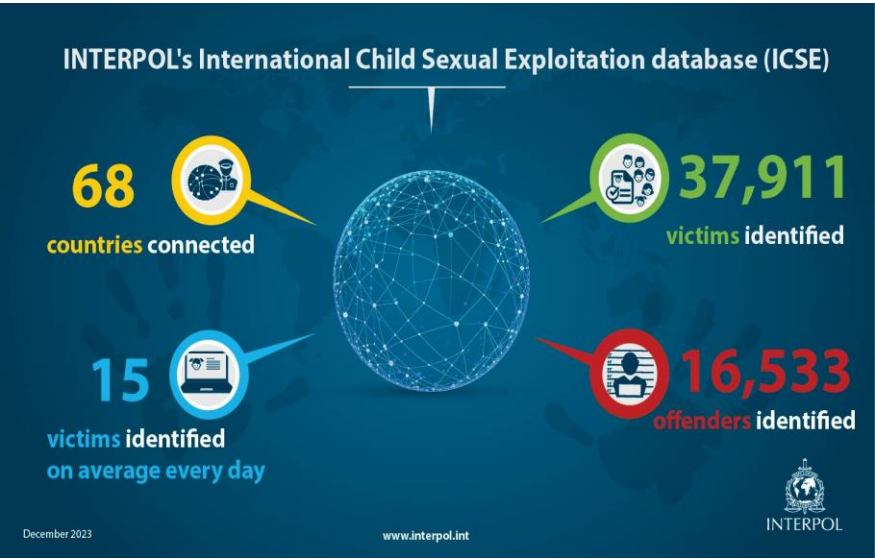
Our International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool, which allows specialized investigators to share data on cases of child sexual abuse.

Using image and video comparison software, investigators are instantly able to make connections between victims, abusers and places. The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images.

It also allows specialized investigators from more than 68 countries to exchange information and share data with their colleagues across the world.

By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse.

INTERPOL's Child Sexual Exploitation database holds more than 4.9 million images and videos and has helped identify more than 37,900 victims worldwide.



Young victims, severe abuse

Most people don't realize that when we talk about child sexual abuse, this includes the abuse of very young children, and even babies.

Following the examination of random selection of videos and images in the ICSE database, INTERPOL and **ECPAT International** published a joint report in February 2018 entitled Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material.

The study identified a number of alarming trends:

The younger the victim, the more severe the abuse.

84% of images contained explicit sexual activity.

More than 60% of unidentified victims were prepubescent, including infants and toddlers.

65% of unidentified victims were girls.

Severe abuse images were likely to feature boys.

92% of visible offenders were male.

[India's CBI now has access to Interpol's International Child Sexual Exploitation database in some of published magazine information:](#)

The ICSE database uses video and image comparison to analyse child sexual exploitation material and make connections between victims, abusers and places, the Interpol said.



For representational purposes (Express Illustrations)

NEW DELHI: The CBI has joined Interpol's International Child Sexual Exploitation database accessible to select countries, giving the investigative agency sharper snooping abilities to identify abusers, victims and crime scene from audio visual clips on Internet using specialised soft wares, officials said on Monday.

India is the 68th country among the total 295 members of the Interpol to have access to this database and software, which will be available to the Central Bureau of Investigation (CBI) -- nodal body for Interpol coordination in India as it is the country's National Central Bureau, they said.

An intelligence and investigative tool, the database, on an average, helps identify seven child victims everyday globally using audio-visual clips which are reported by various sources, including social media giants and search engines, they said.

So far, it has identified over 30,000 victims of child abuse and over 13,000 criminals.

The International Child Sexual Exploitation (ICSE) database uses video and image comparison to analyse child sexual exploitation material (CSEM) and make connections between victims, abusers and places, the Interpol said.

The database also allows specialised investigators to share information on cases of child sexual abuse.

Using the image and video comparison software, the investigators can nail down the criminals by identifying victims and places of crime.

"The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images," [according to Interpol](#).

The detectives in all 68 countries of the grouping can exchange information and notes with their colleagues across the world.

"By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse," the Interpol web site said.

India reported over 24 lakh instances of online child sexual abuse during the three year period 2017-20, with 80 per cent of victims being girls below the age of 14 years, according to the Interpol data.

The data indicates content and consumers of CSEM are growing at a sharp rate with one finding saying that 1.16 lakh queries on child pornography were made on a single internet search engine.

The CBI has set up a special unit 'Online Child Sexual Abuse and Exploitation Prevention/Investigation (OCSAE)' which tracks and monitors posting, circulation and downloads of CSEM on the internet.

Based on intelligence developed by the unit, the CBI had started a countrywide operation against the alleged peddlers of online CSEM in India last year, with the role of several websites under the scanner for their liability in hosting such material, officials said.

In its massive crackdown across 14 states, the probe agency had carried out searches at 77 locations and arrested seven people in an operation launched on November 14, Children's Day, last year.

