IT'S A SCAM. DON'T FALL FOR IT.

In the fall of 2017, we received a message from an AGO chapter treasurer who said he had received an email that appeared to be from the former dean of the chapter. The email requested that he send a check for $1,750 to a vendor in New Jersey. The treasurer complied with the request. Later the treasurer received a second email request from the same former dean requesting that additional money be sent to a third party. A third request subsequently came from the former dean asking that $1,450 be paid to him via MoneyGram. The treasurer contacted the former dean and discovered all of the requests were bogus. It was a scam. The dean's name and email address had been criminally appropriated to extort money from the chapter. Fortunately, MoneyGram was able to put a hold on the last request and the chapter was able to get that amount back, but last we heard the treasurer was still trying to recover the original $1,750 from Wells Fargo.

This has happened to quite a few chapters. No one can stop these phishing attacks. Treasurers must be vigilant and suspicious of any request to send money somewhere, especially out of state. Never hesitate to call the person who appears to be making the request to confirm whether it's for real. You may discover it's a scam. Don't fall for it.

Recently my AGO spam filter caught up to a dozen posts sent to me by some creep (or a community of creeps) trying to extort money from me. These pernicious emails appeared to be coming from me, from my AGO email address, and were addressed to me at my AGO email address. The writer tells me that he has taken over my computer and its camera and photographed me while I've been visiting adult websites. He threatens to release pictures of me enjoying these sites and of images from the sites themselves unless I send him a tidy sum in Bitcoin. Other staff members have received essentially identical emails. We all know it's a scam. We are not falling for it. Here are excerpts from the actual email.

> Subject: Caution! Attack hackers to your account!
>
> I hacked your device and then got access to all your accounts
>
> Moreover, I know your intim secret, and I have proof of this.
>
> In fact, I posted a malicious code (exploit) to an adult site, and you visited this site . . .
>
> While watching a video Trojan virus has been installed on your device which gave me access to your microphone and webcam. Soon after, my software received all your contacts from your messenger, social network and email.
>
> I will give you two suitable options. The first option is to ignore this email. If you choose this path, I will send your video to your contacts, including family members, colleagues, etc. The second option is to pay me. If you choose this path, your secret is your secret. I immediately destroy the video. You continue your life as if none of this has happened.
>
> Now you might think: "I'll call to police!" I have taken steps to ensure that this letter cannot be traced to me Let us hope that you decide to pay me a fee for confidentiality. You make a Bitcoin payment. Shipping amount: $750(USD).
>
> I have a spetial code in Trojan, and now I know that you have read this letter. You have 48 hours to pay. If I don't get BitCoins, I'll send your video to your contacts, including close relatives, co-workers, and so on. But if I get paid, I immediately delete the video.
>
> This is a one-time offer that is non-negotiable, so do not waste my and your time. Bye!

A few years ago I bought a new Mac desktop computer. While browsing the Internet, an alarming notice suddenly commandeered the whole screen, advising me that a truly dreadful virus had attacked my computer and I needed to call a special number at once to clear it. I froze in horror. The screen also appeared to be frozen. The message looked legitimate to me. I called the number in a near panic that I had caused major damage to my brand-new Mac, and before I knew it I was being asked for my name, address, and telephone number; my bank's name, its routing number, and my account number; my social security number; and other very sensitive information. I finally realized it was a scam. I hung up, called AppleCare myself, and after they did some diagnostic tests, they assured me my computer was fine and no viruses were on it. It was a scam. (I had just begun to fall for it.)

Last night, returning home from a weekend getaway, there was a voicemail on my answering machine. A robotic voice informed me that I was being called by Microsoft and that the Microsoft license on my computer was about to expire, which would disable the computer and lock me out of all of my files. The solution was to call a number I was given and select option 2 immediately. My wife and I listened to the message together. Then she reminded me that we don't have a computer that runs on Microsoft anymore. It was a scam. We didn't fall for it.

Scams are everywhere. This is just a representative sample of those I've personally experienced. Be on the alert for them. Don't fall for them. Please secure your data by regularly backing up your computer and by installing antivirus software to protect yourself against phishing attacks and malicious ransomware. Above all, don't give away personal information to complete strangers!

JAMES THOMASHOWER