# KCSD Cyber Safety Newsletter

**DANGER**

**Action Needed, Increasing Attacks!**

Failure to take action could result in losing all files on your computer.

## What is Ransomeware?

$ ——— $ ——— $

Ransomware is malicious software which locks your screen or encrypts—or scrambles—a user's computer and/or files. It's often delivered via harmful email attachments, outdated browser plug-ins, websites, text messages, and more.

### Your Money or Your Data!

It may take over an entire network of computers, external hard drives, USB devices, and Web servers. Unlike most viruses that work to corrupt your files or system, ransomware essentially kidnaps your files—everything from confidential customer information to family photos—for an anonymous ransom payment.

### What Does Ransomeware Look Like?

Once files are encrypted, instructions appear on your computer or device, demanding a large payment in exchange for the decryption key to unlock them. The instructions may appear as a text document, a graphic on your desktop or a Web page on your browser.

### What's the Worst that Could Happen?

A recent incident with a staff laptop reinforces the dangers of Ransomware

- Ransomware encrypted multiple files stored locally on the laptop and spread to most files within days.
- Could have continued onto the KCSD servers, possibly encrypting our entire network in a matter of days.
- Only way to decrypt files is to pay a "**ransom**" or fee, ranging from ***hundreds to thousands of dollars***, otherwise hard drive is wiped clean and ***all files lost!!!***
- To further complicate the issue, the laptop was never backed up, therefore previous versions of the files could not be retrieved.

Okay, so what can I do about it?

## Follow the Email & Web Do's and Don'ts

### Do's

- Backup your files using CrashPlan . . . NOW and often!
- Contact Tech Dept if you receive mailbox quota email
- Look for misspellings & fake email addresses in emails
- On the web, look for secure sites starting with **https**
- Contact Tech Dept immediately if error message and/or pop-up appears within your web browser
  - If this occurs, hold power button to shut down laptop
- Change District password once a month if possible
- Always be on the lookout! Even emails that appear to be from friends & relatives could have been hacked

### Dont's

- Don't click on links within emails unless completely sure they're safe
- Don't Trust emails promising money or rewards, or emails with aggressive timelines like "Must respond now!"
- Don't EVER provide personal or financial information on an untrusted website, i.e. password, credit card number
- Don't Click on pop-ups and ads that appear along the side banners or embedded in a webpage
- Don't access confidential info via public Wi-Fi networks

## District Prevention Strategies

- Increased Email Spam Filtering:
  -over 130K emails filtered every 24 hours, 98% of total received
- Updated Firewall to monitor all network traffic
- Evaluating more comprehensive protection for Staff Laptops
- Support resources and more proactive communication
- Building Cyber Safety & File Backup Training Sessions
  **Schedule to follow*
- Click here more information and to stay "KennectEd"

Kennett ConnectED