Aug 19, 2019

Contact Kylie Mason

Phone 850-245-0150

OFFICE OF THE ATTORNEY GENERAL STATE OF FLORIDA

Florida Attorney General's Office News Release

CA: Equifax Phishing Scam



TALLAHASSEE, Fla.—Attorney General Ashley Moody today issued a Consumer Alert warning Floridians about scammers attempting to steal consumer information using fake Equifax claims webpages. Fraudsters are reportedly sending phishing emails that impersonate Equifax encouraging consumers to enter personal information on a webpage that looks like the Equifax claims page. Last month, Attorney General Moody, along with 49 other attorneys general, announced an historic $600 million settlement with Equifax over failed security measures in a massive data breach that affected millions of Floridians. The agreement includes a Consumer Restitution Fund of up to $425 million, a $175 million payment to the states and injunctive relief.

Attorney General Ashley Moody said, “Online bad guys are trying to make a bad situation worse for millions of Americans whose personal information was exposed in the Equifax data breach. Scammers have set up fake claims sites and are sending phishing emails to drive consumers to their sites in an attempt to exploit victims of the Equifax data breach. This is a truly despicable scam. DO NOT FALL FOR IT. To file a claim, go directly to the Equifax claim page.”

To download the Attorney General's video message, click here.

Tips for steering clear of phishing attacks related to the Equifax data breach:

- Visit the official website to file a claim: EquifaxBreachSettlement.com;
- File your Equifax claim now on the official website. By filing now, you reduce the risk of falling for any future Equifax claims scam;

- Know that the claims process is free, so be wary of any site requiring a filing fee; and
- Remember that the claims process is underway, and the deadline to file a claim is Jan. 22, 2020. Additionally, know that the deadline to object to, comment on or to be excluded from the settlement is Nov. 19, 2019.

Phishing attacks occur when an email, text message or website is designed to look like a legitimate communication from a trusted source but is actually a scammer attempting to gain access to personal information. These messages often try to get victims to follow a link to input private information such as Social Security Numbers, banking login, birthdates, etc. Others use attachments to trick victims into unwittingly downloading a virus or malware.

Here are some general tips for avoiding phishing scams:

- Do not open emails or attachments from an unfamiliar sender;
- Hover over links in emails to see where the link leads and determine if it is a known and trusted web address;
- Study the message carefully for any spelling or grammar issues;
- Verify the legitimacy of the message with its source. Contact the institution at the web address or phone number listed on a bill or statement; and
- Notify the institution of any phishing attempts made in its name; it may wish to send an alert or warning to its customers.

Forward phishing and spam emails to the FTC at spam@uce.gov. Report scams to the Florida Attorney General's Office by calling 1(866) 9NO-SCAM or by visiting MyFloridaLegal.com.

# # #

The Florida Attorney General's Consumer Protection Division issues Consumer Alerts to inform Floridians of emerging scams, new methods used to commit fraud, increased reports of common scams, or any other deceptive practice. Consumer Alerts are designed to notify Floridians about scams and available refunds in an effort to prevent financial losses or other harm caused by deceptive practices. Anyone encountering a scam should report the incident to the Florida Attorney General's Office by calling 1(866) 9NO-SCAM or visiting MyFloridaLegal.com.