**Introduction**

**Social media**

Social media refers to the means of interactions among people in which they create, share, and/or exchange information and ideas.

In simple words, social media is an online platform, where people share their ideas and they communicate with each other.

Social media has become a powerful tool for businesses to use in connecting with their customers.

But rather than this, what if people share their personal information on social media?

By posting personal information cybercriminals can get access to your personal data, they can impersonate (they can act as u or stealing your identity).

Hacks target people's social media accounts to extract sensitive and private data for malicious intent.

If we overshare our personal data online, we'll encourage these online criminals to commit business fraud in our name.

Examples: 1) posting a picture of credit card

2) posting personal information like any password.

Personal information should not be shared online because it can be exploited by others.

**How to create a fake account on Instagram**

**Why do you need to create a fake Instagram profile?**

**To Align with marketing goals, branding, and strategy.**

Especially if your brand has a specific look and feel, or key colors and themes, creating a fake Instagram profile will allow you to get an overview to see how you can best align it with marketing goals, branding, and strategy.

## Simple steps to create a fake Instagram profile.

**1. Gather your intended account details**

Gather all the details you need to fill in the basic aspects of your Instagram profile:

* Account name
* Website
* Brand/profile description
* Profile picture or logo

**2. Prepare intended posts and categories**

With your branding, color scheme, and marketing goals in mind, prepare the following:

* At least 6 mock posts (think both pictures and stills of videos) you intend to have
* At least 3 categories you’d like for your Instagram Story highlights

**3. Choose the Instagram mock-up** **template you’d like to use and start creating**

* Insert your text (channel title, small title) using the sidebar menu.
* For all picture sections (profile picture, highlights, posts), drag and drop your picture directly into the section you want.
* If you’d like to have fewer highlights, you can take away the other highlights by turning off the following in the sidebar menu:
  + Highlight Title
  + Highlight

**Steps to share personal information on Instagram such as mobile number, address, etc.**

Sharing your personal information on Instagram such as your mobile number email address or address might be helpful for contact purposes but also might be risky at the same time.

For example: if you are a content creator on Instagram and somebody is interested in your videos, if anybody joins with you then you have to share your personal number information like address etc. through Instagram, we can get in contact with interested people in our topic. So instead of sharing information individually in direct messages we can have a contact button feature on our Instagram profile so that anybody can easily contact with us

**Here are the steps to share the contact number on our Instagram profile:**

**Step 1:** Open your Instagram

(Now you have to change your personal account to a business account)

**Step 2:** open the Insta profile & click on edit profile

(Here you will get the option to switch to a professional account)

**Step 3:** Click on switch to professional account & here you will get some instructions

**Step 4:** Click continue

**Step 5:** then select the category & click done

(Here you will be having options such as video creator, blogger, artist, etc you can choice)

**Step 6:** select creator and click next

Now here you will get welcome greetings you can skip this

**Now your account is switched to a professional account**

**Step 8:** Now click on edit profile

**Step 9:** here click on the contact option

**Step 10:** now click on the business phone number icon and type your mobile number

**step 11:** now by clicking the right tick mark on top save changes

Now in your profile, you will get this type of call option. Whoever opens your Insta profile they can see the call option there so that they can contact you easily.

**How the process of posting something personal is risky?**

Personal and financial information are currency for cybercriminals online. With your stolen identity, a cybercriminal may be able to access your bank account or obtain credit cards or loans in your name and potentially ruin your credit rating.

You need to be careful with how much personal information you reveal online. Sharing your address, phone number, birthday and other personal information can mean you are at a greater risk of identity theft, stalking and harassment. This includes information you post on social media.

Cybercriminals can piece together your identity from information that is publicly available about you, so think about what information you are sharing online.

Treat your personal information as you would treat your money—protect it and don't leave it lying around for others to take.

**How to protect your personal information in social media**

1. Don’t Share your live location on Daily routines: Just an example many of us share photos while we are on a vacation this can be fun, but those photos immediately let another know that you’re away from home.
2. Don’t share identification Numbers: You may not think so, but your identity can be stolen just with your identification numbers
3. Share less in the “About” section: Social media platforms let you share all kinds of personal information online. But all this information just adds to your online footprint.
4. Only accept connection requests from people you know: On social media platforms, you should always accept followers and friend requests from people you know.
5. Create a strong password, a unique password.
6. Don’t ignore software updates.

**Effective ways to hack personal information from social media**

**Phishing Attacks**

The attacker usually shares something tempting that increases the chances of you clicking that link. If something sounds too good to be true, it probably is. Some common scam campaigns may include Whether you stick to email communications or instant messaging, you will find phishing attacks everywhere

**Impersonating You to Get into Your Network**

Your photo, your work details, and other bits of key information can usually be found with a quick search for your social media profile.

Anyone can easily create a fake account impersonating you using the data you have shared over Facebook, Twitter, or even LinkedIn.

The attacker may use this account to connect with your colleagues or friends to conveniently get access to more data; your contacts might not realize they’ve connected to a fake profile until it’s too late.

