SEPTEMBER 2018

THE SIDE BAR

Newsletter of the Martin County Bar Association

IN THIS ISSUE

President's Message (Pg. 1)
Executive Director Update (Pg. 3)
CLE Luncheon Meeting (Pg. 6, 44)
Constitution Week (Pg. 4)
Annual Fall Reception (Pg. 7)
Law Day 2018 Recap (Pg. 10)
TD Bank "Free $" (Pg. 16)
Cheers (Pg. 22)
2018-19 Committee Chairs (Pg. 24)
Annual Membership Renewal (Pg. 28)
Free Legal Info. (Pg. 32)
Online Courses (Pg. 33)
Member Benefit Program (Pg. 37)
Free CLE (Pg. 39)
Pro Bono Service Awards (Pg. 41)
Links, Jobs & Legislation (Pg. 42)
Calendar of Events (Pg. 43)

Law/Bar Related Committee Reports:
Appellate (Pg. 21)
Bankruptcy (Pg. 20)
Criminal (Pg. 40)
Elder Law (Pg. 15)
Employment & Labor (Pg. 34)
FAWL (Pg. 36)
Florida BOG (Pg. 33)
Immigration (Pg. 13)
19th JNC (Pg. 5)
Judicial Relations (Pg. 7)
Justice Teaching (Pg. 5)
Legal Resources (Pg. 30)
Legal Aid (Pg. 32)
Lady Lawyers (Pg. 41)
Paralegal (Pg. 29)
Pro Bono (Pg. 17)
Professionalism (Pg. 12)
Real Property (Pg. 38)
Scholarship (Pg. 16)
Trial Law (Pg. 19)
Wills, Trusts & Estates (Pg. 29)
YLD (Pg. 11)
5K (Pg. 11)

THE SIDE BAR NEWSLETTER

Published monthly, excluding June & July, by the Martin County Bar Association as a service to its membership.

If you have an article, opinion, news or other information for publication in the *SideBar*, please call (772) 220-8018 or email information to: martincountybarassociation@msn.com

The due date for all advertisements, articles and announcements is the 1st of the month preceding publication.

MESSAGE FROM THE PRESIDENT

On Spoofing


Barbara Kreitz Cook
2018-19 President

Modern "phishing" and identity theft scams increasingly rely on a technique known as spoofing. Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message. It has been an ongoing successful tactic because people are more likely to open an email when they think it has been sent by a legitimate source. Years ago spammers used to get contact lists from malware infected PCs while today's data thieves choose their targets carefully, phishing them with messages that look like they came from friends, trustworthy sources, or even their own account.

Continued On Next Page . . .

Continued From Previous Page . . .

No one is immune. In fact, for the past 4 to 5 years, with the change of the Martin County Bar Association officers on July 1, the incoming Treasurer receives an email from the President asking the Treasurer to make an urgent wire transfer payment to a vendor before a deadline. Of course, the President's email ID is spoofed, but without warning, the new Treasurer may think the email is legitimately from the President.

Early "spoofers" did not mask the ID as well as now, so it was easy to pick up the trickery. The MCBA has instituted procedures to assure payments are not made except as invoiced, authorized and approved by multiple board members.

You may be savvy and not likely to be taken in by an online scam but we all have friends, relatives (especially children) and office staff we worry about. Here are a few tips to help avoid falling victim to an online scam:

- **Never, Ever Click a Link to Your Bank or Financial Institution From an Email.** Legitimate banks or financial institutions like Paypal will never email you asking you to click a link to verify your information, reset your password, or login to view anything. You should simply create a browser bookmark to your bank, and when you receive an email, use the bookmark or type in the bank name manually into the address bar.

- **Never Give Out Your Email Password.** It's become a trend of new sites to ask people to invite their friends to join by entering their email address and password into the website, but this is something you should always avoid. Not only will you most likely end up spamming all of your friends with invite requests, but some sites will keep that information and continue to spam your friends forever. Of course, that is secondary to the fact that all your password reset requests will go to your email address so if the wrong people get your password, they can access your entire online life. You should simply never give that information out to anybody for any reason.

- **Use Strong Passwords (and Secret Questions).**

- **Ignore Website Pop-Ups Saying You Have a Virus or that your Email Account Will Be Voided . . .** because it is probably a virus you are downloading or from a scammer who is trying to get you to divulge your email password!

Other areas to consider include:

- Do you work from home at times such that your children have access to your work email and confidential client files? That is what sealed Hillary Clinton's fate in her run for the presidency, via trusted staffer Uma Abedin, whose husband, Anthony Weiner, of iconic name infamy, had access to his wife's emails sent from her boss to their shared home computer.

Continued On Next Page . . .

- Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station.

  I am sure you have received calls from "Rachel" at card member services looking to verify your credit card number to lower interest rates, from many different caller ID's that are not her real number. When you call that number back, it is not "Rachel" but some other person or not a working number. If you ever question the number that you see on your caller ID, remember to be cautious. The final check you could make is to enter the number in question in a search engine. This allows you to see if the company has the number on their website or if the company has mention of a scam that is going on. It also allows you to figure out what other people are saying about the number. The FCC also prohibits the use of using caller ID spoofing with intent to defraud, cause harm and wrongfully obtain anything of value. When anyone has the ability to call you as another person or company, it's impossible to know his or her intentions. Make sure to take the time to verify the person on the other end of the phone.

Join us at this month's Bar luncheon (see Page 6 for details) as Carolyn Timmann, Martin County Clerk of the Circuit Court & Comptroller, will be our speaker presenting relevant legal technology updates and resources.

Sincerely,

Barbara A. Kreitz Cook

Barbara A. Kreitz Cook
President