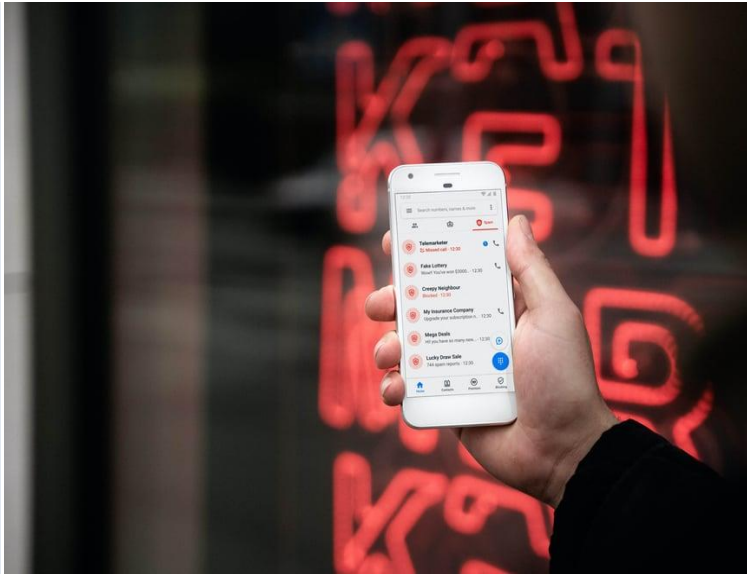
The search operation on 83 accused had resulted in seizure of huge tranche of electronic data and gadgets showing patterns of money trail and involvement of various offenders giving fresh leads to the agency which are being pursued, they said.

The operation had targeted over 50 social media groups having more than 5,000 alleged offenders sharing child sexual abuse material with some accused based in Pakistan, Canada, Bangladesh, Nigeria, Indonesia, Ajarbaijan, Sri Lanka, the United States of America, Saudi Arabia, Yemen, Egypt, the United Kingdom, Belgium, Ghana, among others.

3. Identify five suspicious SMS/emails you've received, cross-reference the sender phone no. or email against the NCRP Suspect database, and present the findings.

Spam text messages – or phishing texts – are unsolicited messages meant to scam you into revealing personal data. These texts appear to be sent by a trusted organization, business or even a family member, so it can be tricky to know when you receive one. Spam texts are typically computer-generated and sent to your phone via email or an instant messaging account. Sometimes, scammers even “spoof” your phone’s Caller ID to make it seem like a text is coming from a local or government-associated number.

These texts can look so real that they commonly trick mobile users into sharing personal information (like credit card information or Social Security numbers) or clicking on malware links.



Here are some common indicators of spam or phishing texts:

- **It's from an email address or untraceable phone number**
- **It includes suspicious links**
- **It contains obvious spelling errors**
- **It extends an offer that is too good to be true**
- **It requests personal information**

To protect yourself—and your finances—from the wrath of spam texts, it's essential to know how to identify them. This blog will share 14 common examples of spam messages and provide some tips for dealing with text-based scams.

14 Examples of Spam Messages

Here are 14 common text message scams to look out for:

1. [Free Prizes, Gift Cards or Coupons](#)
2. [Bank Account Verifications](#)
3. [Texts from Government Agencies](#)
4. [Order Deliveries](#)
5. [Texts From Your Own Number](#)
6. [Credit Card Offers](#)
7. [Unexpected Job Offers](#)
8. [Issues With Your Payment Information](#)
9. [“We’ve Noticed Suspicious Activity”](#)
10. [Family Emergencies](#)
11. [Two-Factor Authentications \(2FA\)](#)

- 12. [Texts From Your Boss](#)
- 13. [Refunds and Overpayments](#)
- 14. [Suspicious Group Texts](#)

Spam Text Messages Can Look Like:

- Free Prizes, Gift Cards or Coupons
- Bank Account Verifications
- Texts from Government Agencies
- Order Deliveries
- Texts From Your Own Number
- Credit Card Offers
- Unexpected Job Offers
- Issues With Your Payment Info.
- “We’ve Noticed Suspicious Activity”
- Family Emergencies
- Two-Factor Authentications (2FA)
- Texts From Your Boss
- Refunds and Overpayments
- Suspicious Group Texts



1. Free Prizes, Gift Cards or Coupons

Free prizes are quite uncommon. So if you get a text about free gifts, think twice before taking action!

Example: *Congratulations! You’ve won a \$500 Amazon gift card. Claim it here [Link].*

2. Account Verifications

Banks rarely text their customers with important information or updates. Scammers frequently pose as banks to trick customers into revealing valuable information.

Example: *ACTION REQUIRED. Please verify your Bank of America account information to avoid a hold on your account. Click here to confirm: [Link]*

3. Texts from Government Agencies

Like banks, government agencies like the Internal Revenue Service will **not** text you regarding important information. This is another common scam technique used to steal money.

Example: *You’ve been overcharged for your 2021 taxes. Get your IRS tax refund here: [Link]*

Sunday, Oct 23 • 12:48 PM

Texting with (843) 713-0566 (SMS/MMS)

EDD Alert: You are required to reactivate your EDD Visa Prepaid starting 4427434*** within 4 hours at <https://www.roamnana.nl/wp-content/plugins/ioptimization/o.php>

12:48 PM

+ 📎 Text message 😊 🗣️

4. Order Deliveries

If you receive a text regarding an order, double-check the confirmation number before following any suspicious links. Since online orders are common, it's easy for scammers to convince mobile users that they have made a recent order that must be tracked.

Example: *Get delivery updates on your USPS order [Number] here: [Link]*

5. Texts from Your Own Number

Getting a text from your own number is super weird. Spammers manipulate phone networks to get you to click on something that seems familiar and safe, but don't fall for it! This fairly new scam will often impersonate your phone carrier to lend more legitimacy.

Example: *Thank you for paying last month's bill. We're rewarding our very best customers with a gift for their loyalty. Click here! [Link]*

6. Credit Card Offers

Texts about low- or no-interest credit cards are a common way to get you to click on malware links.

