Boulder County Fires:

Be wary of attempts to steal your personal information

The great loss and outpouring of emotion due to the Boulder County fires unfortunately creates fertile ground for fraudsters and identity thieves. It's important that Coloradans remain vigilant about protecting their personal information. Before entering any personal information online, make sure to review websites thoroughly to determine if they are safe, secure, and legitimate.

Reviewing a website's "privacy policy" can be a good resource to find out how sites are encrypting the information they collect as well as how they keep users' information safe. Users that are navigating the internet on a smartphone, tablet, or other electronic device should also be cautious of entering personal information into websites. Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a public Wi-Fi network and send information through websites or mobile apps, someone else might be able to see it. For tips on keeping your information and devices safe visit our Digital Fraud Center.

Here are some important tips to keep your information safe:

- Review the website to determine whether the business has a posted privacy policy and a description of how they encrypt personal or financial information they receive from you. Read all policies carefully. If a site does not post this information or if you cannot understand a company's policies, do not do business with them.
- When making purchases, never provide any "optional" information requested on these websites. Be wary of any website that requests personal information not relevant to the reason you are visiting the site.
- Never provide your Social Security number unless you have independently verified that it is absolutely necessary (e.g., you may need to provide your SSN to check your credit reports online).
- Never respond to emails or "pop-up" messages on your computer claiming there is a problem with your credit card, internet access, or other account. Instead, contact your credit card company or internet service provider directly to verify if there are issues.

- Set up credit card accounts to require a secret password or PIN in order to be used. When it comes to creating passwords or PINs, do not use common numbers like birth dates or part of your Social Security number and do not use commonly chosen words, such as a child's, spouse's, or pet's name.
- Never store passwords on your computer. Memorize them or keep them in a separate, secure location in your home or office.
- Keep up-to-date, anti-virus software on your computer. There are computer viruses that may come as an email attachment that are designed to capture personal information from your computer.
- Never post personal or financial information on discussion threads, chat rooms, or public bulletin boards or forums, even if they claim to be private.

Boulder County Fires:

Be wary of attempts to steal your personal information

Important things to know about “phishing” and “pharming”:

Your inbox is no doubt full of emails from complete strangers with even stranger messages. “This is the email confirmation of your recent purchase,” “VERIFY YOUR ACCOUNT,” “THIS IS YOUR FINAL NOTICE,” “U.K. NATIONAL LOTTERY (WINNING NOTIFICATION),” and so on. All of this is part of an elaborate internet scam known as “phishing.”

In a very real sense, these scam artists are fishing for your personal and financial information. You should be especially wary of any outreach specifically tied to the fires as fraudsters may be using heightened public emotions to steal personal information.

“Pharming” refers to another internet scam where identity thieves misdirect your attempt to visit a legitimate website to a fake site of their design. They do this by attacking corporate domain name system (DNS) servers, which means identity thieves don’t need to persuade you to visit their bogus website, you are automatically misdirected there.

Basic tips on how to avoid these identity theft scams:

- Never respond to email messages from unknown persons or with suspicious messages in the “subject” line. Your real bank, credit card company, or internet service provider will not contact you this way.
- Install trusted anti-virus and anti-spyware on your computer. Most new computers come equipped with such software, but you’ll need to download updates (usually free) on a regular basis to keep up with all the new viruses being developed.

Boulder County Fires:

Be wary of attempts to steal your personal information

Avoiding identity theft scams (cont.):

- Verify that commercial websites you visit offer security features, including encryption technology to protect your personal and financial information. Look for a locked padlock icon in the URL address bar or a website address that begins with “https” rather than the traditional “http.”
- Review the website’s posted privacy and security policies. These should describe to your satisfaction how the business is securing your personal and financial information. They should also disclose whether they sell your information to third parties.
- When a website requires you to establish a password to access certain payment or other features, it will often ask whether you want them to “save your password.” This is tempting, especially since consumers have to remember so many passwords. However, you should never save important passwords online. Keep them somewhere safe at your home or office.

If you believe you have been victimized by a scam or wish to report suspicious activity, please file a report here or by calling 1-800-222-4444.