The Washington Post

Get There

What to do if you are affected by the OPM data breach

By Michelle Singletary
December 11, 2015

Following massive hacks at the Office of Personnel Management, some people are meeting an offer of assistance from the government with skepticism.

In one hack discovered by OPM in April, personal information — birth dates, home addresses and Social Security numbers — for 4.2 million current and former federal government employees was compromised.

A second breach uncovered in June involved an astounding 21.5 million individuals. Social Security numbers were stolen from background investigation records, including nearly 2 million mostly involving spouses and others connected to applicants. Also included were 5.6 million records that contained fingerprints.

To help potential victims, OPM is offering credit and identity monitoring, identity-theft insurance and identity-restoration services for three years through ID Experts, a private company.

People whose information was stolen in the background-investigation breach are receiving letters offering the free services. (The agency has reached out to folks affected by the earlier hacking incident.) Once they get the letter with a PIN code, they can either call or enroll online.

“How can you tell if it’s real or not?” one reader wrote me about the letter she received.

Another worried reader wrote: “I got a letter in the mail with a 25-digit pin number encouraging me to sign up. . . . The letter heading gives ‘Washington, D.C. 20415’ as their location. I called. It is a computer permitting you to enter your PIN number. It did not sound like a government response at all, and the letter content sounds strange. This is definitely a scam. Why doesn’t the government go after them for mail fraud?”

The reader also thought the return address was bogus. But I compared the letter he received with a sample on a special site set up by OPM. His letter, as it turned out, wasn’t a fake.

People have reason to be nervous and suspicious. The Federal Trade Commission issued a warning this summer to government employees, contractors and others affected by the hacks. It cautioned about imposters pretending to be from the FTC offering compensation to victims of data breaches.

Here’s what you should do if you’re affected:

● Start your own investigation. The letters from OPM direct people to www.opm.gov/cybersecurity. Identity thieves may create spoof sites so similar that a slight typo could put you in harm’s way. If you want to make sure you don’t type in the wrong URL and get misdirected, go to OPM’s site and click the link for the “Cybersecurity Resource Center.”

It’s important that you keep in mind that the URL listed in your letter is the *only* official place for information about the hacks, OPM press secretary Sam Schumach said. If you get a letter with any other reference, it’s definitely fraudulent, he said.

Schumach said the mailings involving the background checks should be completed soon.

● Compare your letter to the samples. On opm.gov/cybersecurity, scroll down about halfway and look for the section that says "Sample Notification Letters." There are two examples, one for if records show that your fingerprints were not compromised and one for if they were.

Schumach said the return address the skeptical reader was concerned about is legitimate as well. Mail is sent and received at a location where it can be screened, which is why it doesn't carry OPM's address in downtown Washington, he said.

You'll need to stay vigilant for years about fake letters, emails or phone calls about the hack. "Please note that OPM and ID Experts will not contact you to confirm your personal information," the agency's letters say. Never give out personal information if you haven't initiated the call or contact.

● Verify whether you've been affected by the breach. OPM said if you underwent a federal background investigation in 2000 or later, it is likely that you are affected by the background investigation thefts. But it's still possible that people who went through checks before 2000 could have had their personal information compromised.

A verification center has been set up to help people who have lost their PIN codes or think they may be affected but have not received a notification letter. If you get a letter after contacting the center, it will be similar to the sample letters.

● Check OPM's cybersecurity site often. You can sign up to get email updates or create your own calendar reminder to prompt yourself to check for new developments or warnings.

I'm glad people are double-checking information they are receiving. Cynicism in this case is a good thing.

Write Singletary at michelle.singletary@washpost.com. To read more, go to http://wapo.st/michelle-singletary.

163 Comments

Michelle Singletary

Michelle Singletary writes the nationally syndicated personal finance column The Color of Money. Her award-winning column is syndicated by The Washington Post Writers Group and is carried in dozens of newspapers nationwide. Follow