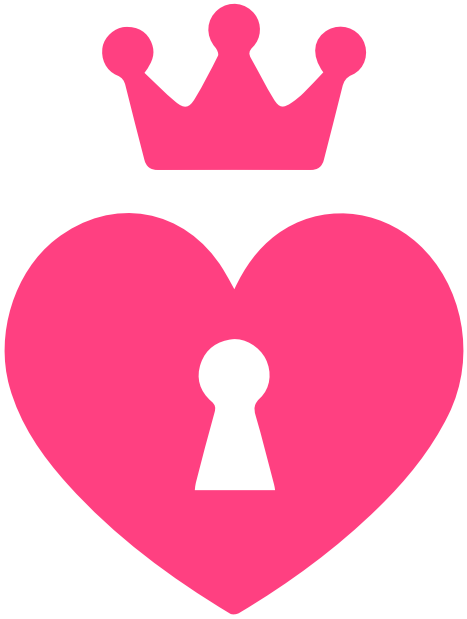

MANYVIDS

Privacy Checklist

Introduction

Welcome to ManyVids, and thanks for checking out our Privacy Checklist. While camming is some of the safest sex work around, every occupation has its hazards. We've compiled this list of tips and tricks for you to use to have a safer, more pleasant experience using MV. Of course, every MV Star is free to decide what is best for them and their circumstances, and this information is simply provided as a guide for increasing your privacy—so feel free to only use what fits your needs.

1 Tech Tips and Services

Keep separate "business" and "personal" email and social media accounts:

Using a separate email to access your ManyVids account and associated social media platforms will reduce the impact on your privacy should your email get hacked. Make sure to not include your legal name or personally identifying information in this email address.

Beware of social media algorithms:

As social media algorithms are particularly good at attempting to "connect" people with similar interests, keeping separate followers on your adult-industry content-creator social media account and personal accounts is essential for privacy. For instance, if you have personal friends who follow your adult-industry content-creator social media account, their followers (likely other people you know) may receive suggestions to follow you, and effectively 'advertise' your ManyVids, adult content, within your personal social circle. For Instagram (IG) in particular, you can log in to your personal account and search for your adult industry IG account, and it will show 'mutual followers'. You can then block those from your personal life who have been following your adult industry account.

Post different photos on your "business" and "professional" social media accounts:

This reduces the possibility of these accounts being linked to one another through Google's "Reverse Image Search" app. This app allows people to search for images (instead of words or phrases), and can find other locations that the photo has been posted—effectively linking your ManyVids and personal social media accounts if you share the same photo on both.

Refrain from giving out your phone number:

While giving out your phone number may seem like a good way to increase contact and interest with MV members, it creates more opportunities for harassment and/or stalking. Such close personal contact with MV members can also breed a false sense of intimacy for the MV member, and lead them

to demand in-person meetings with you, followed by threats of harassment or violence if they don't receive it. If you insist on providing your phone number...

Use a burner phone or separate number:

In the rare case someone "hacks" your phone, having a separate phone or phone line reduces the impact of this event. You can download a free app onto your existing phone like "TextMe Up Free" or "Burner - Free Phone Number" to create temporary second line, or pay a monthly fee through an app like "Hushed" that creates a permanent second line.

Password protect all devices:

You never know who's around if you need to step away from your computer in a library or cafe (although it's not recommended you do this!). Having a password protected lock screen stops people from easily gaining access to your information.

Always use strong and unique passwords.

Passwords should not contain any personal dates, names, or usernames. They should include at least one letter and one symbol. As an added protection, change your passwords regularly. TIP. Set an "Reminder" on your calendar (on your desktop or phone, or wherever you'll see it) every three months to alert you to change your passwords.

Use a Two-Step Password Verification Service for ManyVids, email, and all other sites requiring sign-in:

ManyVids offers this service through your account, and gives you enhanced security by requiring a 6 digit code be entered whenever you log-in, in case someone figures out your password. Check out this MV Blog for step-by-step instructions:

https://www.manyvids.com/Article/825/Bulletproof/

For other sites, a two-step verification process will be available through your account settings.