Example: *Congratulations! Your credit score entitles you to a no-interest Visa credit card. Click here to claim: [Link]*

7. Unexpected Job Offers

When you haven't applied for a job, receiving a job offer can initially seem flattering. Employment-related scams lure you into clicking a link to learn more about a job offer or sometimes provide a phone number to call for more information.

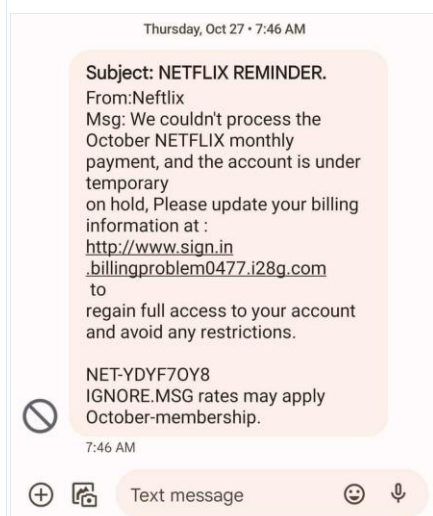
Not only are texts like these (if they were legitimate) a violation of **TCPA laws**, employers and recruiters would never "roll the dice" and extend a job opportunity randomly.

Example: *We've received your resume and would love to set up an online interview. Click here [Link] or call us at [Phone Number] at your earliest convenience.*

8. Issues with Your Payment Information

Requesting payment information details is another way scammers steal credit card information. Call your credit card company directly if you're in doubt about a suspicious text.

Example: *There's an issue with your payment information from your recent order [Order Number]. Take action now: [Link]*



9. "We've Noticed Suspicious Activity"

A text about suspicious activity from a scammer seems hypocritical, right? Unfortunately, this common spam text message example targets many mobile users. To eradicate any suspicious activity, users frequently take action on text messages like these.

Example: *We have detected suspicious activity on your Wells Fargo account. Log in at [Link] to update your account preferences and protect your information.*

10. Family Emergencies

Scammers often use fake family emergencies to trick people into clicking on a scam text message. For example, they may claim that a family member has been involved in an accident, is in the hospital, or needs money immediately.

By creating a sense of urgency and tapping into people's emotions, scammers hope to exploit their targets' goodwill and compassion, prompting them to respond quickly without verifying the message's authenticity.

Example: *Hi Grandpa, it's me – I've been in a car accident, and my parents aren't around. Can you please send me money so I can get home? You can wire funds to me here: [Link]*

11. Two-Factor Authentication (2FA)

Two-factor authentication, or 2FA, is commonly used as a security step by banks and financial institutions as an extra security layer. Scammers may send a message claiming an issue with your 2FA settings and instruct you to click a link to resolve the issue.

Once you click the link, they may prompt you to enter your login credentials or other sensitive information, which the scammers use fraudulently.

Example: *"Your 2FA settings are not up to date. To avoid account suspension, please click the following link to update your settings: [Link]."*

12. Texts from Your Boss

Scammers may impersonate your boss or another company executive to get you to carry out a task, such as buying gift cards, transferring funds or providing sensitive information. However, the message is likely to be fraudulent, and any action taken could result in financial loss or data theft.

Example: "Hey, it's [Boss Name]. I'm in a meeting now and need your help with something urgent. Can you transfer \$5,000 to this account ASAP? I'll explain everything later. Please keep this confidential."

13. Refunds and Overpayments

Who isn't intrigued by the promise of free money? Scammers send texts claiming that you're owed a refund due to an overpayment on an account. Unfortunately, clicking on a phishing link is the only way to get paid.

Example: "We're happy to inform you that you're entitled to a refund for overpayment on your AMEX account. Click on this link [Link] below to claim your refund."

Thursday, Aug 18 • 3:11 PM

Texting with (606) 203-8668 (SMS/MMS)

Order Placed:-AMZ@#DV91453EW
for KONAL Western Table Set,
Amount of \$1360 will be deducted
from your card . Not you? contact
us [+18443060679](tel:+18443060679)

3:11 PM



Text message



14. Suspicious Group Texts

In recent years, there has been a significant rise in spam group texts, unsolicited text messages sent to a large group of people. A tip-off to spam group texts is that the other numbers in the group aren't in your contacts list. These scams contain phishing scams, malware links, and other fraudulent offers.

Example: Congratulations! You have all been selected to receive a free gift card worth \$1000. Click on this link [Link] to claim your reward now. Limited time offer, so act fast! Don't miss out on this amazing opportunity.

