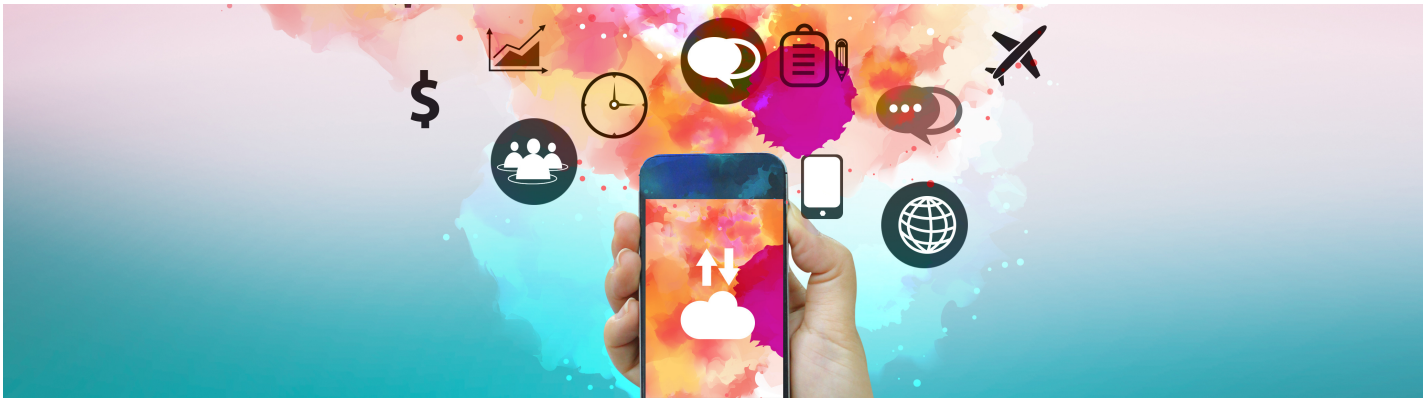
UNIVERSITY OF TEXAS ARLINGTON | INFORMATION SECURITY OFFICE

7 April 2022



The Weekly Briefing

The latest cybersecurity updates from the Information Security Office.

Staying Secure on Social Media

Social media is an integral part of our world. And as social media becomes more important to individuals, companies and organizations, so too do the dangers associated with it. Cybercriminals flourish on these platforms. Even with safety measures put in place, they still present a formidable threat to your security.

One thing to keep in mind is to pay attention to geopolitical conflicts. Events such as the 2022 Russian invasion of Ukraine strain the relationship between the US and adversary countries. The Russian state regularly employs cybercriminals to target American citizens online in a form of hybrid warfare. Your information could be at greater risk of being stolen during these periods of worsened relations.

There will never be a situation in which sharing your location is a good and safe idea.

Sharing your vacation plans online provides a golden opportunity for cybercriminals. Doing this gives them two things: access to your active location (which allows them to find you), and the knowledge that you are currently away from home (which allows them to know when your home is an easy target).

When on vacation, keep information about your trip to a minimum. Disclosing your hotel, cruise or resort is far too risky of information to trust to the internet. Remember, what you post can be seen by anybody. You never know when the wrong person will take advantage of your information.

Don't lose control of your security on social media.

There is no delete button on the internet. Be careful about what you choose to post and share. Even if you delete it later, chances are, somebody has already seen it. Not only that, but everybody has the ability to see it. Even if you restrict viewership, skills cybercriminals can bypass these restrictions with ease.

Keep your privacy settings updated, and pay attention to how you are being tracked. Social media apps and companies track everything from what you post, see, like and follow. But it extends beyond this as well: pay careful attention to what permissions you give companies when sharing your information. Especially be sure to disable geotagging, which allows anyone to see your active location at any given time. When social media sites update their privacy options, pay close attention to this as well.

Don't accept strange friend requests. Only connect with people that you know and trust. Cybercriminals love to hide behind what seems like a real person on sites such as Facebook and Instagram. Accepting their friend requests allows them greater access to your information, and also makes it easier for them to hack into your account as well. Be wary when you receive a friend or follow request from a new profile of an existing friend.