WV Executive Branch Privacy Tip

TMI – Be Careful What You Share!

April the Giraffe is Expecting Again! Is She Also Due For a Privacy Checkup?

This tip is brought to you by the Identity Theft Resource Center © Copyright 2018

April the Giraffe became an internet sensation in 2017, bigger perhaps than any pop-star-behaving-badly, for her adventure park's YouTube live stream of her pregnancy and delivery. It took a little longer than expected, but she gained a following of millions of viewers for the birth of her first baby to be born at the park, Tajiri.

At that time, many people had a tongue-in-cheek criticism of the whole sensational affair: how would *you* feel if someone broadcasted your pregnancy and delivery to the entire internet?! In fact, in recent years, more and more hospitals have instituted policies against this very thing, banning video cameras, digital cameras and even cell phones from the delivery room to give the mom and baby both some privacy.

Obviously, April didn't seem to mind either the jokes or the constant attention directed towards her medical condition. Hopefully, she's just as calm about the April Cam going live once again for her next delivery. But that doesn't mean we should be so laid back about our own privacy and oversharing of personal information.

Oversharing happens when we post more information or content online that might be safe. It could be sharing too many details in your social media profiles, entering information online without finding out where it will end up, even posting photographs that in hindsight probably shouldn't have been made public. In any event, oversharing is a serious problem that can lead to consequences like identity theft, account takeover, repercussions at school or in the workplace and more. In order to avoid oversharing, there are a few things to keep in mind:

1. Social media settings – Who can see your posts? Do you know how to keep others' prying eyes out? Depending on the platform, such as Facebook versus Twitter versus Instagram, you have options when it comes to keeping your content limited to people you personally know. To check up on your privacy settings, log into your account and go to your profile. Note: that's not to say everyone must lock strangers out altogether, but it's good to know how to set up your preferences and change them if you wish.
2. Locations – If you have location settings turned on for your phone or other devices, you might be handing a criminal the exact location to where you've taken a photograph, even down to which room in your house. A concept called geotagging incorporates these coordinates into the digital file for the image, and when you upload that image, you can retrieve the coordinates by someone who accesses the picture. In order to keep your location under wraps, be sure to turn off the location settings for your device's camera so, anyone with malicious intent doesn't come looking for the flat-screen TV or MacBook in the background.
3. Sensitive content – Finally, once you're certain that the posts aren't giving away too much, really think about what's in the post, photo or video. Is this something that paints you in the best light? What will an employer say about it? Is it embarrassing to anyone in your family, including your kids?

Remember, April the Giraffe may not understand that millions of people around the world watched her every move—including an event that most people consider to be very, very private—but you and your friends or family might care a great deal. Protect your privacy and your dignity with safe, smart sharing behaviors.

Contact the Identity Theft Resource Center for toll-free, no-cost assistance at (888) 400-5530. For on-the-go assistance, check out the free ID Theft Help App from ITRC.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.