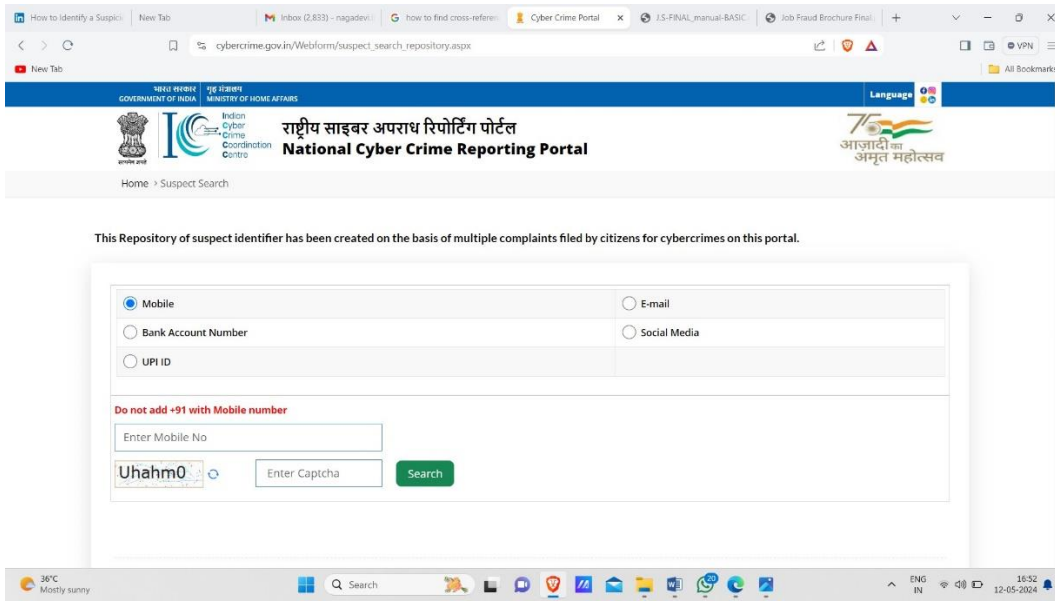
How to Block and Report Spam Text Messages

Fed up with receiving unwanted spam text messages? Here's how to block and report annoying or dangerous spam messages.

In The National Cybercrime Reporting Portal (NCRP) portal we can register a complaint.

The screenshot shows the homepage of the National Cyber Crime Reporting Portal (NCRP). The website is in Hindi and features a blue header with the Government of India and Ministry of Home Affairs logos. The main content area is a large banner with a green and black background. The banner contains the following text in Hindi: "आधुनिक टेक्नोलॉजी के इस्तेमाल के कारण साइबर सुरक्षा वर्तमान जीवन का अभिन्न अंग बन गया है" (Modern technology has become an integral part of modern life due to the use of technology), "साइबर स्वच्छ प्रथाओं का पालन करें और साइबर क्राइम से बचें" (Follow cyber hygiene practices and avoid cybercrime), and "ऑनलाइन वित्तीय धोखाधड़ी की रिपोर्ट करने के लिए 1930 पर कॉल करें" (Call 1930 to report online financial fraud). The website URL "cybercrime.gov.in" is prominently displayed. Below the banner, there are three smaller images: one showing a group of people, one showing a bank card and a skull and crossbones, and one showing a network diagram with a warning sign. The footer of the page includes a "What's new" section and a Windows taskbar at the bottom.

In this portal we can register a suspected phone number and email/messages etc. After the complaint we can track the complaint also and we can register complaint anonymously.



The National Cybercrime Reporting Portal (NCRP) under I4C was launched on 30.08.2019. The older version of the Cybercrime reporting portal under CCPWC scheme enabled the filing of Cybercrime complaints pertaining to Child Pornography (CP)/ Rape or Gang Rape (RGR) – Sexually Abusive Content only. The revamped version of the portal allows reporting of all types of Cybercrime. The National Cybercrime Reporting Portal (NCRP) was dedicated to the nation by the Hon'ble Home Minister of India on 20th January 2020.

Website: <https://cybercrime.gov.in/>



NCRP Features

All types of Cybercrime incidents can be reported from anywhere.

Special focus on content reporting of online Child Sex Abuse Material/Rape-Gang Rape incidents.

National/State/District-Level monitoring dashboards.

Online status tracking facility for the complainant.

Cyber Volunteers registered as Cyber Awareness Promoters.

An automated Chatbot having predefined features created and named Vani- CyberDost Chatbot has been deployed on NCRP.

A new Module “Citizen Financial Cyber Fraud Reporting and Management System” has been developed, connecting 85 Banks/Payment Intermediaries and Wallets etc. with the Cybercrime Backend Portal. This helps citizens to report cyber financial frauds on National Helpline number 1930.






1930 National Helpline number is running in all States/UTs.

Citizen Financial Cyber Fraud Reporting and Management System [CFCFRMS]

To deal with the complex subject of financial frauds, it is imperative to create a common integrated platform where all concerned stakeholders i.e., Law Enforcement Agencies (LEAs), banks, RBI, financial intermediaries, payment wallets, NPCI, etc., work in tandem; to ensure that quick decisive and system-based effective action is taken to prevent flow of money siphoned off from innocent citizens to the fraudsters. Citizen Financial Cyber Frauds Reporting and Management System has been developed for quick reporting of financial cyber frauds and monetary losses suffered due to use of digital banking/credit/debit cards, payment intermediaries, UPI etc. Complaints can be reported through helpline number 1930 or on National Cybercrime Reporting Portal.

**WORKING OF
CITIZEN
FINANCIAL
CYBER FRAUD
REPORTING
AND
MANAGEMENT
SYSTEM**

HELPLINE : 1930

	Victims of cyber fraud call on Helpline no. 1930(earlier 155260), which is manned and operated by the concerned State Police.
	The Police operator notes down the fraud transaction details and basic personal information of the caller and submits them in the form of a Ticket on the Citizen Financial Cyber Frauds Reporting and Management System.
	The Ticket gets escalated to the concerned Banks, Wallets, and Merchants and so on. Depending on whether they are the victim's bank or the bank/wallet in which the defrauded money has gone.
	An SMS is also sent to the victim with an acknowledgement number of the complaint with direction to submit complete details of the fraud on the National Cybercrime Reporting Portal (https://cybercrime.gov.in) using the acknowledgement number. An SMS regarding the complaint is also sent to Nodal officer of the Financial Institution (FI).
	The concerned Bank, which can now see the ticket on its dashboard on the Reporting Portal, checks the details in its internal systems.
	If the defrauded money is still available, the Bank puts it on hold, i.e., the fraudster cannot withdraw the money. If the defrauded money has moved out to another Bank, the Ticket gets escalated to the next Bank to which the money has moved out. This process is repeated until the money is saved from reaching into the hands of the fraudsters. The information regarding the action taken by respective FI will be informed to the concerned State Police.

