PHYS ORG

Data privacy research front and center at human computer interaction event

May 1 2019, by Laurel Thomas

Credit: CC0 Public Domain

Shortcomings of security breach notifications, best practices for phishing warnings and lessons learned from the use of analytics to improve student performance are among several studies University of

Michigan researchers will present beginning this weekend in the United Kingdom.

Florian Schaub, assistant professor at the U-M School of Information, and colleagues will share their work May 4-9 at the CHI Conference on Human Factors in Computing in Glasgow, Scotland.

Data Breaches

Building on their previous research that showed consumers often take little action when faced with security breaches, the School of Information team led by doctoral student Yixin Zou and Schaub analyzed data breach notifications companies sent to consumers to see if the communications might be responsible for some of the inaction.

They found that 97% of the 161 sampled notifications were difficult or fairly difficult to read based on readability metrics, and that the language used in them may have contributed to confusion about whether the recipient of the communication was at risk and should take action.

"Our analysis shows that requiring companies by law to send data breach notifications alone is not sufficient," Zou said. "It is important to ensure that important information such as what happened and what consumers should do to protect themselves is communicated in those notifications in a way that is understandable and actionable by consumers."

Citing statistics from the Privacy Rights Clearinghouse, the authors note that in 2017 there were 853 data breached that compromised 2.05 billion records, which included consumer names, contact information account numbers, credit card details, social security numbers, shopping and purchasing records, social media posts and messages, and health records.

In response, most countries, including the United States, adopted data breach notification laws. In the U.S., each state has its own data breach law, therefore, the threshold for when consumers must be notified, how soon after a breach, and what that notification must look like vary across states.

This allows much freedom for companies to use hedge terms that downplay risk—using phrases like "you might be affected" and "you are likely to be affected" in 70% of notifications and saying "at this time, we have no evidence of exposed data being misused" 40% of the time.

It also allows a lack of consistency in addressing the cause of the breach, the date of occurrence and the amount of exposure time, the researchers say.

"There's little incentive for companies to invest in making data breach notifications more usable," Schaub said. "For most companies, those notifications are only seen as a requirement for complying with data breach notification laws rather than a way to educate and protect their customers. We need to rethink and rework consumer protection laws such as these to ensure that companies' notifications are actually helpful to consumers."

Most state laws require companies to notify affected consumers in written letters or by telephone. Emails, website announcements, notices to statewide media or other electronic methods are usually substitutes. The study shows a consistent pattern with 95% of the analyzed notifications delivered by mail. The researchers say the slow speed of a mailed letter might increase the time when consumers stayed uninformed of the breach.

Phishing

Just when we think we have a handle on the tricks data thieves have up their sleeves to hack our devices in an attempt to steal our information, someone comes along with a new way to fool us, and phishing schemes on the computer can catch even the savviest of users.

Organizations that provide email services, including the commercial email clients that consumers use every day, have put numerous measures in place to fight phishing attempts,and work to educate users about avoiding suspicious links in email. Among the efforts are various warnings that alert users of potentially suspicious links.

In a study involving 700 participants ages 20 to 71, Schaub and colleagues at the School of Information evaluated three warning design features to help users more effectively assess phishing risk and avoid suspicious websites. They compared them to the more commonly used static email banner—often a colored band or box using a bold color like red that appears as a warning across the top of an email page. The three features for comparison are:

- Warning placement, or moving phishing warnings close to the suspicious link in the email.
- Forced attention to the warning by deactivating the suspicious link in the email body and forcing the user to click the unmasked URL to proceed.
- Warning activation, which calls for the warning to show up only when the user hovers over a link.

They found that when compared with banner warnings, link-focused phishing warnings reduced the chance of participants clicking through to a phishing link. Forced attention warnings were the most effective.

"Detecting phishing emails is difficult for people and the common advice to 'check the link before you click' is good but not really supported by email clients," Schaub said. "Our research shows that welldesigned phishing warnings can help consumers better detect phishing links by clearly identifying which links in an email are suspicious, prominently showing the suspicious link's destination, and forcing users to click on the warning if they want to still continue to the link's destination.

Learning Analytics

Over the last half-dozen years or so, universities have been gathering data about student performance in select courses in order to create warning dashboards to help those who are underperforming. The goal of this tailored, personalized approach to education is to intervene at key points in a semester to help them improve so they can succeed.

For the most part these dashboard interventions have shown positive results in improving student outcomes.

But a study by Schaub and a School of Information team of a learning analytics application reveals that students haven't always known about or understood how their data has been gathered and used. The researchers find that students want more input into that process and a say over what happens with their data.

The U-M program known as Student Explorer started as a way to help encourage STEM students to stick with courses in science, technology, engineering and math, as many were becoming discouraged and giving up early on careers in those fields. It proved successful and later was adopted by multiple programs across campus.

For their study, the researchers conducted interviews with four program developers, eight academic advisers, and 20 students. The research concluded that all stakeholders—students, faculty, academic advisers—should collaborate on these programs and be part of their creation and evolution.

"It's really important to discover these various user needs and usage habits to make sure the system design and function can address them," said Kaiwen Sun, doctoral student and lead author of the paper.

"Many advisers and instructors are unfamiliar with the concept of learning analytics. They see new platforms roll out and think they are just the users. They might not consider themselves able to play a key role in the learning analytics process.

"I also think it's important to educate people and promote awareness around campus about the goal, benefits and impact of learning analytics, why these different stakeholders should care, and what they can do to contribute to the learning analytics process."

More information: Yixin Zou et al. You 'Might' Be Affected, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems—CHI '19* (2019). DOI: 10.1145/3290605.3300424

Kaiwen Sun et al. It's My Data! Tensions Among Stakeholders of a Learning Analytics Dashboard, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems—CHI '19* (2019). DOI: 10.1145/3290605.3300824

Justin Petelka et al. Put Your Warning Where Your Link Is, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems—CHI '19* (2019). DOI: 10.1145/3290605.3300748

Provided by University of Michigan

Citation: Data privacy research front and center at human computer interaction event (2019, May 1) retrieved 11 May 2024 from https://phys.org/news/2019-05-privacy-front-center-human-interaction.html