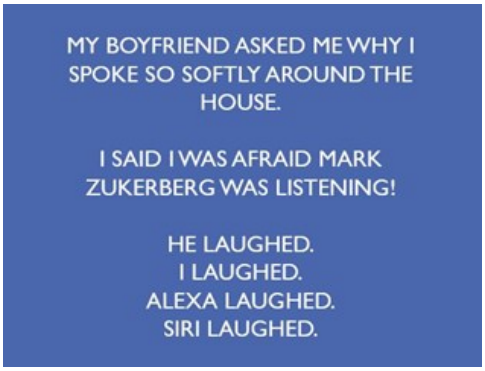
SCAM SPOTTER

Denver DA
Beth McCann District Attorney

National Cybersecurity Awareness Month



October is _____. As consumers we use the internet to pay our bills, shop, file our taxes, and stay connected with friends. But each year millions of people are victims of internet scams, have their identities stolen, and some even lose their life savings. There can be life-long ramifications to being a cybercrime victim and undoing identity theft can take years.

I am asking for your help in spreading the word about how critical it is to protect yourself from cybercrimes. Book one of our free presentations which provides safety tips for everyone – remember scammers target anyone no matter what age. Encourage organizations with which you are involved to for this monthly *Scam Spotter* newsletter and to pass along the information to their members.

Once you know the red flags of an online scam, are familiar with how scams work, and understand that anyone can be targeted by scammers, you are well on your way to being cybersecurity aware.

Beth

What Social Media Do You Use?	What Have You Registered For?
Facebook	Credit Card
Twitter	Rewards Programs
Instagram	Magazines
Tumblr	Subscriptions; Sign up for auto emails
Google	Coupons/ Club members

Staying Cyber Safe Starts with You.

What is your Digital Footprint?

Ever wonder how crooks steal your personal identifiable information (PII)? Do you register for rewards programs, use social media, or search on Google? If you do, then you are populating the internet with your personal information.

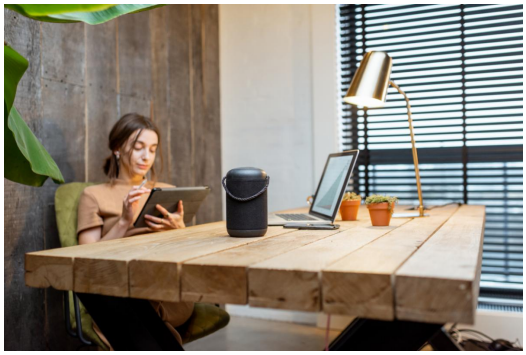
Engaging in any online activity puts your personal information out to the world. While it isn't likely you will stay off the internet, it is in your best interest to learn some cybersecurity best practices to limit your exposure to scammers.

TIPS:

1. Set your social media accounts to private.
2. Stop oversharing. The more you put out there, the more a scammer will know about you. The more scammers know about you, the more convincing they will sound if they try to reach out to you.
3. Review the privacy settings for each and every service and app that you download. Privacy settings can help you increase control over your personal information online. The default privacy settings may not be the best option as information may still be collected and used in ways you might not want and can often leave you exposed. If you are not comfortable with what they will collect, don't sign up.
4. Limit location tracking on apps and services. Turn off 'share location' and use it only when really needed.
5. Coordinate your settings so they are all the same on all your devices.
6. Consider using the incognito mode when internet surfing. Doing so reduces tracking. Norton's website provides information about what cookies are and what happens when you accept or block cookies here.

Need to be convinced as to how easy it is for anyone to capture your personal information? Watch this YouTube video.

DIGITAL ASSISTANT DEVICES



Speaking of oversharing, those home digital assistant devices such as Siri (Apple), Alexa (Amazon), Cortana (Microsoft) or Google Assistant are designed to respond to your commands and take action. In addition to telling you what the weather is, these 'assistants' are collecting vast amounts of personal information about your daily activities and sending the information back to the parent company. Those

companies in turn, can sell that data to other companies to use in their sales and marketing efforts.

Working from home? If you are having confidential work calls or speaking of issues that should not be recorded, consider turning off the microphone or moving the device to another room. Above all, check the privacy settings on the device. This article from CNET will help you get started.

What About CryptoCurrency?

According to a Federal Trade Commission report, cryptocurrency scams are on the rise and account for a fourth of all dollars lost to such fraud. The report found that people between the ages of 20 and 49 were more than three times as likely as older cohorts to be taken in by cryptocurrency scams.

Increased time on social media means increased exposure to ads, posts, and messages promising big profits and quick returns. A first-quarter 2022 FTC report states that 49% of scams that required cryptocurrency as a form of payment were initiated on social media.

Here are the FTC's tips:

- **Only scammers will guarantee profits or big returns.** No cryptocurrency investment is ever guaranteed to make money, let alone big money.
- **No legitimate person or organization will require you to buy cryptocurrency.** Not to sort out a problem, not to protect your money. That's a scam.
- **Never mix online dating and investment advice.** If a new love interest wants to show you how to invest in cryptocurrency or asks you to send them cryptocurrency, that's a scam.

PASSWORDS

Tired of constantly hearing security experts tell you to change your passwords? We all have online accounts and keeping up with which password goes to which account can be overwhelming. So overwhelming in fact that many use the same password and username for multiple online accounts. Compromised passwords are one of the easiest ways to be hacked.

Tip: Use a password manager like these click on the word to access the link. Last Pass, RememBear, 1Password.

DEVICE PROTECTION

Remember to protect your online accounts (Facebook, TikTok, Amazon) as well as your physical devices phones, computers, and tablets.

TIPS

- Use a PIN or biometric to lock your devices. If you lose your device and have not password-protected it, all your information is available to whoever finds your device.
- Install Find My iPhone or a similar app for Android devices. If you lose or misplace your device, you can use the find my phone app to reset the phone completely, making it useless to the thief.
- Apply software updates ASAP. This includes updating your home router and mobile devices.
- Download apps from trusted sources. Malicious malware-laced apps such as the Joker malware allows scammers access to your contact list along with other data on your device. Look for apps that have very high install numbers and positive reviews.

PEER-TO-PEER PAYMENTS

Peer-to-Peer payment services like PayPal, Venmo and Zelle are apps that allow you to send money to other people simply by using their phone number or email address. The convenience is wonderful. Generally safe, but these services operate just like cash so there is no way to dispute any payment. Once you pay, your money is gone and there is very little chance of getting it back.

TIP: Only pay people you know. If you receive a request for payment, verify you know the person through a different messaging system.

Do you suspect you've been scammed or exploited? Report it to us by calling our Fraud Hotline.

Contact:
The Denver DA's
FRAUD HOTLINE
720.913.9179

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 720-913-9000