4. What are the guidelines to be followed by children while accessing public systems, as per ISEA portal (www.infosecawareness.in)?

The guidelines to be followed by children while accessing public systems, as per ISEA portal

Now a days everyone using internet kids from the age of 2 year and above to watch YouTube for rhymes and stories after when they grow up gradual increase in screening time and they play games using internet play a vital role among children.

Internet is considered as the greatest platform and technology in this century and has become an integral part of our daily lives. It helps us as a learning and communication tool and offers us a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination.

Do they follow ethics?

Internet ethics implies our behaviour while using it. We should be aware that we should always be honest, respect the rights and property of others on internet.

Step 1: Do they share about internet access with your family?

Sharing about internet activity with your family members is the first step to being safe on internet. Your parents always love you and look about your safety so that they would be with you in all difficult periods.

So share each and everything what you do and face on internet.

Step 2: Do they use family computer?

If Yes, then follow some family rules and guidelines as the family members use internet for different purposes like banking, shopping, sometimes even doing office work, etc.

Most online games or videos may require credit/debit card details to play, watch videos etc. So, when using the family computer you may share such sensitive data to known/unknown people without the knowledge of your family members which can create financial losses to the family.

Also there are chances that when using family computer you may even share important office files or documents to your online friends which can create career threat to your family members. Therefore always follow some rules and guidelines of family for accessing internet.

Step 3: Do they love to see videos?

Watching videos on internet is always fun and pleasure, but at the same time there are risks like malicious links could take you to inappropriate or illegal content. If you encounter any such activity, intimate it to your family members.

Remind family members that people met online may be strangers.

Step 4: Do they follow any celebrity over the internet?

Like any other child, you may follow and chat online about your favourite celebrities in all kinds of fields. There are lots of celebrity sites, only the ones operated by the celebrities themselves or entertainment news publishers are appropriate to follow.

You need to be extra careful of fan sites that turn up in search results but aren't actually run by the celebrities and the people who cover them. It's not always easy to tell, but at least they'll lower down in the search results.

Step 5: Do they believe everything on internet is true?

It's common for you to think everything on internet is true. But, the content on internet is a collection of lot of people's views as they can write and post without any guidance and control. Internet contains a wealth of valuable information, but at the same time it is a great medium for disseminating falsehoods and inaccuracies.

Though the information on the internet is very valuable, but you should realize that there are still biased views and information to market their products and agenda. So, you need to be careful and confirm the same by going into various sources of internet.

Step 6: Do they love to play games?

Yes, Children love to play games. We always love to play online games and extend our arms further with unknown members on internet.

To play games on internet, some websites ask credit/debit card details though they tell it is free. Be careful while playing free online games as sometimes automated charges can apply which can be burden to the family members.

Also, the details and identification passed on the web site can be accessed by others and identification theft can occur.

Step 7: Do they love to be social?

Yes, Children love to be social and make new friends. Internet helps you to keep in touch with old friends and extend your arms to new members. Though it is a great opportunity to extend friend circles, never share passwords even with the closest buddies because bullying is common as some kids or hackers try to post embarrassing messages by using shared password or post links to malicious sites.

At the same time, you should also know that there are social reasons why kids are hacked. So always log out of accounts when you are finished using computers shared with other people especially those used in public, such as at school or public libraries.

Step 8: Do they keep open your identification?

For hackers or attackers, Children's identification is more valuable. Criminals get most of the information about children such as name, address, class, school name to target them. The collected information may be useful for guessing passwords of children and their parents as in general passwords of family members are related with family names.

Further they may use the same information for making friendship with you online and try to get to know about your family and consequently they may apply credit cards on your family member's name.

It is suggested that children should not share any information related to sensitive and financial aspects in social networks and maintain privacy with known and unknown members.

Few tips to enable privacy and security features on digital devices for safety and protection:

Authentication for accessing mobile with finger print or Face recognition and a lock screen with a pattern pass code or a password is necessary to avoid misuse of the mobile.

Steps to enable biometric authentication and passwords: Authentication - 1- settings; 2 - lockscreen and password

Enable google play protect on your mobile. It scans your mobile and alerts you on signs of misbehaving apps or anything suspicious. Confirm and make sure it is working by checking if it is active.

Steps to enable google play protect:

- 1- Google play store ;
- 2- 2- at the top right tap the profile icon;
- 3- 3- click on play protect ;
- 4- 3 - check whether option is enabled n active

Enable find my device option to trace your mobile device by finding its exact location of the on an interactive map.

Steps to enable find my device option:

- 1 - Settings;
- 2 - Google;
- 3 - Security;
- 4- Enable find my device

Update emergency contact information on your mobile to display the contact number on lock screen in case of emergency.

