



Denver DA
Beth McCann District Attorney



October is National Cybersecurity Awareness Month

We talk about it all the time – change your passwords, secure your Wi-Fi network, enable multi-factor authentication, limit what information you post on social media, practice safe web surfing and on and on and on. Some adhere to these best practices, while some have the best of intentions but just don't take the time to implement security precautions.

Security surrounding all types of cyber connections is getting more and more critical. There has been an increase in fraudsters hacking emails, phishing for your data and accessing your home networks. It is time to do your part to protect yourself.

This month, we are dedicating the newsletter to **National CyberSecurity Month** by providing tip sheets that walk you through the steps to ensure your devices are securely connected.

Download and save these tip sheets, forward them on to friends and family and most of all, take action.

Keep in mind we provide virtual presentations on this topic. See below on how to schedule a talk. And above all,

Stay safe and well,

Beth

The National Cyber Security Alliance Tips

Click on each ICON to access the tip sheets

IDENTITY THEFT



TRAVEL SECURITY



During National Cybersecurity Awareness Month (NCSAM), the following tip sheets are invaluable tools for reducing cybersecurity risks.

MULTI-FACTOR
AUTHORIZATION



Use these resources in your communities and share them with your friends and family members.

PASSWORD SECURITY



*CLICK ON THE ICON TO ACCESS
THE TIP SHEETS.*

PHISHING

PROTECTING YOURSELF FROM FRAUD AND SCAMS

VIRTUAL PRESENTATIONS

We are offering **FREE** virtual presentations on how to protect yourself from fraud and scams. Call to schedule "Stand Up Against Fraud" to learn more about COVID-19 scams and other scams happening in our area.



Contact:

Maro Casparian | amc@denverda.org

720-913-9036

GIVE WISELY AFTER A DISASTER

We continue to watch and wonder what additional damage the hurricanes and fires will bring. Emergency preparations are in place and those in the path of these disasters are being updated on what they can and should do to protect themselves.



But what about those of us who are standing ready to help with donations? Here's what you need to know about how to avoid charity relief fraud.

If you want to provide assistance, first and foremost, make sure you know exactly where you are sending your money. If you are not diligent, you may end up being victimized by an opportunist scammer hoping to take advantage of your generosity. The best way to avoid charity fraud is to go online and do your research to make sure your money goes to a reputable organization.

- **Research** – Search for a cause you want to connect with. Use search phrases like "hurricane relief" or "California fire relief."
- **Payment** – Do not pay by cash, gift card or by wiring money. That's how scammers collect, not legitimate charities. Instead, pay with a check or credit card. If you are paying through [an online portal make sure you know how your money is getting to the charity.](#)

Use these organizations to help research charities:

These organizations offer reports and ratings about how charitable organizations spend donations and how they conduct business:

- [BBB Wise Giving Alliance](#)
- [Charity Navigator](#)
- [CharityWatch](#)
- [GuideStar](#)

The [IRS Tax Exempt Organization Search](#) will identify if your donation is tax

deductible. The Colorado state charity regulator link and other important consumer resources can be found on our [Denver District Attorney website under the Consumer Protection tab](#). In order to ask for donations, Colorado requires a charity, or its fundraiser, to formally register the organization. If you believe you were approached by charity scammers or were a victim of charity scams, connect with your [state charity regulator](#) and report it to the [FTC.gov/complaint](https://www.ftc.gov/complaint).

Keep these tips in mind when considering donating:

- Donate to charities you know and trust with a proven track record of dealing with disasters. And, as always, research a charity before you give.
- Designate your dollars to a program rather than the organization's general fund.
- Do not assume that charity messages posted on social media are legitimate. Research the organization yourself. Search its name and add "complaint," "review," "rating," or "scam" to your word search.
- Text-To-Donate can be easy, but first confirm the number before you donate. The charge will show up on your mobile phone bill, but donations are not immediate.

Colorado requires charities and fundraisers be registered in the state. This site outlines each states requirements for charities to run [National Association of State Charity Officials](#). If the charity should be registered, but is not, consider donating through another organization.

W.W.S.D. – (What Would Scammers Do?)

Be alert for scammers tricks! Scammers love to:

- Rush you into making a donation.
- Trick you into paying them by first thanking you for your "previous donation" that you never made.
- Change the caller ID to make it look like a local call and area code.
- Use names that sound a lot like the names of real charities.
- Give vague claims and sentimental stories about their "work" but provide no specifics on how your donation will be used.
- Say that your donation is tax-deductible.
- Ask you to pay via money card or wiring the money.

If you get a call from a new charity, ask them to mail you their information. If there is nothing to send, it's likely there is nothing legit about the charity.

Denver District Attorney's Office | 303-913-9000 | 201 W. Colfax Ave. |
DenverDA.org



Denver District Attorney's Office | 201 West Colfax Ave., Dept. 801, Denver, CO 80202

[Unsubscribe jgriffiths@wadeash.com](mailto:jgriffiths@wadeash.com)

[Update Profile](#) | [About our service provider](#)

Sent by amc@denverda.org powered by

Try email marketing for free today!