Attention all CABQ staff,

Email Cyber Security Alert

Recently, the Multi-State Information and Sharing Analysis Center (MS-ISAC) received notifications from a trusted third party informing us that select entities across the United States had been targeted by Advanced Persistent Threat APT attack groups. Through the course of these investigations, the MS-ISAC became aware of several campaigns that leveraged highly targeted **phishing e-mails** that encouraged users to click on a link and download files that contained malware. This malware allows a remote attacker to have complete control over the victim machine and can carry out reconnaissance on the impacted users system which includes the ability to monitor activity on their web browsers, e-mail, and also the ability to run arbitrary commands on the system.

The City of Albuquerque employees have been targeted by this malicious email attack.

What to look for:
The email will have a subject line of:

Subject:
*   **"Contact info update"**

The email **message body** could have the following:

*   Photogellrey
*   Photogalaxyzone
*   aeroconf13
*   aafbonus
*   .asp?id=

Additionally, malicious phishing e-mails related to this incident can be identified by the following senders:

Sender:
*   Alice.smith158@yahoo.com <mailto:Alice.smith158@yahoo.com>
*   jon.abeln@yahoo.com <mailto:jon.abeln@yahoo.com>
*   tsmith1317@yahoo.com <mailto:tsmith1317@yahoo.com>
*   rebecca.smith363@yahoo.com <mailto:rebecca.smith363@yahoo.com>
*   mdye54@yahoo.com <mailto:mdye54@yahoo.com>

- Be cautious when opening email attachments from unknown sources.
- Never provide personal information from an unsolicited email.

As always, if you have inadvertently clicked on a suspicious link or feel your computer may have picked up a virus, contact the ITSD Service Desk at 768-2930.

For further information on preventing the spread of a computer virus or other cyber security related items visit the City of Albuquerque Cyber Security Website at http://eweb.cabq.gov/cybersecurity/default.aspx.