How to set up an Android emergency contact

There are a couple of ways to set up ICE contact information on an Android phone. First, you can add your info to the emergency information feature:

- . Open the “Settings” app. Tap “User & accounts,” then “Emergency information.”
- . To enter medical information, tap “Edit information” (you might have to tap “Info” first, depending on the version).
- . There’s a separate section where you can enter emergency contacts; tap “Add contact” to add a person from your contacts list (you might have to tap “Contacts” first)

Enable 2 factor authentication to rule out the possibility of misuse or theft of passwords. This feature ensures another layer of security.

Steps to enable 2factor authentication option: (On your Android phone or tablet)

- 1- Settings app;
- 2- 2 - Google;
- 3 - Manage your Google Account;
- 4- Click security;
- 5- enable 2 step verification and enable options

Enable safe browsing options on your mobile to get a warning on trying to access or open a malicious site or download dangerous content. Chrome is a default android browser that is enabled with safe browsing feature.

Steps to enable safe browsing option on your mobile

- 1- Click on chrome;
- 2-go to settings/ tap the profile icon on top right;
- 3 - Privacy;
- 4 - Enable safe browsing

Use YouTube kids app for safely viewing YouTube videos

This is a free downloadable app that is created by YouTube for kids. It allows parents the option to set an age level of their child to view only specific related content that has been reviewed by Google and marked as appropriate for that age group.

For using it-

download the app from play store into your device

set it up for your child by entering the year of birth, choosing appropriate age group and other options,

after you enter your email and send parental consent,

you receive 4 digit verification code

Using the code you can start using this app for your child on the device. (this is available on ios and android devices)

Other options to view YouTube safely especially for children–

-Watch and share videos on safeyoutube.net

This is another solution to watch and share YouTube videos without any other distracting content in view.

<https://safeyoutube.net/w/xOxE>

To use the safeyoutube.net –

copy the url of the YouTube video that you want to share or watch,
later paste it on the on the website safeyoutube.net in the option given for ‘Generate your safe YouTube link’

Once you generate the link you can use or share this safe link for viewing the YouTube videos without any other content or advertisements appearing on the screen.

-Subscribe to the selected channels

You may also subscribe to specific selected channels by selecting subscribe button. This will ensure that you will be directed to the specific videos that you want to watch.

For subscribing to selected channels

open the YouTube app or go to youtube.com

sign in with your credentials

select the type of videos you want to view

Select the subscribe button.

-Enable restricted mode on YouTube

YouTube provides the ‘Restricted Mode’ on regular YouTube website, which will enable a kid-friendly setting, with restricted content. Parents may use the same for older children, to avoid inappropriate content.

To set up YouTube Restricted Mode

go to YouTube.com and sign into the account you created

Scroll down to the very bottom of the page.

Then click Restricted Mode.

You will see some safety buttons appear below.

Click the circle labelled “On,” to enable Restricted Mode.

Then click Save to save the changes you’ve made to your settings.

-Upload videos by selecting private or unlisted option and restrict comments

For a safe video sharing option you may guide the child to upload video privately to selected members, you may use the unlisted option so that they do not show up on YouTube option but anyone with specific link can only see it, you can also restrict comments from viewers, to avoid disturbing reviews.

To enable this option sign in to YouTube studio, from left menu select videos, hover over the video you want to update, click down arrow under visibility and choose private or unlisted option and save.

(Reference: <https://techboomers.com/youtube-parental-controls>)

Enable parental controls for activating security features and safeguarding children

Parental controls are restrictions that parents can implement on child's usage of digital devices by enabling certain features available in the software of specific devices and monitor their online activity. It helps reduce the risk of child viewing inappropriate content on web.

The parental control can help

Block inappropriate apps., games and media child can access

Set restrictions on web browsers to show only pre-approved websites

Restrict search engines by defining what child can search online

Restrict child from using certain unwanted services

Steps to set up parental controls:

Open google play store app

Tap menu in the top right corner

Got to settings

Go to parental controls option and turn it on

Create a PIN

Tap the type of content you want to filter

Choose how to filter or restrict access.

(ref.: <https://support.google.com/googleplay/answer/1075738?hl=en#zippy=%2Cwatch-how-to-set-up-parental-controls>)

Other options to monitor online activities of children

Parents may **use security features enabled parental control/ child monitoring apps**, available on google playstore to help them in guiding children appropriately on digital device usage and safeguard them against possible online dangers.

Examples of few parental control Apps – Net Nanny, Norton Family, Kaspersky safe kids, Bark, mspy etc.,

Have digital device usage family agreements, where all the family agree to follow certain common family rules for using digital devices.

Have digital free zones like bedtime, dinner time, play time, driving time etc.,

Model kindness and good digital usage habits, when using digital medium for communication.

Be a good Digital Role Model

Modelling good digital habits is essential for parents. This is important as the parent's behaviour and habits are unspoken permission to children to practice the same later on.

Do not engage too much in digital devices when you are around children.

Pay attention to children and to what they want to tell you.

Engage in positive, encouraging and motivating approach while talking to children

Create an environment wherein children can put across their digital issues, to parents to seek suggestions.

Help children to form confident ideas and beliefs about themselves to deal with crisis situations.

Be accessible to children; have certain time in a day allocated to family and children.

Android OS Privacy Settings

This section provides the privacy-related recommendation for Android OS.

(L1) Ensure 'Notifications on the lock screen' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable notifications on the lock screen.

The recommended state for this setting is: Disabled.

Rationale:

If the device is lost or is unattended, then disabling notifications do not display any notification information on the locked screen.

This information might be private or confidential and thus unwarranted disclosures could be avoided.