NOTE: Recovery codes will be provided in case you were to lose your device—make a physical copy of these and put them in a safe place!

Use a Password Manager:

Keeping track of all of the passwords required for two-step verification can get overwhelming. So if you're using two-step verification across the platforms you use, or if you're prone to using the same password for everything, or recycling previously used passwords, a password manager can help generate and store all of your passwords using one centralized application. Each one is slightly different, but basically a password manager creates highly complicated passwords for the accounts you choose and stores them in one central place for you to access. One example is Dashlane, which also allows you to download the app on your computer and mobile device, and sync passwords between devices.

Ensure location services are "OFF" on all your devices:

Photos taken on your phone automatically have the location where they we taken stored in them if the location services are not disabled. This means that by downloading a photo of you taken with your phone, a user could (easily) gain access to your exact location using GPS data embedded into the photo.

To disable GPS data, follow these steps:

For IPHONE:

Head to Settings > Privacy > Location Services > Camera, and then select "Never" for the "Allow Location Access" option.

For ANDROID:

Each device will have a different process, but should follow a similar path. It may look something similar to this: "Apps > Camera > Permissions or Location Services > Locations or Disable toggle". By looking around on your Camera app's settings page, there should be something indicating the ability to "disable" this feature. If you're unable to find it, you can always Google the make and model of your phone along with "disable location services".

What if I already took photos without disabling geolocation? No problem! We found this link:

https://www.howtogeek.com/203592/what-is-exif-data-and-how-to-remove-it/

to have clear and useful instructions for removing this data on photos you have already taken (although you will have to remove the content and replace it with the photos that no longer have the location data).

Cover your webcam while not in use:

Mark Zuckerberg (creator of Facebook) does it, which is as much evidence that you should do it that we can think of. You can simply put a piece of a post-it over your cam lense, or purchase a webcam cover.

ManyVids takes action on copyright infringement:

Sometimes, your content can be taken and re-posted on other sites without your consent. To help counter this, ManyVids now offers the latest in anti-piracy protection to our MV Stars through our partnership with DMCAForce and DigiRegs. We automatically scan the entire web on behalf of our MV Stars to locate any stolen content featuring this ID.

- We issue **DMCA** takedown notices everytime we find an illegally uploaded vid. Not only that, through **DMCAForce** and **DigiRegs** we are in collaboration with many major tubes sites to prevent piracy at the source. These sites will block stolen content from being uploaded in the first place.
- We stay on top of the latest initiatives and upgrade our technology to help protect our MV Stars.

Use a VPN (virtual private network):

Even though we may feel safe behind a computer screen, your Internet Service Provider (ISP) actually sends out information (your IP address) that, for the tech savy, can be used to find your location. (NB: While you are Live on MV Takeover, your IP is protected by the site.) Using services like Skype and Hangouts can also reveal your IP address to those communicating with you. A VPN is a simple and legal way to make your online presence more secure and private, by masking your location and making it appear that you are connected to the internet in a different region (the region the VPN service is located in). While there are both free and paid services, free services often limit the amount of data you can use through their service per month, which will make it unsuitable for most cam models. On the plus side, paid services only cost between $3-6 USD a month (on average).

This article:

https://www.vpnmentor.com/blog/criteria-look-evaluating-vpn/

outlines some great criteria for choosing a VPN service (“bandwidth” is super important for camming!) and this article:

https://www.comparitech.com/blog/vpn-privacy/best-vpn-for-porn/

provides some tested and recommended products, such as anti-virus software. After you download the software that suits your needs, it will guide you through set up access instructions.

2 Performance Management Tips

Do not share personally identifying information on your ManyVids account:

Including in your ManyVids content, or through content shared through 3rd party platforms (Snapchat, Twitter, Blogs etc.).

