Denver DA
Beth McCann, District Attorney

NATIONAL EMOJI DAY
BEWARE THE SMILING EMOJI

Who among us hasn't enjoyed enhancing a text or an email with a wink, a nod, or even a hat? These icons are adorable. They take the place of words, save on character space, and provide a little emotional intent behind your words. And, for the most part, emojis are harmless. But we wouldn't be talking about emojis in this newsletter if there wasn't a more sinister aspect to them.

"Emojis have become the 'bait-of-choice for scammers," says the Identity Theft Resource Center. Scammers fill up emails, texts, Facebook posts, and Match.com conversations with them to make the person seem more friendly, lighthearted and approachable. The more friendly and approachable a text, even from a stranger, then, ***obviously,*** the more truthful, honest and safe the person. Right? Wrong! Remember, scammers are professionals. They will pose as most anything and say anything to capture your trust and get you off guard.

Additionally, if you've downloaded an emoji keyboard from an

unapproved source, you may have downloaded viruses, malware or a way for hackers to mine your data.

WHAT TO DO?

First, remember that scammers can easily pose as a friend or someone you'd like to connect with, or by spoofing an existing account of someone you already know. Check to make sure you are connecting with the person you know. Be wary about accepting friend requests. If you receive a friend request from someone you are already connected to, reach out to that person directly and see if they were hacked. And, always practice sound judgement. If a new friend is overly friendly early in the relationship, be open, but wary.

Second, if you are downloading emoji keyboards, make sure the app is approved and vetted. And always remember, if you receive an unfamiliar message, don't click on the link. Exit out of the program and check the account directly.

AMAZON'S NOT SO PRIME DAY ALERT!

If you were a Prime customer last year, a new phishing scam may be coming to you in an email phishing scheme. Scammers are sending mass emails-- that look just like they are from Amazon. The realistic email thanks the customer for making a purchase last Prime Day. The email then invites the Amazon customer to write a review of last year's purchase and by doing so, the customer will receive a special $50 "bonus" credit for doing so.

The email will look like Amazon. BUT- if you click on the link you will get directed to a criminal's clone of the Amazon site. The site is all set up for you to put in your private login credentials and just like that, you are hacked.

Here are the clues that this is not legit:

1. The email never mentions the particular item you purchased. Amazon knows EVERYTHING you've ever purchased and is quick to tell you. Not mentioning the purchase is very un-Amazon.
2. We've told you never to click on a link without first verifying that it is a legit hyperlink. Hover over the link in the URL. If it doesn't show www.amazon.com, then step quickly away from your keyboard before you click.
3. Do your research. Amazon NEVER pays customers for reviews.

Bottom line: To be ultra safe when surfing or shopping, do not click on a link. Instead, type in the web address directly into the URL.

SPEAK UP AGAINST ELDER ABUSE

Elder Abuse is not ok, yet each year approximately 1 in 10 Americans aged 60+ have experienced some form of elder abuse. Some estimates range as high as 5 million elders who are abused each year. One study estimated that only 1 in 14 cases of abuse are reported to authorities.

Know the signs of Elder Abuse. If anything sounds familiar, call the Police or Adult Protective Services right away.

THINK YOU'VE BEEN SCAMMED?

If you suspect you've been scammed or exploited, call our Fraud Hot Line to report it. 720-913-9179

SCHEDULE A SPEAKER

Interested in learning more about scams happening in Denver? Do you want to know how to protect yourself from identity theft? Maro Casparian is available for speaking engagements to any group or organization. Presentations are free! Contact her by email: amc@denverda.org or via phone: 720.913.9036.