Headline: Teaching online privacy.

Subhead: *Is there a need for expanded education about online privacy?*

Most of us post pictures and personal information online and freely enter our phone number or email address when shopping. When you download and use an app or a website you also give away a lot of personal information about yourself. Your location, shopping preferences, and pictures can no longer be considered private. The benefit of getting a discount off your purchase may be tempting, but do you know what happens to your personal information? Perhaps we need better education on how to deal with our personal information online.

Teaching online safety is part of the curriculum in schools, starting in elementary school. Some teachers post pictures on Facebook with the request to share so their students can see how far a picture can spread around the world. As a teacher, I wonder if this is enough? And how could adults become better educated about their online safety? Over the past three months, I spoke with twelve respondents in order to find out what they know about their online privacy. My goal was to find out whether smartphone users are aware of how their personal information is collected, managed, and potentially used when downloading and using an app on their phone. I also wanted to see if users in the United States (US) and in the European Union (EU) perceive their online privacy differently. Six respondents were from Norway and six from the United States, all of different ages and occupations. Norway is not considered a full member of the European Union. However, it is associated with the EU through its membership of the European Economic Area (EEA), established in 1994. Because of this connection, my respondents in Norway are representative for online users in the EU.

Smartphones and their security issues have been well studied (Ameen et al.; Goth; Gutierrez et al.; Tao et al.), but the literature on security awareness and how smartphone users behave is more limited. A survey from NortonLifeLock showed that 79% of participants said they believe consumers have lost control over how their personal information is collected and used (Whitney, 2020). Almost 75% believe it is impossible to protect their online privacy, and 60% feel it is too late to protect their personal information because it is already out there (Whitney, 2020). Breitinger and Nickel (2010) found that people had low security levels on their phones, and this was mainly due to the lack of security awareness. The study focused on participants who self-identified as more tech-savvy than the general public and found that the respondents had a high degree of security awareness when it came to their smartphones, but the findings also suggested that most users were "not concerned about the privacy and protection of their personal data, with some believing that they did not have anything worth taking" (Breitinger et al., 2019, p. 2). For many of the respondents in my study, their concern over their online safety was diminished because they felt their information would not be of value to anyone else, which coincides with the findings in the NortonLifeLock survey. Respondent 1 (Male, 20, United States), said this about how he thinks about his personal information online: "[A]s I've gotten older, I've realized: So, what? What are they going to do with it? They probably don't care about some random citizen that doesn't have much power, I can't really do anything to them. The worst that could happen is they get my credit card information. And should that happen, I just call the bank and freeze my account. So, there's lots of backdoors. So ultimately, I'm not too scared or worried about what happens if my information gets out. Because no one really cares."

Users have to accept privacy policies before they can create online profiles or download new apps, but researchers found that only 35% of users look at required permissions before

installing an app (Breitlinger et al., 2019). To use an installed app, a user has to accept the end-user license agreement (EULA) document, which informs users about the app's activities. Accepting this does not mean the user has read and understood the terms, however, and people often rely on user reviews and popularity to tell them about the quality and security of an app (Koyuncu & Pusatli, 2019). Eight of the twelve respondents said they sometimes check the privacy settings for the applications they have on their phone. Only four claimed to always check those. Respondent 10 (female, 48, United States) said she found it difficult to remember to check all the privacy settings on her applications. "I couldn't tell you right now which ones I've done that on and which ones I haven't. But over time, every time somebody reminds me, oh, did you know that this is how you go and, you know, change your privacy settings all I'll say, Oh, I should do that".

When users connect their devices to the Internet, whether a mobile phone or a computer, it can pose a challenge to their privacy. Most of the respondents in my study said they had some knowledge of how their information is used online and what the risks are, but the extent of how their information may be sold and used was limited. Respondent 8 (female, 33, Norway) said "I have a vacuum cleaner, and it creeps me out. When we tried to connect that to the Wi-Fi in the house, we had to download an app on our phone, and then you have to accept everything for it to be able to connect to the Wi-Fi. I mean, there's no way to hook it up without having to accept everything. So, that has access to everything. And, you know, it takes pictures and runs on GPS. And, you know, how Scandinavian or European people live? China knows that now. And just the fact that the app is Chinese is kind of scary".

Most respondents found it difficult to keep track of what types of information the different apps have about them. They said they knew how to change the settings on their phones in order to

restrict the app's access to their phone and their information, but either weighed the benefits of using the app as more beneficial than the downside of giving out their personal information, or they simply found the process of constantly checking the privacy settings too much to keep up with.

There are ways consumers can protect themselves from giving away their personal information, but to avoid it completely may be impossible. About half of the respondents were concerned about their personal information being breached online. The highest was among the age group of 26-40, where three of the four respondents said they were concerned. Respondent 4 (male, 32, United States) said he was scared about what information was out there about him. He said he checks some of the privacy settings for his apps, but found it confusing to be sure that his information was safe. "Privacy on each app is different. It says what it will give out and what it will not give out of information. So, you never know".

Whether the difference in the perception of the safety of their online information is due to geographic location or age, is hard to say from my findings. It seems that the level of safety awareness depends on their level of online experience. One thing that showed in my findings was that most of the people who claimed concern or were somewhat concerned were female. Four of the six females interviewed noted they were worried about their online information being breached. Of the males, only one of the American respondents was concerned, the rest of the males were not particularly worried.

Laws are changing, for instance with the implementation of The General Data Protection Regulation (GDPR) in Europe and the Consumer Privacy Act (CCPA) in California. As much as this will restrict the personal information a company can access and use, the need for better training in online privacy is necessary. Online privacy and security awareness is a subjective

matter and involves personal choices, which makes it difficult to generalize. However, in order to make responsible choices, awareness and education is vital. Based on my findings, the age group that was the most concerned about their online safety were adults over the age of 26. Since digital privacy and security awareness are taught to the younger generation, perhaps we need to make an effort to create a curriculum for teaching adults how to keep their information safe online. Respondent 7 (Male, 38, Norway) said "[a]wareness is really important. But I think no matter how many campaigns you have about awareness, the fact that it's being taught in school is probably really good. We teach about tracking information online and who gets that information. So digital competency is very important. Knowledge about what your information can be used for."

References

Breitinger, F., & Nickel, C. (2010). User Survey on Phone Security and Usage. BIOSIG.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2019). A survey on smartphone user's security choices, awareness and education. *Computers and Security, 88*. doi:10.1016/j.cose.2019.101647

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, 1.

Whitney, L. (2020, April 2). *Most consumers worry about online privacy but many are unsure how to protect it.* TechRepublic. https://www.techrepublic.com/article/most-consumers-worry-about-online-privacy-but-many-are-unsure-how-to-protect-it/