YCPARMIA Safety Journal

Yolo County Public Agency Risk Management Insurance Authority

July 2012

e-Awareness

Cyber scams come in different forms, but the intent is all the same: criminals are attempting to trick you out of money or gain access to personal, confidential, or proprietary information. To protect yourself, the health of your computer, and the security of your agency's work product, keep in mind the following tips from the SANS Institute:

- Don't trust links sent in email messages: A common fraud called "phishing" involves email messages that appear to be from well known banks, delivery companies, or internet stores, and include a link to a fake website that may look like the real site. If you follow the link and confirm your account details, the defrauders will use the info to purchase goods or transfer money out of your account. Remember that no reputable organization will send a message requesting your confidential information.
- Don't trust email attachments - especially zipped files: To sneak a virus past spam and virus filters, hackers can use an encrypted ZIP folder. Other potentially dangerous attachments may look like harmless PDF or Office files. Remember that just because the spam filter didn't catch it, doesn't mean the attachment is safe. If you don't recognize the sender or were not expecting the attachment, delete it. When in doubt, ask your IT department or Help Desk.
- Free software isn't always free: When downloading free software, never click "Agree" without reading ALL the fine print. Often people click "agree" and skip over pages of legal jargon, but buried in the middle can be a sentence allowing the software to do whatever it likes. It may send your information to advertisers, make unauthorized changes your PC, prevent other programs from running, install unwanted software, contain viruses or spyware intended to damage your PC or steal confidential information...and you technically agreed to it in the End User License Agreement. If the conditions in the EULA are difficult to understand, it is probably deliberate; don't risk using the software.
- Read ALL error messages: When you see an error message pop up on the screen, read it! You may not understand everything, but if you look through the message, you can get the general idea. Hackers can generate errors to collect your keystrokes and everything that comes up on your screen. If you don't understand the error, ask tech support.
- An email might say it's from a friend, BUT: Your friend's computer may have been infected or their email account may have been comprised, allowing malware to send unsafe emails to their contact list. If you get a suspicious email from a trusted friend or co-worker, especially one without a personalized greeting or note, don't open the attachment or click the link. Either call them to confirm they sent it or delete it.
- Change your passwords to passphrases: Whenever possible, try using a passphrase like "I love getting to work at 8:00!" It's long, easy to remember, and has a mix of upper case and lower case letters and symbols. Avoid familiar or famous quotes, and never use real names, especially your own, your family member's, or your pet's. Nonsensical passphrases are the hardest to crack. Since password cracking time increases exponentially, a criminal with substantial resources can crack short passwords quickly; while a 31-character (the length of this example) would take 231,935,475,118,605,000,000,000 years to crack AND is easy to remember.
- Browser Plug-ins and Add-ons: Cyber attackers know that your Internet browser (Internet Explorer, Firefox, Chrome, or Safari) is the primary tool you use to interact with the Internet, and since your browser can collect a significant amount of personal information over time, your browser will always be a primary target. To protect yourself, always use the most current version of your browser and install only the plug-ins that you absolutely need. Plug-ins (aka Add-ons) are additional programs you can install in your browser, but they can expose your system to greater risk. Occasionally a website may ask you to install a plug-in, but use caution since these can be attempts to fool you into installing infected software. Whenever possible, install plug-ins directly from the original website and once you have installed a plug-in, make sure you keep it updated. Many plug-ins don't update automatically; you have to manually check and update them yourself.

WORKER RIGHTS AND RESPONSIBILITIES

Cal/OSHA is charged with encouraging companies to reduce workplace hazards and implement safety and health programs to protect workers. But both Cal/OSHA and your employer need your help to keep the workplace safe. So workers have certain rights and responsibilities.

You have a right to:

- A safe workplace free from recognized hazards that could cause death or serious physical harm.
- Proper training regarding the hazards in the workplace and performance of your job assignments according to Cal/OSHA regulations.
- Information about Cal/OSHA inspections, citations, and correction of unsafe conditions.
- Communicate to Cal/OSHA about safety violations in the workplace without fear of retaliation.

You have a duty to:

- Report hazards you see and correct those you are authorized and able to fix.
- Comply with all safety standards and all other government regulations.
- Perform your job in accordance with workplace safety rules and procedures.
- Report all accidents, injuries, and illnesses to your supervisor.
- Properly use all required personal protective equipment and all safety devices for machinery.
- Cooperate with all medical testing, counseling, and treatment to maintain your physical and mental health.

Dead Car Battery?

Dealing with a dead battery may be a nuisance, but it doesn't have to be dangerous or damaging to your vehicle. **Before you attach the cables** make sure the vehicles do not touch and turn the ignition off. DO NOT allow anyone to stand over the batteries while jump-starting is in progress.

Attaching the cables:

1. Clamp the red jumper cable to the positive pole (+) of the dead battery. Then clamp the red cable's other end to the positive pole of the charged battery.
2. Clamp the second (black) cable to the negative pole (-) of the charged battery and clamp the second cable's other end to the dead vehicle's engine block on the side away from the battery.
3. Start the vehicle with the charged battery. Then start the disabled vehicle.

Removing cables:

1. Remove the black cable from the engine block and the other vehicle's negative pole.
2. Next remove both the red cables.