**Accessing Your Account with Publicly Available Information**

You may have shared your date of birth, phone number, pet’s name, and many other things on social media

So, if your password or security questions includes the name of your pet, your family, or your phone number, a malicious attacker may be able to guess the passphrase or otherwise gain access to your accounts.

**Creating a Filter Bubble**

Creating a filter bubble refers to building a network around you that exposes you only to one type of information.

In other words, it’s using a network of friends, influencing you to follow certain topics, so they control the type of posts you come across in your social media feed.

This is not something easy for an attacker to do—but if they manage to do it, your actions and may be a result of the information you are exposed to.

Sometimes, social media itself becomes the culprit by showing you only one type of information and prevents you from knowing the other side of a story or something that you do not believe in

**Coordinating Physical Scams**

Most people share their travel plans, location, material interests, and similar data in social media platform.

Using this information, an attacker can coordinate a physical attack or even visit you purporting to be gathering official details via a survey related to your interests to extract more information about you. Or of course, if they know you’re away on vacation, your house might be a target for physical attackers.

**How Do You Avoid Getting Hacked**

Do not overshare information (personal interests, recent purchases, details about your family) online.

Do not share your real-time location anywhere.

Carefully select the friends you connect with and respond to.

**WHAT CAN HACKERS DO WITH YOUR DATA**

**1. Hackers can sell your data to other criminals**

One way hacker profit from stolen data is by selling it in masses to other criminals on the dark web. These collections can include millions of records of stolen data. The buyers can then use this data for criminal purposes.

**2. Stolen personal information is fuel for identity theft**

Identity theft is a crime in which the victim’s personal information is used to gain benefits at the victim’s expense. Many online services require users to fill in personal details such as full name, home address, and credit card number. Criminals steal this data from online accounts to commit identity theft, such as using the victim’s credit card or taking loans in their name.

**3. Login details are needed for account takeover**

Criminals use stolen login credentials to break into accounts with payment details, such as shopping accounts. This is called account takeover, and it often leads to identity theft. If the hacker changes your password, you will also lose access to your account. Account takeover can be costly if the hijacked account includes payment details.

**4. Stolen data is used to target phishing attacks and extortion**

With stolen personal information criminals can target victims with phishing attacks. In phishing scams, victims are lured into giving information like credit card details willingly to criminals by masking the scam as something legit. If criminals get access to very sensitive information, they can also extort the victim.

**5. Stolen personal information can be used to harm companies**

In addition to the personal problems stolen data can cause, it can also damage companies. With stolen data criminals can target company personnel to give sensitive information or to trick them to make payments. Such phishing attacks targeted against a specific individual are called spear phishing. Criminals can also try to gain access to company networks to spy on them and infect them with malware.

**6. Distributed Denial of Service (DDoS)**

A Denial of Service (DoS) attack that uses multiple devices to launch. Hackers flood you with traffic to eat up bandwidth and resources. You have to scramble to fix it and go offline if you haven’t crashed already. Why hackers bother: It’s a revenge move and a useful diversion for hackers trying to break into your otherwise monitored system.

**7.SQL Injection**

Hackers sneak malicious code into an SQL database or website. It tricks the backend into releasing information that otherwise wouldn’t be public—like a list of payment info stored on a retail site. How easy is it: So easy that automated programs exist. A hacker could destroy your business just by inputting your URL.

**8. Hacker need data to Preform Phishing attacks**

So popular that 80 percent of 2019’s reported attacks were phishing attacks. Hackers send emails posing as reputable contacts—someone in your organization or a known brand—hoping to trick you into sharing information or downloading malware. is a targeted attack by the same methods, where hackers go after individuals with higher access or privileges. Vishing is phishing over the phone. Your voice confirms your PII, credentials, financial information, and more to the very reputable lady who was calling from the bank. Smishing is similar but uses SMS instead of voice.

**How our personal information is being scraped from the social media**

**First let us discuss about data/web scraping?**

🡪 A scraping simply refers to the extraction of the data from a website, this information is collected and then is exported into a format that is more useful to the user

* for example, the user can simply use the this to extract a list of product names and their prices from amazon ecommerce website Later then store them in an excel sheet in order to sell them for the best price possible.

**How do web scrapers actually work?**

🡪 At the very initial step a web scraper will be given 1 or more URL to load unambiguously.

Then they load up the entire HTML page in question, most advanced scrapers render the entire website including CSS and java script.

* The scrapers will not only focus on extracting each and every ounce of data present in the page instead they target some of very particular parts.
* Let’s here an example of the amazon ecommerce website as I mentioned earlier the items name and the price list that are sourced out the scrapers then download the gathered intel into a excel spreadsheet, similarly our very own credit card details are collected through such ecommerce websites and then can be sold accordingly, to many of the other hackers there.
* The scrapers can come in many other different forms with the various other features included like browser extensions or more powerful desktop applications that is downloaded into our computer.
* Web scrapers can get access to our classified intel using our computer resources and also using our internet connection or on cloud without even using our computer.
* You guys might be wondering how is this even possible, well answerably these can also be built just like websites by coding as well.

