UNIVERSITY OF TEXAS ARLINGTON | INFORMATION SECURITY OFFICE

21 April 2022

The Weekly Briefing

The latest cybersecurity updates from the Information Security Office.

Cybercriminals & Your Social Media Accounts

There are several ways that cybercriminals try to prey upon users of social media. While these methods are too many to list, some methods are more prominent than others. The reason that these work so well is because many people on social media are unaware that these are actually methods used by cybercriminals to gain access to accounts, personal data and sensitive information. Users on these sites oftentimes innocently participate in activities designed solely for the harvesting of personal information. Practicing awareness and caution will prevent yourself from falling prey to these methods. Read the two listed below and use this knowledge to your benefit while browsing social media sites.

Cybercriminals may takeover existing accounts.

Through a method called "account takeover", cybercriminals hijack an existing social media account. This could be the account of an individual, company or organization. They will then use this account to their benefit in several ways, from posting offensive or damaging content to your profile, harvesting the information stored on your account, or even through trying to gain access or information from your list of friends or, in the case of a company or organization page, your list of page administrators.

The best method to avoid having this happen to your account or page is actually to pay attention to other accounts or pages which have had this happen to them. Cybercriminals will use the hacked account to send friend requests and messages to accounts on the hacked account's friends list. If you receive a strange, uncharacteristic message (oftentimes sent with a link) from a friend on Messenger, don't interact with it or click any link sent. Instead, say something to the friend on another platform. They may not even know that they have been hacked.

One of the most popular Facebook trends, the copy-paste game, is actually something designed to harvest information that will put your information at risk.

Anybody who uses Facebook can remember seeing these surveys posted and filled out by friends and loved ones. In fact, many have participated themselves. On the surface, these games look like fun ways to pass the time and share interesting trivia about yourself to your friends.

The games might ask the following questions: "What is the name of your first pet?", "Who is the last person you texted?", and "What is your favorite number?". These games will always have an "empty form" pasted into the comments so that you can post it onto your own page.

Your friends posting them aren't posting them to harvest your information – that's why it's so easy to trust. However, this game is a tried and true method used by cybercriminals and bad actors to gain information about you that could be used to figure out your security answer questions, your passwords, and other personal information.