Audit:

To verify Notifications on the lock screen are set to don't show notifications at all:

1. Tap Settings Gear Icon.
2. Tap Apps & notifications.
3. Tap Notifications.
4. Verify that on the lock screen is set to don't show notifications at all. **Remediation:**

Follow the below steps to set the on the lock screen to don't show notifications at all:

1. Tap Settings Gear Icon.
2. Tap Apps & notifications.
3. Tap Notifications.
4. Tap On the lock screen and set it to Don't show notifications at all. Locks Are Configured Configure screen locks on systems to limit access to unattended workstations.

Impact:

The user will not be able to see contents of notifications on lock screen requiring her to unlock the device each time.

Default Value:

By default, notification content is shown on the locked screen.

References:

https://support.google.com/pixelphone/answer/6111294?hl=en&ref_topic=7078221

CIS Controls:

Version 6 16.5 Ensure Workstation Screen Locks Are Configured

Configure screen locks on systems to limit access to unattended workstations.

(L2) Ensure 'Location Services' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable Location Services when not in use.

The recommended state for this setting is: Disabled.

Rationale:

Location Services allows applications such as Maps and Internet websites to gather and use data indicating the user's location. The user's location is determined using available information from cellular network data, local Wi-Fi networks, Bluetooth and GPS. If the user turns off Location Services, the user will be prompted to turn it back on again the next time any application tries to use this feature.

Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means without user's consent. Thus, it should be

disabled when not in use.

Note: Location service is very important for tracking your lost device if the device data is not disabled. Make a judicious call and decide what works best for you or in your environment.

Audit:

Follow the below steps to verify that Location services is Disabled:

1. Tap Settings Gear Icon.
2. Tap Security & Location.
3. Scroll to the Privacy section.
4. Tap Location.
5. Verify that Location is OFF.

Remediation:

Follow the below steps to disable Location Services:

1. Tap Settings Gear Icon.
2. Tap Security & Location.
3. Scroll to the Privacy section.
4. Tap Location.
5. Toggle to the OFF position.

Impact:

Each time an application needs location data, the user activity would be interrupted to enable the location services.

Another impact could be on finding your lost device. If the device is lost and the location services are disabled, you cannot use remote locate services such as Android Device Manager.

Default Value:

By default, Location Services is enabled.

References:

https://support.google.com/pixelphone/answer/3467281?hl=en&ref_topic=7083817

CIS Controls:

Version 6

Data Protection

(L2) Ensure 'Back up to Google Drive' is 'Disabled' (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable Backup to Google Drive.

The recommended state for this setting is: Disabled.

Rationale:

You can back up content, data, and settings from your device to your Google Account. You can then later restore your backed-up information to another device. Due to privacy concerns, backing up personal data such as text messages, emails, photos and contacts to any third party is not recommended unless you accept the risk of sharing the data with the 3rd party. Moreover, if you are using a personal device for business apps such as emails, that data might be backed up as well in the Google Drive related to your personal account and might be exposed. Hence, disable the automatic backup to Google drive and carefully choose what data backup you need.

Audit:

Follow the below steps to verify Back up to Google Drive is Disabled:

6. Tap Settings Gear Icon.

7. Tap System.
8. Tap Advanced.
9. Tap Backup.
10. Verify that Back up to Google Drive is OFF.

Remediation:

Follow the below steps to disable Back up to Google Drive:

1. Tap Settings Gear Icon.
2. Tap System.
3. Tap Advanced.
4. Tap Backup.
5. Tap Back up to Google Drive.
6. Toggle it to OFF position.

Impact:

A backup of the device will not be taken and hence restoration would not be possible. Also, the user would have to carefully choose the data to be backed up and manually back it up periodically.

Default Value:

By default, Back up to Google Drive is disabled.

References:

<https://support.google.com/pixelphone/answer/7179901?hl=en>

CIS Controls:

Version 6

(L1) Ensure 'Web and App Activity' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable linking of web and app activity to your account when you are logged out. Note: This setting is applicable only for Google Pixel range of devices.

The recommended state for this setting is: Disabled.

Rationale:

When this setting is enabled, your searches and activity from other Google services are linked and saved to your Google Account, even when you are logged out or offline. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that Web & App Activity setting is Disabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Verify that Web & App Activity setting is disabled.

Remediation:

Follow the below steps to disable Web & App Activity setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.

8. Toggle Web & App Activity setting to OFF position

Impact:

Web and App activities would not be linked to your account. You might not get personalized user experience.

Default Value:

By default, Web & App Activity is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
1. <https://support.google.com/websearch/answer/54068>

CIS Controls:

Version 6

(L1) Ensure 'Device Information' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing device information to your account.

Note: This setting is applicable only for Google Pixel

range of devices. The recommended state for this setting

is: Disabled.

Rationale:

Turning on Device Information setting saves various device related information to your account to give you personalized results, suggestions, and experiences. The information saved might include contact lists, calendars, alarms, apps, and music. Additionally, information such as whether the screen is on, the battery level, the quality of your Wi-Fi or Bluetooth connection, touchscreen and sensor readings, and crash reports are also saved and shared with Google. This could be privacy-invasive

and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that Device Information setting is disabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Verify that Device Information setting is disabled.

Remediation:

Follow the below steps to disable Device Information setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Toggle Device Information setting to OFF position.

Impact:

You might not get personalized user experience.

Default Value:

By default, Device Information is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/accounts/answer/6135999>

CIS Controls:

Version 6

(L1) Ensure 'Voice & Audio Activity' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable saving your voice and other audio to your Google Account. Note: This setting is applicable only for Google Pixel range of devices. The recommended state for this setting is: Disabled.

