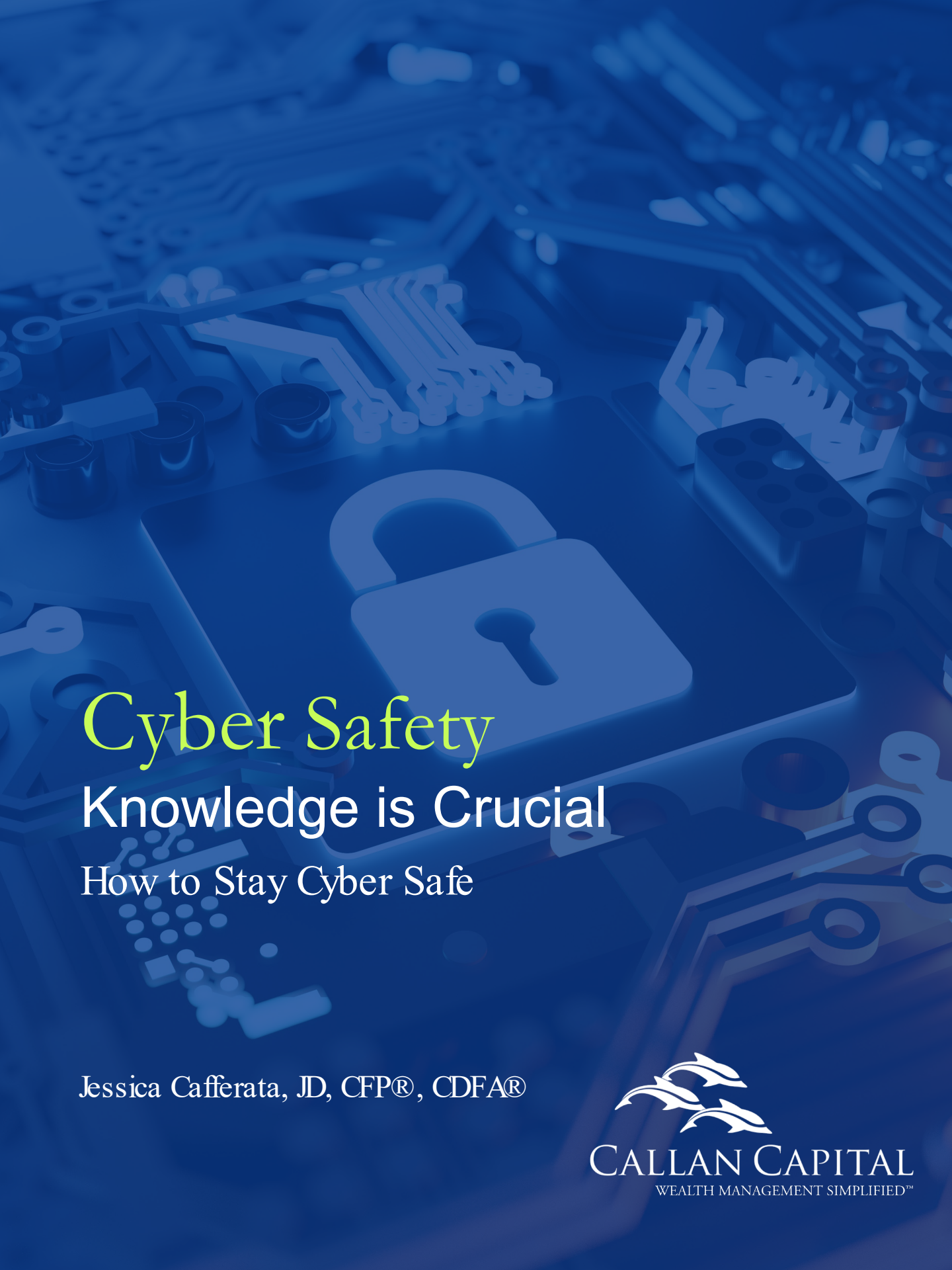

Cyber Safety

Knowledge is Crucial

How to Stay Cyber Safe

Jessica Cafferata, JD, CFP®, CDFA®

CALLAN CAPITAL
WEALTH MANAGEMENT SIMPLIFIED™

At **Callan Capital,** we are committed to cybersecurity awareness, education, and training. It is our hope that the following is helpful for you, your family, and friends as a resource for cybercrime prevention, knowledge, and mitigation. This is part of a monthly cyber awareness series aimed at helping our clients stay cyber safe.

Four Steps Towards Cyber Safety

1. Were you expecting it (the call, e-mail, attachment, request)?
    a. Do you know the sender/caller?
    b. How do you know the person is who they say they are?
        i. Independently verify the sender/professional by calling them from a number you found on our own and not from the number the person provided to you in the e-mail, text or by phone

2. Think Before You Click
    a. Hover over the e-mail address
    b. Hover over the link

3. Treat Attachments as Suspect

4. Look for Red Flags
    a. Is the request unexpected?
    b. Is there a sense of urgency?
    c. Does the request make sense?
        i. Financial professionals will never ask for your login credentials for example
        ii. Is it an usual request from someone you know?
    d. Is sensitive information being asked (DOB, SS, account numbers)?
    e. Is the person exploiting your emotions?

Regardless of who the e-mail, text, or phone call is from, ask yourself, “Was I expecting it?” Since fraudsters access e-mails and texts, it can be easy to impersonate your bank, realtor, friend, family member, doctor, trusted professionals, and the IRS or other government officials for example. If you were not expecting a text from your medical provider, a phone call from the social security office or IRS, or a surprise bill in your e-mail, for example, do not respond to it. Close the e-mail or text or hang up from the call and look up the contact information for who just called, text, or e-mailed you by searching on Google. Do not use the phone number or e-mail provided in the e-mail, text, or by phone. After independently finding the contact information, call the person or individual and verify that they reached out to you and what was being requested of you. If there is any uncertainty, even if the request or ask may be legitimate, you can always conduct business in-person.

Even if you were expecting it, treat all *requests, links, and attachments* as suspect. Fraudsters often obtain access to e-mail and wait for an opportunity. For example, wife fraud often happens when a fraudster gains access to e-mail and seizes the opportunity to pretend to be the other party in the e-mail and changes the wire instructions. Even if a wire transfer is expected, or your accountant is e-mailing you an attachment, always look very carefully at the e-mail address, the link, and the attachment without clicking on the link or e-mail address by hovering over both the e-mail address and link. Cybercriminals make slight changes to impersonate e-mail addresses and count on you not looking at where the link is taking you.

91% of cyber attacks begin with a spear phishing email

Source: KnowBe4, 2018

Always independently verify the request and sender/caller by contacting the organization or individual from a phone number you know to be true or that you independently verified yourself. Please keep in mind that Callan Capital will never e-mail you or call you requesting password information and we verbally verify all wire requests.

Contact Us:

Callan Capital is committed to bringing clarity, direction, and peace of mind to financial choices.

Disclaimer: Callan Capital does not provide individual tax or legal advice, nor does it provide financing services. Clients should review planned financial transactions and wealth transfer strategies with their own tax and legal advisors. Callan Capital outsources to lending and financial institutions that directly provide our clients with, securities-based financing, residential and commercial financing and cash management services. For more information, please refer to our most recent Form ADV Part 2A which may be found at www.adviserinfo.sec.gov.