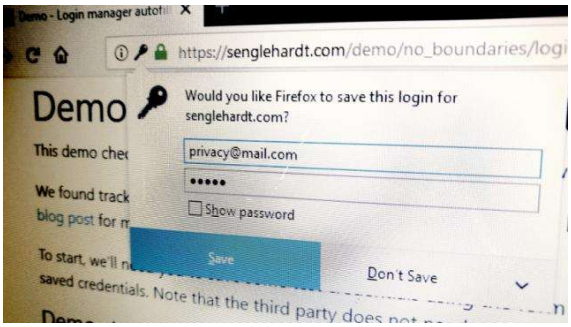
Web Trackers Lift Email Addresses Via Browser's Autofill Feature

BY MICHAEL KAN 28 DEC 2017, 3:48 P.M.

Two marketing firms appear to be behind the web tracking, which occurred over 1,100 websites, according to Princeton researchers.



Researchers have uncovered a disturbing way marketing firms can secretly learn your email address. It involves abusing your browser's built-in login manager.

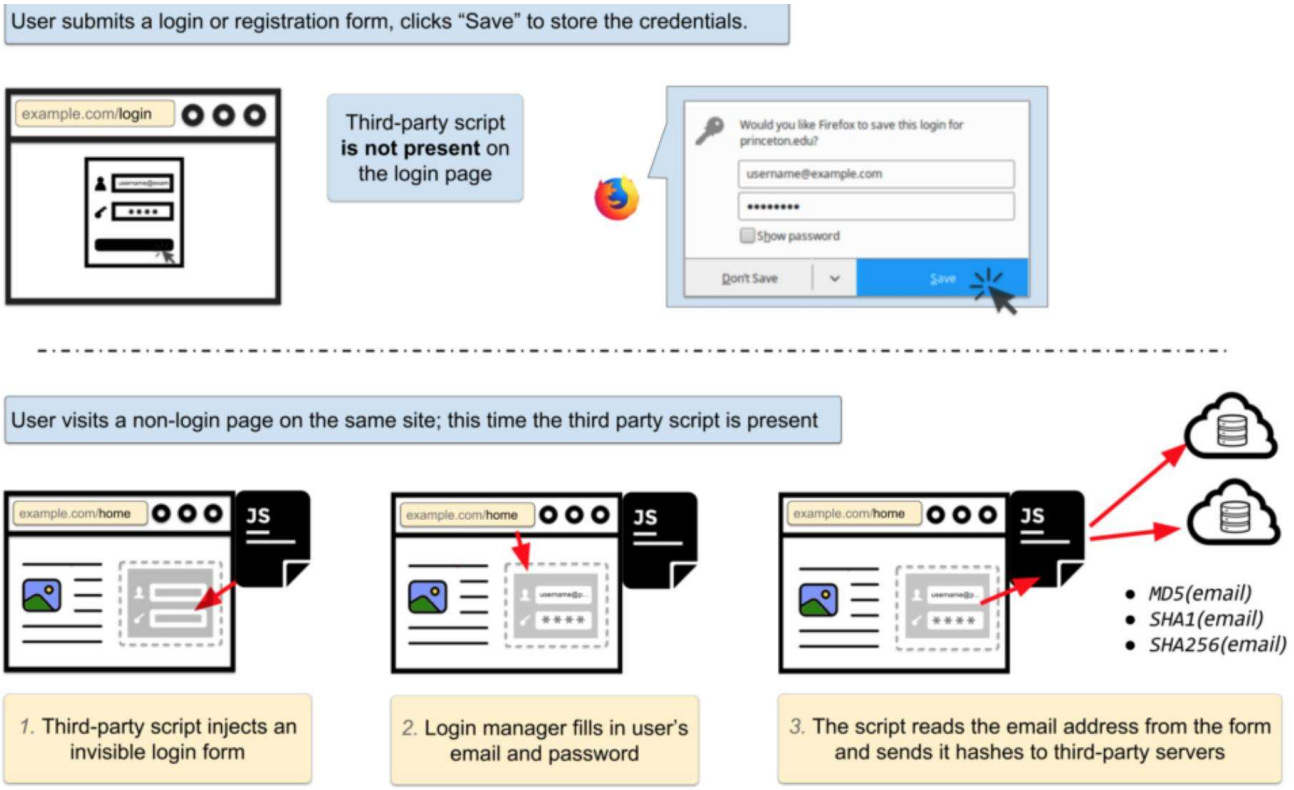
Popular internet browsers including Chrome, Edge, Firefox, and Safari all have a feature to save and autofill your email address and password whenever you log into a site.