Rationale:

Google records your voice and other audio when you use audio activations. Audio can be saved even when your device is offline. When Voice & Audio Activity is off, voice inputs won't be saved to your Google Account, even if you're signed in. Instead, they may only be saved using anonymous identifiers. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that Voice & Audio Activity setting is Disabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Verify that Voice & Audio Activity setting is disabled.

Remediation:

Follow the below steps to disable Voice & Audio Activity setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.

4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Toggle Voice & Audio Activity setting to OFF position.

Impact:

You might not get personalized user experience.

Default Value:

By default, Voice & Audio Activity setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/websearch/answer/6030020>

CIS Controls:

Version 6

(L1) Ensure 'YouTube Search History' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Search History to your account.

Note: This setting is applicable only for Google Pixel

range of devices. The recommended state for this setting

is: Disabled.

Rationale:

Turning on YouTube Search History setting links and stores all your YouTube searches to your account across any device. Also, your YouTube and Google search history influences the recommendations that you see on your YouTube homepage when you are logged-in.

This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that YouTube Search History setting is Disabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Verify that YouTube Search History setting is Disabled.

Remediation:

Follow the below steps to disable YouTube Search History setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls
8. Toggle YouTube Search History setting to OFF position.

Impact:

You might not get personalized user experience.

Default Value:

By default, YouTube Search History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/youtube/answer/57711>

CIS Controls:

Version 6

(L1) Ensure 'YouTube Watch History' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Search History to your account.

Note: This setting is applicable only for Google Pixel

range of devices. The recommended state for this setting

is: Disabled.

Rationale:

Turning on YouTube Search History setting links and stores all your YouTube searches to your account across any device. Also, your YouTube and Google search history influences the recommendations that you see on your YouTube homepage when you are logged-in.

This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that YouTube Search History setting is Disabled:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Verify that YouTube Search History setting is Disabled.

Remediation:

Follow the below steps to disable YouTube Search History setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls
8. Toggle YouTube Search History setting to OFF position.

Impact:

You might not get personalized user experience.

Default Value:

By default, YouTube Search History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/youtube/answer/57711>

CIS Controls:

Version

(L1) Ensure 'YouTube Watch History' is set to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Watch History to your account.

Note: This setting is applicable only for Google Pixel

range of devices. The recommended state for this setting

is: Disabled.

Rationale:

Turning on YouTube Watch History setting links and stores all your watched YouTube videos to your account from any device. Also, this influences the recommendations that you see on your YouTube homepage when you are logged-in and other YouTube video recommendations. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that YouTube Watch History setting is Disabled:

11. Tap Settings Gear Icon.
12. Tap Google.
13. Scroll to the Services section.
14. Tap Search.
15. Scroll to the Search section.
16. Tap Accounts & privacy.
17. Tap Google Activity Controls.
18. Verify that YouTube Watch History is Disabled.

Remediation:

Follow the below steps to disable YouTube Watch History setting:

1. Tap Settings Gear Icon.
2. Tap Google.
3. Scroll to the Services section.
4. Tap Search.
5. Scroll to the Search section.
6. Tap Accounts & privacy.
7. Tap Google Activity Controls.
8. Toggle YouTube Watch History setting to OFF position.

Impact:

You might not get personalized user experience.

Default Value:

By default, YouTube Watch History setting is enabled.

References:

1. <https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en>
2. <https://support.google.com/youtube/answer/95725>

CIS Controls:

Version 6

Android OS Chrome Browser Settings

(L1) Ensure 'Microphone' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

This setting controls if a site asks before accessing the microphone. The recommended state for this setting is:
Enabled.

Rationale:

Websites will have to ask permission before being allowed to access the microphone which will help prevent unwanted access to the microphone and help protect against potential privacy concerns.

Audit:

Follow the below steps to verify that Microphone is Enabled:

1. Tap Chrome icon.
2. Tap Menu icon.
3. Tap Settings.
4. Scroll to the Advanced section.
5. Tap Site settings.
6. Verify that Microphone displays Ask first.

Remediation:

Follow the below steps to Enable the Microphone permission request:

1. Tap Chrome icon.
2. Tap Menu icon.
3. Tap Settings.
4. Scroll to the Advanced section.
5. Tap Site settings.
6. Tap Microphone.
7. Toggle to the ON position.

Impact:

Users will be prompted each time a website requests access to the microphone.

Default Value:

Enabled.

CIS Controls:

Version 6

13 Data Protection

Data Protection

(L1) Ensure 'Location' is set to 'Enabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

This setting controls if a site asks before accessing the location. The recommended state for this setting is: Enabled.

Rationale:

Websites will have to ask permission before being allowed to access the location which will help prevent unwanted access to the users location and help protect against potential privacy concerns.

Audit:

Follow the below steps to verify that Location is Enabled:

7. Tap Chrome icon.
8. Tap Menu icon.
9. Tap Settings.
10. Scroll to the Advanced section.
11. Tap Site settings.
12. Verify that Location displays Ask first.

Remediation:

Follow the below steps to Enable the Location permission request:

1. Tap Chrome icon.
2. Tap Menu icon.
3. Tap Settings.
4. Scroll to the Advanced section.
5. Tap Site settings.

6. Tap Location.
7. Toggle to the ON position.

Impact:

Users will be prompted each time a website requests access to the location

Default Value:

Enabled.

CIS Controls:

Version 6

