West Virginia Executive Branch
Privacy Tip

IDENTITY THEFT RESOURCE CENTER
888.400.5530

Be Alert: The Equifax Breach Is Just the Beginning

When news broke that the credit reporting agency Equifax had suffered a data breach, consumers around the country began to question the safety of their personal information.

After all, credit reporting agencies have access to most of your personal identifiable information (PII): name, address, birth date, Social Security number, and more. Finding out that the PII for more than 143 million US consumers had been stolen was upsetting, to say the least.

Now, consumers are being cautioned about what can happen with that information, and what steps they can take to protect themselves.

1. Beware of phishing attempts in "news" articles:
Immediately after the announcement of the data breach, articles began circulating that contained a link that lets you find out if your data was stolen. While Equifax has a dedicated web page that lets you enter your information and see if you've been exposed, it takes no work at all for scammers to create their own link, request your information for "verification" purposes, and then steal your data. Before clicking any links or entering any personal data, make sure you're using a verified link that was issued by the correct source.

2. Emailed phishing attacks have already been reported:
There are already scam emails in circulation that suggest you check your credit report by using their handy link. The easiest way to verify an email's sender is to hover your mouse over the sender's name. The actual address used will appear in a small box. To be on the safe side, don't click through from any emails you receive; if you're told to check your credit report, use a verified request service or form instead of the emailed link.

3. Be on the lookout:
Because genuine information was stolen, be extra diligent about monitoring your account statements, looking for unauthorized charges, tracking and reporting any suspicious activity, and keeping a close eye on your credit reports. Never provide your sensitive information for verification purposes; if you receive a warning or alert, contact your financial institution directly using an approved contact method.
To visit Equifax's verified link to discover if your information was stolen, click here. If you do experience any strange activity on your accounts, report it immediately, no matter how minor it might seem at first. Be sure your antivirus software is up-to-date to block any malicious threats from fraudulent emails or messages, and consider placing fraud alerts and security/credit freezes on your credit report with the three reporting agencies if your information was accessed.

© Identity Theft Resource Center 2017. All Rights Reserved. Reprinted with permission.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.