A teaching moment in the Ashley Madison hack

31 August 2015, by Peter Krapp

Why did people make their personal information so easily available to a company that facilitates cheating? Credit: Johan Viirok, CC BY

Why would anyone use their official work or school email address to register for a website that promises to facilitate extramarital affairs?

Reports indicate that there are 74,468 unique ".edu" email addresses in the recently hacked user database of AshleyMadison.com. Might we not expect educators and students to have a better understanding of the internet (which, after all, began with a link from UCLA to the Stanford Research Institute)?

I am not only a proud user of a .edu email address, but as a professor at the University of California, I research media culture. It might make us laugh that people would entrust their information to a company that facilitates cheating, in the naive assumption that it would not cheat on its users. But in the information age, using your home address, credit card information and work-related email address to sign up for a service that promises illicit connections is so careless that it constitutes a teaching moment.

The blame or shame game

When the AshleyMadison.com user database (with names, addresses, phone numbers and credit card information) was hacked and then distributed through file-sharing services, the hackers claiming responsibility for taking the data and releasing them stated they did so to criticize not only the lack of security, but also the lack of credibility of a website that promised discretion but profited from hefty but deceptive profile-deletion fees.

In 2014 alone, the company netted US$1.7 million in fees for a "full delete" of user profiles (at $19 each). Several users anonymously confirmed that their payment information, address and other identifying data were in the files, despite assurances from AshleyMadison.com that they had been deleted or not kept in the first place.

Some observers have gleefully outed AshleyMadison.com users who are conservative defenders of family values, while others worry about adverse consequences for people suspected of adultery or homosexuality in places where that is unlawful.

Jokes about divorce lawyers are bandied about, and warnings against wholesale public shaming are made. Brian Krebs, the investigative journalist who first broke the story on July 15 that AshleyMadison.com had been hacked, has warned that it might lead to blackmail.

Since about 15,000 addresses in the database are .mil or .gov (among them 6,788 in the US Army, 1,665 in the US Navy, 809 US Marines and 127 in the US Air Force), it is not surprising that the Department of Defense is combing through to see whether it needs to fend off blackmail. Surely some government employees are facing discipline.

Meanwhile, the Guardian suggested worrying about possible extortion of bankers, and Inside Higher Ed ran a column revealing that there are numerous .edu email addresses in the leaked database.

Address verification

Claims that AshleyMadison.com did not validate emails on sign-up led to speculation that just because someone is listed does not mean they actually were users of the site – someone else could have used their name and email address.

However, the database lists a field for valid/invalid email address checks, and while among the registered users there are 12,358,191 whose email field reads "isvalid = 0," there are also 24,039,705 email addresses marked as "isvalid = 1."

Therefore, millions of people will not be able to use as their excuse that someone else might have used their name and email to sign up. While The Hill has pointed out that some email addresses that might look like government ones are clearly fake, others are not: "several emails were registered at whitehouse.gov, whereas White House officials use eop.gov for email communications."

It is possible that many people merely signed in with their email address out of curiosity and never went much further – but for those there would be no payment information, phone numbers and addresses on file. Yet the database shows that more than 173 million credit cards had been used to pay for the site's services in 2014.

A teaching moment

Inside Higher Ed shows a table with the top 10 most represented institutions, led by Michigan State, Penn State and Kent State. Students and alumni are likely to have other primary email addresses, and a majority of students are probably not yet married and looking for an extramarital affair on AshleyMadison.com.

It is safe to assume that a significant proportion of those .edu email users Inside Higher Ed found in the AshleyMadison.com database are those of current or former college or university employees.

If they chose to use their .edu addresses instead of alternatives, what does that show about their awareness of privacy online, about their critical evaluation of information technology?

I won't argue that people in higher education should conduct their lives according a higher ethical or moral standard than those in the military or in government service, although some educators might want to set an example for values they profess.

But I do think people in higher education do have a greater obligation to value the integrity and security of data. Of course, colleges and universities deal in information, but precisely not for shameless commerce – they deal in information for the greater good of the communities they serve.

Academia depends on verifiable information, and one of the fundamental values of academia is that we share important insights. One of those is that privacy is under siege online, and we need to do better with our passwords, with our social technologies, with our control over personal information.

Education, putting our hard-earned knowledge to use, must act as the opposite of the shameless commerce of AshleyMadison.com and its ilk – reconstituting in the individual affect the public virtue for which it substitutes.

Czech writer Milan Kundera urged:

When it becomes the custom and the rule to divulge another person's private life, we are entering a time when the highest stake is the survival or the disappearance of the individual.

But he was writing about surveillance-riddled totalitarian Czechoslovakia in 1975, not about the United States in 2015.

Source: The Conversation