**What are the precautionary measures we need to mind to secure our data?**

* By not allowing the cookies of each and every website we visit.
* by frequently changing our password of our Gmail account in order to secure our data online.

**Social media privacy Concerns**

Social media plays a greater role in our lives with each passing day. As such, privacy on these networks has never been more important.

1. Account Hacking and impersonation: Increasingly, spammers, hackers, and other online criminals are targeting social networks like Facebook, Twitter, and Instagram and using them to carry out a variety of cyber-attacks.  Example: Once hackers get access to your t they can impersonate you and use the trust you’ve built up with followers to get them to download malware or give up confidential information.
2. Stalking and Harassment: social media is a gift to stalkers and harassers in that it often provides them with a detailed description of what you do and where you go. As such, the more you share on social media, the more vulnerable you are to physical and cyber-attacks.
3. Being compelled to turn over password: occasionally, employers ask job applicants and new hires for access to their social media accounts, usually to help in the candidate screening process or to ensure that employees aren’t sharing confidential information or trade secrets.
4. The privacy downside of location-based services: Most of today’s social media users don’t access the services on a traditional computer, they do it on their smartphones. As social media continues to take advantage of mobile devices and location-based services, this leads to being targeted by thieves or stalkers due to geo-location data automatically shared by their social media apps.

**Some tips to keep your privacy protected:**

1. Use strong passwords, and don’t use the same password for multiple accounts.
2. Don’t use social media on public devices, and if you must, make sure to log out afterward.
3. Disable access to geo-location data for your social media apps.
4. Be wary about clicking links from friends in social media; you never know if they’ve been hacked.
5. Use two-factor authentication or password-reset checks for all your accounts.
6. Even on your private social profiles, [keep personal information to a minimum](https://www.reputationdefender.com/remove-personal-information).

**Real cases that affected during the misuse of data in social media**

**Some cases that happened when the data is lost or data is misused by someone:**

* **FACEBOOK**

In December 2018, Facebook found a bug Facebook found a bug that may have affected personal photos of around 6.8 million users, including photos that users had kept out of their timelines. “The bug potentially gave developers access to other photos, such as those shared on Marketplace or Facebook Stories. It also impacted photos that people uploaded to Facebook but chose not to post," pointed out Tomer Bar, who was then an engineering director at Facebook. When the photos were shown to photographers, they were surprised as they and the subjects in the photos had no idea that those photos were being used for research. There are several cases where photos shared by users on social media or image hosting platforms were stolen, made public to humiliate or blackmail them and misused for fraud and identity theft. A recent McAfee survey involving 1,000 parents found that 30% of the participants were uploading photos of their children daily and 58% of them did it without the child’s consent. However, many of the participants feared that the photos of children could lead to cyberbullying, stalking and kidnapping. "Identity theft is no joke. Photos can reveal a lot about your lifestyle, your habits, and they can unintentionally give away your data," cautions Toni Birdsong, family safety evangelist for McAfee, who authored the survey.

**• GOOGLE**

A few years ago, Google was accosted by a Canadian woman whose photo in a compromising position was captured by a Google Street View vehicle while she was relaxing on the steps of her home. The photo ended up in the Street View platform. Though Google had blurred the face of the woman, they did not blur the number plate of her car which made her identifiable. In 2014, an iCloud flaw led to a major privacy breach involving hundreds of private photos of celebrity users. In another more recent case from March 2019, a mobile tracker app, used by parents to monitor their children, was accused by security experts for leaving 95,000 images of users unprotected on servers that were accessible to anyone. Users can check if their photos have been shared online without their knowledge by using Google’s reverse-image search function on both mobile and PC.

**What personal information should not post on social media?**

To help protect your personal information from identity thieves or other fraudsters, don’t ever post

* usernames or passwords to anything
* debit or credit cards
* paycheck or any financial account numbers
* your social security

**The dangers of sharing personal information on social media**

* Joseph Turow, a professor of communication at the Annenberg School for Communication, says hackers may be using your posts against you.

“

* Hackers looking to break into your private accounts could use any piece of information you share in a viral challenge,” Turow says. Year of graduation, cities in which you’ve lived and the makes and models of all the cars you’ve owned are examples; those cars, cities, and graduation years may show up in photos you share. (Often photos contain side information about date and location.)

**CONCLUSION:**

* Never your passwords with any one
* Criminals can try to use this information to get more information from you that will then allow them to target you for money out of some online accounts,” Turow says. “Hackers are continuously looking for ways to get into people’s files to find out ways to get into their monetary accounts and take on some aspects of one’s identity in some type of way.”
* Be careful when one parties ask you to minimize the overlap of passwords.
* Never click on a link in an email unless they are sure who sent it.
* Common way for scammers to infiltrate your computer.
* Stop and wait before you share anything and think about it. Realize that when you put anything in an email or social media and act as nothing on the internet is private.