



Physical Security

Keeping yourself and your loved ones safe while attending events is just as important as cyber security. Knowing how to properly prepare is vital to the health and wellbeing of you and your family as well. To keep you and your loved ones safe at events, here are some resources for investing in your physical security.

Be properly prepared

1. Bring proper supplies to the event

Ensure that you know what the weather is like on the day of the event, and pack accordingly. For example if it is going to be a hot day and an outdoor event, bring snacks, water, and something to help cool you off, such as ice water soaked handkerchiefs. Regardless of the weather, make sure you have mobile phone chargers.

2. Wear proper attire

As well as checking the weather for proper supplies, make sure you are wearing appropriate attire for the event you are attending.

3. If attending a political event or rally

While attending political events or rallies, your personal safety is even more important. Ensure you have a lawyer's phone number written on your arm, and that any identifying tattoos or piercings are covered by long sleeves and extra garments to help obscure your identity.

Stay Vigilant

Be aware of your surroundings. If you are being followed or witness something alarming such as harassment, communicate with trusted people around you and move to safety if possible. Usually there are designated safety teams for our events, and you should know who they are to make them aware of anything that could be potentially unsafe or dangerous.

There is Power in Numbers

Traveling in groups, and at minimum in pairs, is one of the most effective ways to reduce your chances of being singled out or targeted by anyone trying to harm you. Communicating and moving with people is a good way to practice solidarity in real time: Remember, "we keep each other safe." Always have someone you can call on in case of an emergency.

Before going out, share the time frame and location where you'll be with a trusted friend or family member.

Follow DPS Orders

While on government property, if you are being directed by DPS for any reason, follow orders and instructions, as well as verbally respond. For example if a DPS officer tells you to move you should respond

www.transtexas.org | info@transtexas.org | [@transtexas](https://twitter.com/transtexas)



with "I'm moving as fast as I can" or "I hear you and I am moving". Doing so ensures the highest likelihood of DPS not arresting or using force against you and others.

Do Not Engage with Opposition

While attending events, oftentimes there will be counter protestors or people with oppositional opinions, or even people from well known podcasts. While they may shout or jeer or attempt to get you to interact, we highly encourage you to avoid these people at all costs. We have safety teams in place to assess and handle each situation. If they approach you directly and continue to antagonize you, try to find the nearest safe room to retreat into.



Digital Security

Digital security is always important, especially for the parents of transgender and gender diverse children in Texas right now. In order to avoid unwanted attention from unfriendly people and internet trolls and to protect the privacy and safety of you and your family, here are some resources for investing in your digital security.

4 Easy and Simple steps to Increase Digital Security

1. Set your social media to Private

Your social media is one of the easiest ways for people to find personal information. By setting your social media to private you can protect yourself and your family by not allowing strangers to see things like your city, state, home address, phone number are other identifying information. If you want to exercise additional caution, keep social media accounts for friends and loved ones separate from accounts where you post political content.

2. Practice safe password keeping

Changing your passwords regularly and frequently and avoiding reusing the same password for multiple websites is the best way to avoid having your password stolen. There are many ways to accomplish this if you have too many passwords to memorize, one of the best is to have a password manager. Password managers (like 1password or Dashlane) are software and web plugins that automatically keep track of your passwords for different sites and sometimes will generate and store them for you. Using a long alphanumeric password (and Two-Factor Authentication) is the best way to keep someone from accessing your phone. Using fingerprint sensors and face recognition are the least safe ways to secure your devices.

3. Keep your devices up to date on any software updates

Software updates are an incredibly important part of cybersecurity, as system exploits can only be patched through these updates. New exploits are discovered in software every day, and keeping your devices and software up to date is a great way to make sure you are as protected as possible from hackers or malware.

4. Use a VPN and an anti-malware

A VPN is a virtual private network, and it prevents hackers, your internet service provider and others on your network from monitoring your web traffic as well as encrypting it. VPNs are incredibly useful for digital safety and as a nice bonus you can view streaming content from other countries and region locked content on social media websites. Antimalware is useful for monitoring your computer



for viruses and malware, however it serves as a last line of defense and you should also take preventative steps in responsible internet usage.

Public Data and Data Brokers

Just about everything you put on the internet is sold and bought by data brokers for any number of reasons. There are many sites such as [Spokeo](#) where you can look yourself up and see if you are on any of these data broker lists and request to have yourself removed, as well as [DeleteMe](#) where for a monthly fee you can have your data regularly removed from these lists. These sites hold a lot of information and the older you are the more likely they have information on you, including things like financial information and court documents in some cases.

Data Breaches

Data breaches occur when hackers break into large databases of user information through company or government servers and leak or sell the info online. Data leaked can include names, addresses, login information like passwords, credit card information and much more personal information. Websites like [BreachDirectory](#) can be used to see if your information has been leaked, along with what information was released.

Parent Groups on Social Media

Parent groups are a great way to get information and engage with an active online community, however, you need to be wary of what groups you join. Well-informed internet use is vital for digital safety, as your information becomes increasingly public, especially in social media groups. Public groups are easier to join than private groups are, but they also tend to be less secure and you cannot guarantee that everyone has the same values as you and wishes you the best. Before you join a parent group and start sharing, check the group's privacy settings and make sure that it's private so any information you share won't be publicly released. TENT has a Facebook Parent group that's well moderated by our staff and set to private, for the safety of community members.

Messaging

Use an encrypted messaging app for all sensitive communication. [Signal](#) is the safest option, followed by Telegram. Both applications have end to end encryption, but Signal is the only platform that will not share your data with authorities seeking your information. Avoid Meta platforms such as Facebook Messenger, Instagram, and Whatsapp.