Memorandum

BONITA UNIFIED SCHOOL DISTRICT
Computer Information Services

TO: **BUSD Employees**

FROM: **Aaron Weathersby, Chief Technology Officer**

DATE: **February 29th, 2016**

SUBJECT: **Computer Virus Alert**

District Employees,

Recently several public sector entities have been targeted by computer hackers. These computer hackers have been attempting to install a particular type of virus called **Ransomware** onto victim computers.

These viruses encrypt the contents of the computer and attempt to extort money to have them unlocked. Most recently LACOE was hit with this virus as well as the LA County Health Department (*see article* http://www.latimes.com/local/lanow/la-me-ln-county-health-services-ransomware-20160226-story.html).

Last year several users at Bonita Unified were infected with this virus and they lost access to all of their data. Computers are usually hacked by receiving an infected attachment via email or by browsing a website who itself has been infected by a virus. Unfortunately, modern viruses do not always require clicking on a link, many can infect your computer simply by visiting a compromised website.

Given the danger that these types of viruses represent we felt it was important to let everyone know how they can keep themselves safe and what the district is doing to prevent them from taking hold here at the district.

How To Keep Yourself Safe

Please observe the following recommendations to minimize the potential of getting infected. Ultimately, information security is built around the day to day actions we all take when accessing a computer system.

- **Backup your Data:** Ransomware viruses can sometimes be impossible to defend against. Critical to recovering from an infection is ensuring you have a recent copy of your data. Keep critical data on your district H drive. This network drive is backed up every day. Many users also use portables hard drives. But always have a copy of all your important data in more than one place.
- **Don't open attachments or follow links from SPAM**: Be cautious of any links or attachments contained in an unsolicited email message. To avoid detection by antivirus, many hackers will send a link to a virus instead of an infected file. These links do not show up as a virus until it has been clicked on and it is too late.
- **Be cautious of unexpected attachments from acquaintances that you were not expecting**: Many viruses are spread by one person being infected and that person's computers emailing other users in their address book with an infected file. Always be cautious of emails that look "weird" or otherwise suspicious. Emails that contain nonsense or that contain numerous typos can be an indicator of suspicion. It is a good idea to review the from address of all emails sent to you with links or an attachment. Many hackers will "spoof" email addresses to show the name of a person you know but are actually from someone else. Don't be afraid of calling someone to confirm they sent you an email.
- **Don't give out your passwords**: Never, ever, share passwords. The security of your password is your responsibility. Don't give your passwords to your colleagues or to your students. Some hackers may call you on the phone say they are from "technical support" and ask for your password or ask that you visit

their website to install a file. Be skeptical of someone you don't recognize asking for your password. If in doubt, hang-up and call extension 8880 to speak to a district technology professional.

- **Best Practices for Opening Office (Word/Excel) Documents**
  - Do not click on the "Edit Button" unless you certain on the origin of the document.
  - Do not run or allow to run MACROs when using excel or access. (this is how LACOE was hacked)
- **Call CIS when you suspect you have a virus or are the victim of computer hacking:** Critical to being able to fix a problem is to know about it. We need your help to ensure that CIS is aware of problems in our large computer environment. Call extension 8880 if you have questions or concerns involving how to stay safe or if you think you have a virus.

What the District is Doing to Keep You Safe

The district is taking a number of steps to ensure the security of your data and the data of our students. While not an exhaustive list the bullets below are critical to our preventative information security strategy.

- **Disabled Disk Encryption:** The district has disabled the primary service that most ransomware uses to lock out a hard drive. While some encryption viruses can still operate most cannot without this service.
- **Layered Antivirus:** The district employees 4 distinct antivirus services to scan incoming email. While not perfect this helps to minimize the chances of a virus being received by email.
- **Weekly Updates:** The district attempts to keep all computers automatically up to date with the latest patches and security updates. While sometimes annoying and time consuming, we do this for your benefit. Most viruses and hacking attempts to exploit computers that are lacking a patch. These updates include the Windows Operating System, Flash, Java and other applications. If your computer asks you to install the latest patch or update you are encouraged to do so. Older Operating Systems such as Windows XP are no longer updated, the district is working hard to remove these from the environment.
- **Backups of files on the network:** The district maintains a layered approach towards backing up the data on our servers. We back up, nightly to ensure we can restore data when necessary. We encourage staff to place their critical files onto their network shared drives.
- **Limited Administrator Rights:** Viruses are only as bad as the permissions of the user they infect. CIS has an approach of providing only a limited number of user's administrator rights. This practice ensures that computers when infected do the least harm possible.

In addition to the steps we are currently doing, we will be reviewing our information security posture over the summer and making additional changes to the way wireless, network drives and computer access works to ensure the security of your data.

If you have any questions, please don't hesitate to contact me at extension 5270 or the help desk at extension 8880.

Aaron Weathersby
Chief Technology Officer
Bonita Unified School District
Phone: 909-971-8200 ext 5270
Email: weathersby@bonita.k12.ca.us