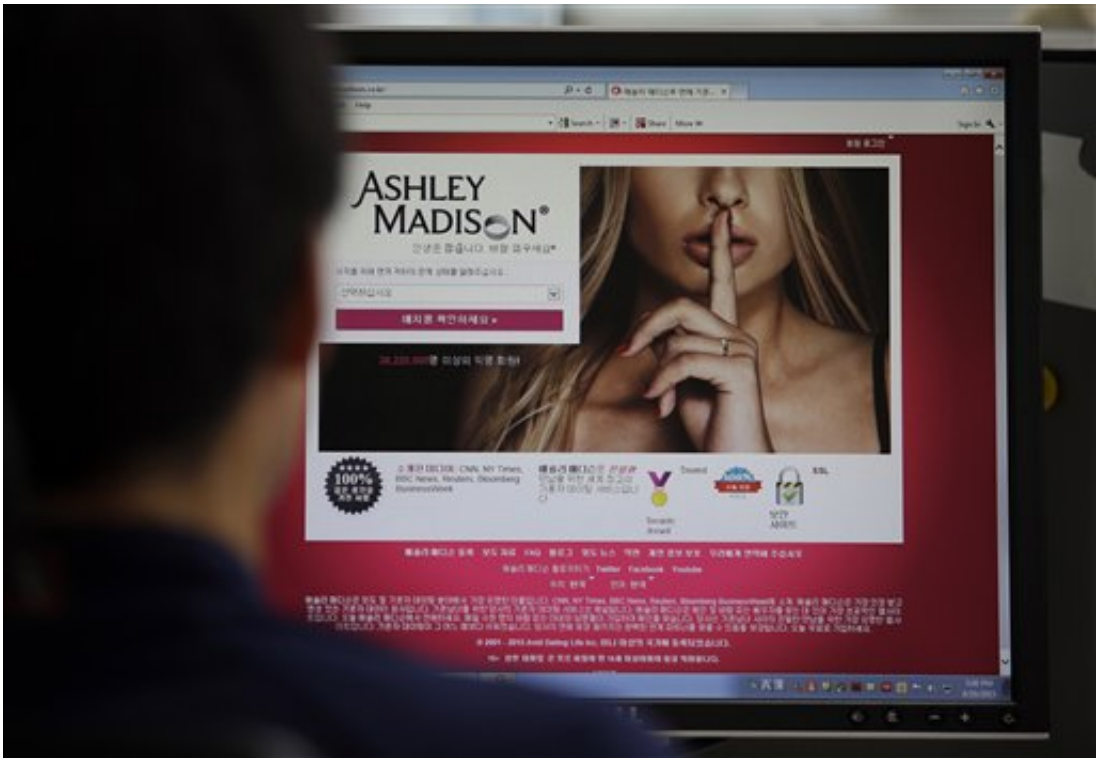
Federal workers with sensitive jobs used cheating website

August 21 2015, byJack Gillum And Ted Bridis



A June 10, 2015 photo from files showing Ashley Madison's Korean web site on a computer screen in Seoul, South Korea. Hackers claim to have leaked a massive database of users from Ashley Madison, a matchmaking website for cheating spouses. In a statement released Tuesday, Aug. 18, 2015, a group calling itself Impact Team said the site's owners had not bowed to their demands. "Now everyone gets to see their data," the statement said. (AP Photo/Lee Jin-man, File)

U.S. government employees with sensitive jobs in national security or law enforcement were among hundreds of federal workers found to be using government networks to access and pay membership fees to the cheating website Ashley Madison, The Associated Press has learned.

The list includes at least two assistant U.S. attorneys, an information technology administrator in the White House's support staff, a Justice Department investigator, a division chief, and a government hacker and counterterrorism employee at the Homeland Security Department. Others visited from networks operated by the Pentagon.

Federal policies vary by agency as to whether employees could visit websites during work hours like Ashley Madison, which could be considered akin to a dating website. But such use raises questions about what personal business is acceptable—and what websites are OK to visit—for U.S. workers on taxpayer time, especially those with sensitive jobs who could face blackmail.

Hackers this week released detailed records on millions of people registered with the website one month after the break-in at Ashley Madison's parent company, Toronto-based Avid Life Media Inc. The website—whose slogan is, "Life is short. Have an affair"—is marketed to facilitate extramarital affairs.

Few connecting from federal networks had listed government email accounts when subscribing. But the AP was able to trace their government Internet connections, logged by the website over five years and as recently as June. They encompass more than two dozen agencies, such as the departments of State, Justice, Energy, Treasury and Transportation. Others came from House or Senate computer networks.

Records also reveal subscribers signed up using state and municipal government networks nationwide, including those run by the New York

Police Department. "If anything comes to our attention indicating improper use of an NYPD computer, we will look into it and take appropriate action," said NYPD spokesman Stephen Davis.

The AP is not identifying the government subscribers it found because they are not elected officials or accused of a crime.

Many federal customers appeared to use nongovernment email addresses with handles such as "sexlessmarriage," "soontobesingle" or "latinlovers." Some Justice Department employees also appeared to use prepaid credit cards to help preserve their anonymity but nonetheless connected to the service from their office computers.

"I was doing some things I shouldn't have been doing," a Justice Department investigator told the AP. Asked about the threat of blackmail, the investigator said if prompted he would reveal his actions to his family and employer to prevent it. "I've worked too hard all my life to be a victim of blackmail. That wouldn't happen," he said. He spoke on condition of anonymity because he was deeply embarrassed and not authorized by the government to speak to reporters using his name.

Defense Secretary Ash Carter confirmed Thursday the Pentagon was looking into the list of people who used military email addresses. Adultery can be a criminal offense under the Uniform Code of Military Justice.

"I'm aware of it," Carter said. "Of course it's an issue because conduct is very important. And we expect good conduct on the part of our people. ... The services are looking into it and as well they should be. Absolutely."

The AP's review was the first to reveal that federal workers used their

office systems to access the site, based on their Internet Protocol addresses associated with credit card transactions. It focused on searching for government employees in especially sensitive positions who could perhaps become blackmail targets.

The government hacker at the Homeland Security Department, who did not respond to phone or email messages, included photographs of his wife and infant son on his Facebook page. One assistant U.S. attorney declined through a spokesman to speak to the AP, and another did not return phone or email messages.

A White House spokesman said Thursday he could not immediately comment on the matter. The IT administrator in the White House did not return email messages.

While rules can vary by agency, Homeland Security rules, for instance, say devices should be used for only for official purposes. It also prescribes "limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services." Employees are barred from using government computers to access "inappropriate sites" including those that are "obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable."

The hackers who took credit for the break-in had accused the website's owners of deceit and incompetence, and said the company refused to bow to their demands to close the site. Avid Life released a statement calling the hackers criminals. It added that law enforcement in both the U.S. and Canada is investigating and declined comment beyond its statement Tuesday that it was investigating the hackers' claims.