Examples of personally identifying information that may be best left out from your ManyVids content (and related social media accounts) include:

1. **Your legal name or the legal name/username of people you know:** With this, access to your location, workplace, family, and friends becomes far more easy.
2. **Details about your life:** Perhaps you have a partner who has a really cool job, or a child that just hit an age milestone, or a friend with X-number of cats. While not likely harmful by themselves, over time, these small details can add up to a pretty clear picture of who you are. To protect yourself and others in your life, you may choose to keep things vague - but this doesn't mean your personality can't shine through!
3. **Your address or location:** Remember, the location you choose for your public ManyVids profile does not need to indicate your location IRL (in real life). If you choose to disclose your general region (state/province), ensure to take extra precaution when mentioning any specifics of your location (including neighborhoods, intersections, nearby attractions, restaurants or non-chain stores you may frequently visit).
4. **Photos of anyone other than you, with the exception of other consenting/verified adults:** It's a small world, and the more details people can associate with you, the more likely it is they may be able to determine your personal details.
5. **This goes double for photos of minors!** Of course, photos of minors on your ManyVids account is prohibited and will be taken down. As for your related social media accounts, we understand how tempting it is to want to share the adorable things your kids, nieces, or nephews do, but keeping these to your personal accounts protects not only your identities, but those of the children you care about.

Be aware of people claiming to be MV Team members:

If ManyVids requires more information or identification from you, we will contact you using official ManyVids channels (emails ending in ...@manyvids.com). You can always double verify the MV Team message or request by contacting our support team at help@manyvids.com.

Do not give out your full name/address when filling out DMCAs:

While this is often unknown, it is not mandatory for you to use your real name. Instead, use your stage name/user name and PO box, and avoid giving your personal information to third party websites.

Post photos / snaps / vids only AFTER you've relocated.

Posting about your daily activities may indicate your location (a specific mall, coffee shop, or library). By posting photos/snaps/vids after you're long gone, you get to share all the details of your day without jeopardizing your privacy.

Keep track of what's around you:

While filming vids, taking photos or camming, make sure to remove anything with your name on it that could appear on your content. This can include necklaces, coffee mugs, Starbucks cups, picture frames, cards, mail, etc. This includes your surroundings—make sure not to post photos or videos that would give away your address or neighbourhood (such as major attractions, the view from your window, or street names).

When filming or camming with others:

Before each session, it may be helpful to discuss what your expectations are for sharing and privacy. Others may have a more lenient sharing policy or not care about sharing their location with others, which could then indicate your own location. Discussing these issues before creating content will help you control your information and privacy. Also ensure to use a Co-Model Agreement which can be accessed through: Drop-down menu > My MV > Settings > Co-Model Agreement.

If you meet another MV Star to film content, meeting in a different city may help protect your identity. Try to always ask for referrals from other performers to make sure you are working with a respected and respectful content creator. Make sure to let someone you trust know the location and time of your meet up, and arrange for them to be expecting you to “check in” with them throughout the shooting or photo shoot to ensure your safety.

When mailing products/gifts to MV members or receiving gifts:

Even when you don’t put your return address on the package (don’t do this either!), the address of your post office will be displayed on the package. You may wish to visit another city, set up a PO box for a return address, or only provide digital products. For Amazon Wishlists this also applies—while you can set your account up as “private” so that regular Amazon users can’t view your address details, some members are savvy, and will set up their account as though they were “Third Party Sellers”. This means they can gain access to your address. For ease of mind, setting up your Amazon Wishlist with a PO box will keep your address from being uncovered.

Be mindful of what gifts you do accept:

Be wary of accepting gifts that can be compromised remotely; this means computers, phones, or even cameras. These gifts may have programs (viruses) installed on them that allow the sender to access them from their own home - gaining access to the webcam, microphone, or even being able to witness everything you do while using the device, including your passwords! Instead, perhaps ask for a giftcard in the amount of the device you’re hoping for so that you can purchase it yourself from a trusted seller.