But what happens when that same feature autofills your login credentials into an invisible form secretly running on the page?

On Wednesday, researchers at Princeton University claimed two marketing firms have been resorting to this very tactic to lift email addresses from unsuspecting internet users. It's been occurring over 1,100 sites through embedded tracking scripts.

The tactic works on major internet browsers for any sites you've chosen to save the login credentials for. As you navigate through the website, the tracking script can kick in, generating an invisible form to trigger the credential theft. (You can test the attack yourself by visiting this demo page the researchers have created.)

Tricking a browser's autofill function isn't a new flaw; it's a hacking risk security experts have warned about for years. But this appears to be the first time researchers have spotted the vulnerability being used for web tracking purposes.



The good news is that the tracking scripts weren't lifting password data, but focused on creating hashes —or digital signatures— of email addresses. The two marketing firms that appear to be behind the tactic are Adthink and OnAudience, which are both based in Europe.

It isn't clear what the data was being used for, but email addresses can be valuable to marketing firms.

"Hashed email addresses are quite persistent identifiers and allow these companies to better track users even if they clear cookies or switch devices," said Gunes Acar, one of the Princeton researchers, in an email.

An email address will also be tied to a whole trail of digital footprints whenever its used for website or internet service sign ups. All that information can be gold for marketing firms in their attempts to home in on potential customers.

For instance, snippets of code from the web trackers suggest that Adthink was interested in collecting users' demographic information including their gender, their nationality, whether they owned pets, and the make of their car.

```
birth date, age, gender, nationality, height, weight, BMI (body mass index), hair_color (black, brown, blond, auburn, chestnut, red, gray, white), eye_color (amber, blue, brown, grey, green), education, occupation, net_income, raw_income, relationship states, seek_for_gender (m, f, transman, transwoman, couple), pets, location (postcode, town, state, country), loan (type, amount, duration, overindebted), insurance (car, motorbike, home, pet, health, life), card_risk (chargeback, fraud_attempt), has_car(make, model, type, registration, model year, fuel type), tobacco, alcohol, travel (from, to, departure, return), car_hire_driver_age, hotel_stars
```

The categories mentioned in the Adthink script include detailed personal, financial, physical traits, as well as intents, interests and demographics (**Link to the code snippet**).

claims: "We do not collect any personal information. We do not know who you are. We do not know your residential address, your email address, your phone number or any other personally identifiable information about you."

Despite that statement, it's often unclear what the marketing firms are exactly up to, according to Acar.

"This is one of the problems with online tracking: it's an opaque process, especially once the data is collected from the users' computer," he said. "It's hard to be certain about the exact use of the data without looking into server side processing and data transfers."

On the plus side, the 1,100 sites found lifting the email addresses weren't major online destinations. Instead, many appear to be lesser-known European websites, and probably partook in the web tracking to earn money without realizing the consequences.

"In my experience, (the website) publishers are by-and-large unaware of the privacy-invasive behavior of the third-party scripts that they add to their sites," said Arvind Narayanan, a Princeton assistant professor who was involved in the research.

"When the privacy violations are pointed out, publishers typically end up removing the third-party scripts in question from their sites," he said in an email.

According to their report, the Princeton researchers also recommend that browser makers stay on guard against "stealthy" attempts to exploit their software's autofill function. A simple way to prevent the vulnerability is to disable the autofill function.

"A less crude defense is to require user interaction before autofilling login forms," the researchers added. Nevertheless, some solutions might come at the cost of user convenience, they said.

So far, the companies behind the major internet browsers, including Google, Microsoft and Mozilla, are still looking at the findings. In the meantime, the researchers say installing an ad blocker can prevent invasive web tracking scripts from monitoring your activity. Both scripts from Adthink and OnAudience are blocked by the EasyPrivacy filter for Adblock.

NEXT ARTICLE

MORE INSIDE PCMAG.COM

Tesla Motors announces Australian charging stations by 2016

Australian summer breaks the internet

MCA app wants to know what you think about art

Perfect Aussie indie games to play these holidays

BY MICHAEL KAN

MICHAEL_KAN@PCMAG.COM

Michael has been a PCMag reporter since October 2017. He previously covered tech news in China from 2010 to 2015, before moving to San Francisco to write about cybersecurity. **MORE »**

MORE STORIES BY MICHAEL KAN

Prank in Call of Duty Feud May Have Killed Bystander

The "swatting" prank deceived local police into thinking a hostage situation was taking place at ... **MORE »**