



**FOR IMMEDIATE RELEASE:**

**Contact:** James Hallinan

September 23, 2016

(505) 660-2216

## **SAFETY ADVISORY from Attorney General Hector Balderas in Response to Yahoo's Announcement that 500 Million of its User Accounts were Stolen**

*AG Balderas and the New Mexico Office of the Attorney General Internet Crimes  
Against Children Unit Issue Tips for New Mexicans to Protect Themselves and  
Their Families from Internet Threats*

*Albuquerque, NM* - Today, Attorney General Hector Balderas and the New Mexico Office of the Attorney General Internet Crimes Against Children Unit issued a Safety Advisory in response to Yahoo's announcement that 500 million of its user accounts were stolen.

"This incident is a stark reminder that all New Mexicans should be proactively protecting themselves online," said Attorney General Balderas. "While Yahoo users are most likely to be affected by this incident, anyone who maintains online accounts should take steps to protect themselves and their families from online threats."

Yahoo users in New Mexico should update their passwords and security questions, review their accounts for suspicious activity, and contact law enforcement if they believe they have been victims of identity theft or any other crime.

### **TIPS TO AVOID BEING HACKED**

**System Updates** - Hackers will attack where they perceive weakness, so it is important to always perform required software updates for your operating system and web browser.

**Firewalls** - A firewall prevents hackers from gaining access to your computer by limiting the number of ports that are open to the public.

- Always install a firewall on your computer and make sure the firewall is turned on.
- When buying a wireless router, make sure it has a built-in firewall. Having both a software and hardware firewall is more protective than just one or the other.

**Anti-Virus Software** - Purchase or download anti-virus software, and run virus scans at least once a week.

- Set up a schedule for your computer in your anti-virus software to run a scan late at night or at times when you don't use your computer.

**Passwords** – Passwords can be an open door to hackers. Change your passwords often and make sure your password isn't the same as your username or email.

- Don't re-use passwords.
- Although it is often advised to combine upper and lower case passwords with numbers to alter a memorable word, for example, "M4raD0na," these passwords are more easily cracked than one might think.
- One recommendation is to compose a memorable, unusual sentence, such as, "I am a 7-foot tall metal dinosaur," and use the first letter of each word with punctuation: "iaa7-FTmd."
- Alternatively, you can use a password manager to generate secure passwords and store them online.

**Authentication** - The best way to protect yourself is to use two-factor authentication, which will send a text with a code or use an app to verify your log-in.

**Emails** - Hackers and spammers send corrupt emails that take you to websites to steal your information and infect your computer with hidden viruses.

- DO NOT open emails from an unknown source. Delete these emails immediately.
- If you accidentally open an email from an unknown source, do not click any links contained within the email or download any files attached to the email. Instead, delete the email immediately.

There is always the possibility of being hacked even when following these steps. Hackers are clever and always devising new methods of stealing information. You might not know if you are or have been hacked. Always be aware of how your computer is running, what email communication is being sent or received, and what programs are installed on your computer.

# # #