The dangers of sharing personal information on social media

May 20 2020, by Dee Patel

Credit: CC0 Public Domain

An innocent, seemingly fun and engaging social media trend has been popping up on news feeds. In an act of solidarity with high school seniors who were finishing out their final semester at home due to the

coronavirus stay-at-home order, Facebook users were sharing their own senior class photos in nostalgic posts.

While it is a nice sentiment and the presence of cameras in nearly every cellphone has made it easy to take and exchange pictures, there are certain considerations one should keep in mind, according to Joseph Turow, the Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication.

"It is a part of life today," he says. "Phones with cameras make it very easy and alluring to share photos, and it is understandable people want to share. It is also difficult to argue that every posted photo is going to lead to a scam or be hacked."

Turow, who has authored 11 books, edited five, and written more than 150 articles on mass media industries, says the technology of hacking is continuously evolving. So, we don't know what will happen in the future in terms of how scammers will use information.

"The more photos reflect the context of a person and their relationships with others, the more that person can be denoted by their location which in turns allows hackers greater access to personal information," he says.

Turow urges participants to beware, because these kinds of posts can make users more susceptible to hackers trying to break into online accounts.

"The problem is that there are so many photos of people," he says. "There is a possibility that someone will attach a name to your photo. If you appear in a photo of friends who also have been tagged, people with malign intent can try to trace these relationships and use them to fool people into giving up information. It is amazing how much stuff is out there about everyone, and what people share about themselves, often

without being aware they're doing it."

When sharing these photos, users posted them with the hashtag #ClassOf020. Scammers can quickly scan sites for this hashtag and possibly find the name of your high school and your graduation year.

These are the two most common online security questions, and if your social media account isn't protected, scammers can find out a lot more about you, according to Turow. Also, a high school graduate year also implies a person's age and, often, the age of friends in the photos.

"Hackers looking to break into your private accounts could use any piece of information you share in a viral challenge," Turow says. Year of graduation, cities in which you've lived and the makes and models of all the cars you've owned are examples; those cars, cities, and graduation years may show up in photos you share. (Often photos contain side information about date and location.) This can be used to infer other revealing details, such as your date of birth and the city you grew up in—also popular security questions to bank accounts and retirement funds.

"Criminals can try to use this information to get more information from you that will then allow them to target you for money out of some online accounts," Turow says. "Hackers are continuously looking for ways to get into people's files to find out ways to get into their monetary accounts and take on some aspects of one's identity in some type of way."

In addition, he says people "use these details to hack social media accounts, guess security questions on financial sites, and send customized 'spear phishing' messages designed to fool you into forking over sensitive information."

The Better Business Bureau (BBB) cited similar concerns about other recent trends involving personal information on social media, including posting about the make and model years of all vehicles you've ever owned, your favorite athletes, and your favorite shows.

"I think the BBB is right," Turow says. "The problem is some people make it very easy to find out what their passwords are. People tend to use the same password over and over again, which makes it easy to steal. The consequence is that if it is stolen, it can be used to get into every aspect of your life."

The trick, he says, is to minimize the overlap of passwords and be very careful. He also says people should never click on a link in an email unless they are sure who sent it, a common way for scammers to infiltrate your computer.

"The information is legally being traded by advertisers, marketing agencies, and data brokers," Turow says. "How many people actually read the privacy policy? And how many people actually understand the wording? It is purposely long and written to confuse the consumer."

If a person does plan to participate in these ongoing trends, because another one will soon come along and users may not be able to resist the temptation to play along, Turow says to take extra precautions.

He advises people to think twice before participating in these types of trends.

"While it may seem like the information is being shared with only your friends and family, it can also be shared with hackers and scammers who troll the social media sites," he says. "Once your data is in the wild, it stays in the wild and can be used by any number of unscrupulous characters."

Before you share too much, Turow suggests tightening up security settings and regularly changing the security questions you use to access online banking and other services.

Turow's final advice: Stop and wait before you share anything and think about it; realize that when you put anything in an email, or social media, you are posting something that has the potential to become public; and act as if nothing on the internet is private.

Provided by University of Pennsylvania