(Approx. 1579 words)

President’s Corner

To Discern the Truth

By Greg Skalka, President, Under the Computer Hood User Group, CA

www.uchug.org

president (at) uchug.org

In the TV game show To Tell the Truth, three contestants all claim to be the same person. Each segment starts with the three lined up next to each other, each claiming to be the described character (“I am John Smith,” for example). A panel of four celebrities was tasked with determining which of the three was the real ‘John Smith’ by asking each contestant (numbered one through three) a set of questions. They knew the authentic ‘John Smith’ was obliged to tell the truth, while the two imposters may lie. After the period of questioning, the celebrity panelists each record their votes for which contestant they believe is the real ‘John Smith’, and the real central character is then asked to stand and reveal themselves. The show first aired in 1956, was popular from the 1950’s through 1970’s, and a revived version has been produced in recent years.

Today we are all unwitting participants in a game played out on the internet to discern the true identities of those we communicate with. Unfortunately, the stakes are higher than some cash divided among the contestants that is proportional to the number of celebrity panelists deceived by the imposters, as in To Tell the Truth. In our game, our confidential personal information, our identities and possibly our finances are at risk.

On the internet, there is a lot of information available, but a lot of it is suspect. Every email, Facebook post, tweet and blog entry could be the absolute truth, totally false or something in between. Even Wikipedia entries could contain biased or even false information, as though they are supposed to be written and reviewed by experts, it is a “crowd-sourced”; encyclopedia. Email is a particularly problematic communications medium for determining the truth of information. The accuracy of statements made in individual emails is obviously subject to the credibility of the sender, and this is usually only judged by the recipient of the email. Unfortunately, it is often difficult to truly know

who the real sender of an email is. For some emails, it is pretty obvious the sender is not the IRS, the Director of the FBI or a Nigerian prince. In other cases, it can be more difficult to verify that the sender is who the email claims. That email from a bank you don’t do business with is probably suspect, but what about the emails from banks, utilities, credit cards and other businesses you do expect dealings with?

How do you determine if the email sender is who they claim to be? How do you get them to tell the truth? There are a lot of checks you can make to help discern if an email is authentic and from the source they claim. Look carefully at the sender’s email address listed; if the email is from wellsfargo@gmail.com, it is probably not really from Wells Fargo Bank. Even if it looks legitimate, hovering over the address by placing your mouse cursor over the text in the email header may reveal that the actual address is different.

Corporate emails that contain misspellings or grammar issues are probably fake. Emails sent at an unusual time of day for the sender (like the middle of the night) could be suspect. A lot of these are phishing emails, sent by bad people with the hope that you won’t notice these inconsistencies and will click on the link included, or open the file attached, actions that will put malware on your device or trick you into entering your real passwords into their fake sites.

I have received my share of phishing emails and think I can spot them in most cases. I know enough to be suspicious and never click on links or open files sent to me, unless I am expecting them or have verified their authenticity. Last week, however, I was part of a fake email scheme that I had not seen before. I was not the target; the fake emails were sent to others I have corresponded with. Fortunately, these were savvy tech users and it does not appear anyone was taken in by the scam.

I first became aware that something was wrong when I got up on the morning of Monday, April 15 (which was tax day, but I don’t think that had any significance). My son sent me a text while I was eating breakfast; he said my UCHUG email address had sent him a strange email at 3 AM and might be hacked. He attached screen shots of the email. The email he had received appeared to come from my president@uchug.org address, and appeared to have two parts, as in an email chain. The first, current part

was a generic message characteristic of phishing emails. It had a zip file attached,

Greg\_Skalka\_UCHUG.zip. The second part of the email, as if it were a prior part of the email chain, was what I recognized as an actual email that I had sent from a work email to my son over a year ago.

I had my son confirm that he believed the email he received was sent from my UCHUG president email address. I found this to be unusual, as I never send emails from that address. Our group’s web hosting and email services are through 1&1 Ionos, and since I am not fond of their email web interface, I have the three uchug.org email address; all are forwarded by the 1&1 email account to my personal email address.

I wondered if someone had actually hacked into my UCHUG president email account but didn’t think too much more about it until I started getting more warning emails. Over the course of the morning I received emails from eleven people that had received a similar email from president@uchug.org with the mystery zip file attachment. These included a few of our UCHUG members and officers, a number of APCUG officers and member group officers, and even Bob Gostischa (our March meeting presenter). Most people replied back to me (the UCHUG president email) questioning why I had sent the zip file. A few tried to open the zip but their security software flagged it as infected.

In each case, the emails they received contained the same generic ‘Good Morning’ message with the same zip file attached. The second part was unique in each email, as were the email subject lines. In most cases that second part was an email that the recipient had received previously, either from me, our editor or another APCUG member.

When I received the first reply at around 7:30 AM, I realized this was likely to be more than just an errant email my son received. I quickly wrote back to the first recipient:

Unfortunately, I did not send you any emails recently. It appears others have been receiving the same email, appearing to come from our president@uchug.org email address. Either that UCHUG email address has been hacked (I&#39;m copying our webmaster so he can look into it) or someone is spoofing that address. In either case, that email is suspect; please don’t open its attachment. I don’t actually send from the president email address (emails sent to it are forwarded to my personal email), so anything sent from it is not from UCHUG. Sorry - it is sad we live in such a world.

As I received additional replies, I copied that first response and sent it to each, to explain what had happened.

Bob Woods, our webmaster, soon let me know that he could find no evidence that our email account had been hacked, or that these bad emails were being sent from our account. As a precaution, he changed the passwords on my three group email accounts. It appeared that someone was spoofing our UCHUG email address when sending these out. Since there was nothing we could do to stop that, all I could do was continue sending my warning response to all replies I received.

By early afternoon, the replies to the bad email had stopped. The ‘infection’ had apparently run its course, with only about a dozen of these impersonating emails sent out, and no one appeared to be the worse for it. Most of the recipients were sufficiently suspicious to not try to open the attachment, and those that did try were protected by their device’s security software.

A few days later, Bob Woods sent me an email with a link describing a situation very similar to mine: <https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/> This ZDNet article describes how the Emotet malware gang has stolen old email threads (probably getting them from a PC previously infected with their malware), attached an infected document and sent it out to others in the thread. This is possibly what happened with the UCHUG president emails on April 15.

Thus it appears there are bad actors out there, trying to impersonate email users, using old email chains to try to deceive other users into opening their infected attachments. Just like in To Tell the Truth, they are imposters, saying “I am the president of UCHUG,” trying to win the game by infecting computers. We all need to be wary and make sure we are certain we know the sender before trusting the message. We all need to ask the equivalent of “Will the real president of UCHUG (or the real email sender) please stand

up!”