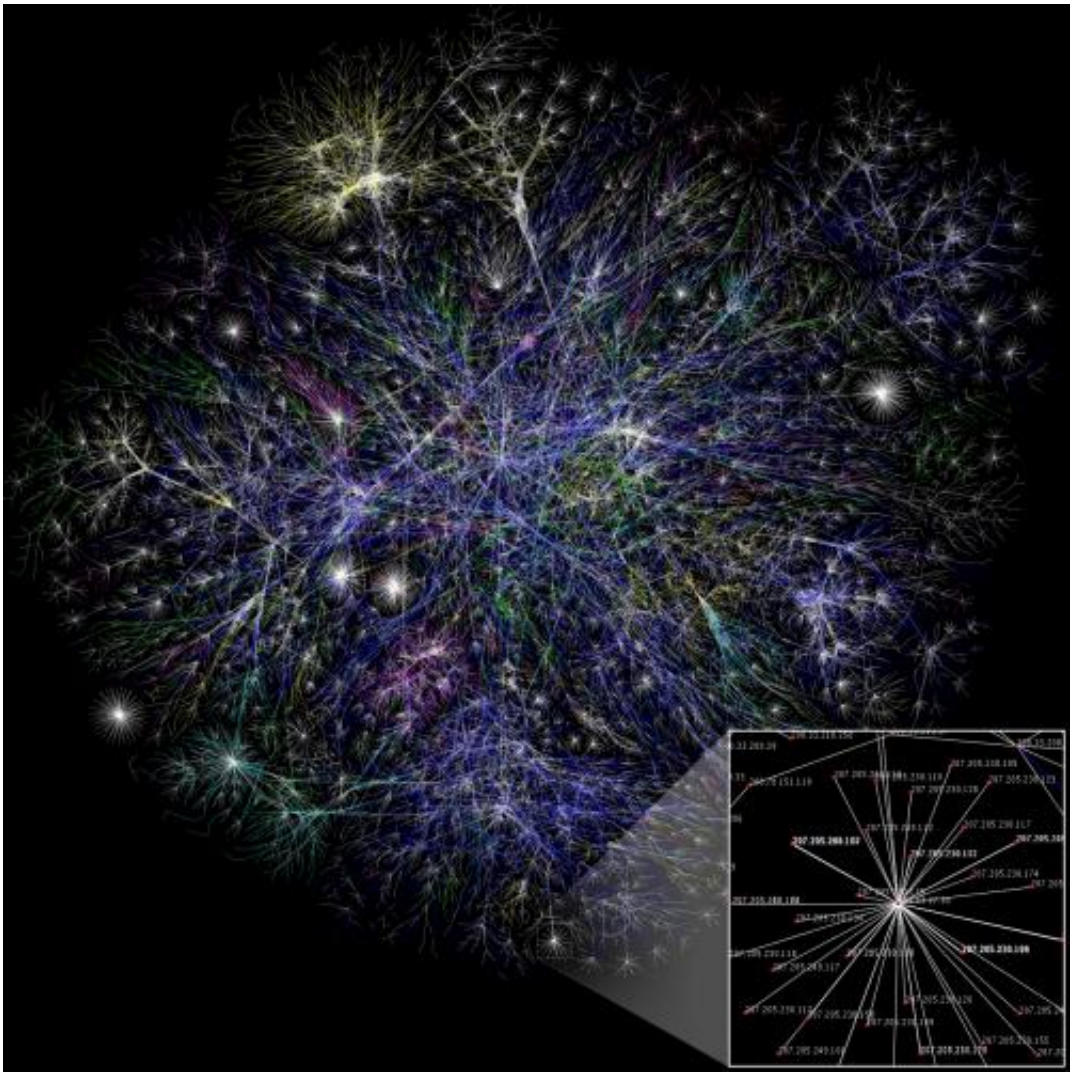
You've been hacked ... do this right now

June 5 2015, byBrandon Bailey And Joseph Pisani



Partial map of the Internet based on the January 15, 2005 data found on opte.org. Each line is drawn between two nodes, representing two IP addresses. Credit: Wikimedia Commons

The entire U.S. federal workforce may be at risk after yet another intrusion from what security experts believe were hackers based in China. The Department of Homeland Security says that data from the Office of Personnel Management—the human resources department for the federal government—and the Interior Department has been infiltrated.

It is not the first and it follows massive data breaches at health insurance companies, major U.S. banks like JPMorgan and retailers such as Target and Home Depot.

Here's what to do if you think you've been compromised.

FIRST THINGS FIRST

— Notify the credit agencies (Equifax, Experian, TransUnion) and request a 90-day credit alert. (Each reporting agency is supposed to notify the others, but you may want to contact all three yourself.) The alert tells businesses to contact you before opening any new accounts in your name. You can renew the alert every 90 days, or you're entitled to keep it in effect for seven years if you find that your identity is stolen and file a report with police.

— You might consider asking the reporting agencies to place a full freeze on your credit. This blocks any business from checking your credit to open a new account, so it's a stronger measure than a credit alert. BUT you should weigh that against the hassle of notifying credit agencies to lift the freeze—which can take a few days—every time you apply for a loan, open a new account or even sign up for utility service.

BE A DETECTIVE

— When your credit card bill comes, check closely for any irregularities.

And don't overlook small charges. Crooks are known to charge smaller amounts, usually under $10, to see if you notice. If you don't, they may charge larger amounts later.

— Get a free credit report once a year from at least one of the major reporting agencies (Equifax, Experian, TransUnion), and review it for unauthorized accounts. Ignore services that charge a fee for credit reports. You can order them without charge at www.annualcreditreport.com . If you order from each agency once a year, you could effectively check your history every four months.

DO PAID SERVICES WORK?

— Some experts say there's not much to be gained from a paid credit monitoring service. But it can't hurt to sign up for any monitoring offered for free by a company or any other entity that may have held your information when it was hacked. NOTE: These services will tell you if a new account is opened in your name, but they won't prevent it, and many don't check for things like bogus cellphone accounts, fraudulent applications for government benefits or claims for medical benefits. Some do offer limited insurance or help from a staffer trained to work with credit issuers and reporting agencies.

SOMEONE DID STEAL MY IDENTITY, WHAT DO I DO?

— Contact the credit issuer to dispute fraudulent charges and have the bogus account closed.

— Request your credit report and ask the reporting agencies to remove bogus accounts or any incorrect information from your record. See tip #1 on setting up a credit alert and/or freeze.

— Submit a report through the FTC website: www.consumer.ftc.gov.

Click the "privacy & identity" tab, which will walk you through creating an affidavit you can show to creditors.

— Keep copies of all reports and correspondence. Use certified mail to get delivery receipts, and keep notes on every phone call.

AVOID ADDITIONAL HACKS

— After a hack, scammers may try to use the stolen data to trick you into giving up more personal information. They can use that info to steal money in your accounts or open new credit cards.

— Don't click on any links from emails. Bad software could be downloaded to your computer that can steal account passwords.

— You might get letters in the mail saying you won a tablet or vacation and give you a phone number to call. Don't do it. It's likely a ploy to gather more information from you.

— Hang up the phone if you get a call asking for account numbers or other information. Scammers may also send texts, so don't click on any links from numbers you don't know.

ONE MORE RESOURCE:

The FTC now has a website www.identitytheft.gov that provides step-by-step advice and more information on what to do if you think you have been the victim of a data breach.