In this issue:

While the world continues to grapple with the coronavirus pandemic, scammers have not missed a beat. We have continued to see an influx of scams stemming from the pandemic—from unemployment cons to social media hacks. We must continue to be vigilant online. Read on to learn more about these, as well as:

- A widespread FINRA phishing campaign
- What happens when a hospital is hit with ransomware during a pandemic
- The security concerns related to Coronavirus tracking apps
- And much more

How to protect yourself from social media scams

Earlier this month I received a follow request on my personal Instagram account. The request appeared to come from my husband's uncle; we'll call him Tom—it had his name and a picture of him and his son—so I accepted. A few minutes later I got a message from Tom, "Hello. How are you?" I didn't think much of it and quickly responded, "We are good. How are you and the family doing?"

"I guess you haven't heard what happened to me," Tom said. This is when I first started to have suspicions whether I was talking to the real Tom. We had video chatted with Tom and his family a few days earlier and everything seemed fine. "No?" I said.

"I'm just wondering if you must have heard anything about the new development in ongoing Contingency Fund for Emergencies (CFE) COVID-19 Coronavirus?" At this point, I knew something was wrong—this really didn't sound like Tom so I stopped answering. A few minutes later I got a text message saying Tom's Instagram had been hacked and the hacker was asking for money.

I took a deeper dive. Tom's regular account wasn't hacked—a hacker created a look-a-like account with the same username of Tom's account, but off by one number. He used the same profile picture and posted the same photos that were on Tom's real account. He then started following Tom's followers and asking them for money.

This type of scam can be even more difficult to detect than an account getting hacked. In these cases, the person who is being impersonated may have no idea what is happening since they can still access and post on their account. They don't see any strange messages in their account because the hacker is using a look-a-like. Usually, they only discover the fraud when a friend or family member reaches out offline to see if everything is OK.

Scams like this have been around for many years but have gained in popularity in recent months. With so much uncertainty stemming from the coronavirus pandemic, scammers are preying on people's desire to help friends and family who may be experiencing financial difficulties. We must all be on the lookout for these types of scams on Instagram and Facebook. Here are some tips to avoid being scammed.

Look closely at the account

If you get a new friend request or follow request take a close look before accepting. In my case, I was already "friends" with Tom's real account on Instagram. Had I looked at my friends, I would have seen his real account and probably would not have accepted the new request.

If you get a new request from someone you are already connected to, there is a good chance it could be a fraudulent look-alike account. You should reach out to the person off of the social media platform to ask if they have created a new account and sent you a request. Not only will this protect you, but it could alert them that they are being impersonated.

Think twice before taking action

If you receive a message from someone you know on Facebook or Instagram like I did from Tom, pause before you respond. Messages like this create a sense of urgency hoping to get you to take action right away. If the person is asking for money or private information, contact them off of the social media platform to confirm. Remember, if your family member or friend were in trouble, they would probably call or text you before messaging you on social media.

Block the impersonator

If you accepted the request from the impersonator, you will want to block the account once you discover it is fake. You should also contact the individual being impersonated and let them know of the fake account. They can report the impersonation to Facebook or Instagram and try to get it removed from the platform. They can also warn their followers and friends to not accept requests from a new account in their name.

Just like with phishing emails, we need to be vigilant about any message we receive on social media. Always take a closer look and if unsure, verify with the person off of the platform.

Cybersecurity shorts

Scammers improve the old bank-fraud scam. You have probably heard of scammers impersonating banks and calling users to gain access to account information. These scams have always been sophisticated, with scammers spoofing the bank's phone number to make it appear as though the call is legitimate. Now they have added another trick—accessing real transaction information to gain your confidence. Security expert Brian Krebs says that a reader contacted him after falling victim to the scam. The reader banks at Citi and discovered that anyone could access transaction information by calling the main number from the phone number on file (easily spoofed). While this has not been reported at other institutions, it is important to remember to always be cautious when receiving a phone call from your bank. If you are unsure, hang up and call them directly.

Widespread FINRA phishing campaign is making the rounds. The regulatory agency is warning advisors and firms of fraudulent emails appearing to come from the organization. The email asks recipients to download an attachment immediately. If you receive an email like this, delete it.

Cybersecurity attacks have increased three to five times, according to the Harvard Business Review. And many of these attacks are directed at businesses. Recovering from a cyberattack is costly and difficult for most organizations. The Harvard Business Review has released a list of actions all businesses should take now to help prevent an incident. Read more here.

European private hospital system hit by ransomware during the COVID-19 pandemic. Fresenius, the largest private hospital operator in Europe, had its systems taken offline by ransomware in early May. Some operations within the company were limited by the attack, but Fresenius says that patient care continued.

Some legitimate unemployment benefit letters sent to prevent identity theft have people thinking their identities have been stolen. Security expert and writer, Brian Krebs reported on the confusing letters this month. U.S. Bank, a financial institution that handles unemployment payments for many states, sent letters out to confirm recipients' addresses for payments to be sent. The letter said the recipient's address has been updated, but provided no address to confirm. These letters are legitimate, but if you receive one and are unsure, call the company directly.

Women are better at cybersecurity than men according to a new study by NordPass. The survey found that women are more likely to use unique passwords for banks, personal email, and online shopping accounts. And that means fewer fall victim to cyber hacks—46% of women compared to 54% of men. However, only 24% of cybersecurity jobs are held by women.

Mobile payment apps are playing a large role in coronavirus-related scams. Security experts are warning that many scammers are asking victims to send money via payment apps like PayPal and Venmo. Often, victims do not understand how these apps work and send the money thinking they will be able to get it back. Before you send any money, be sure you are sending it to the right person for a real service.

Coronavirus tracking apps raise security concerns. As companies like Apple and Google race to create a contact tracing app to track the coronavirus outbreak using Bluetooth, many experts express their worries. Bluetooth technology tends to be less accurate than GPS and is susceptible to hacking. You can read more about the possible issues here.

New ransomware scam impersonates the FBI and targets Android phones. The scam starts with a malicious link that locks the victim's phone. They are told the data has been locked because they possess pornographic material and their data has been sent to the FBI. Victims are told to send $500 to avoid legal action and get their devices unlocked.

EasyJet data breach exposes information on 9 million customers. The European budget airline experienced a massive breach this month resulting from a sophisticated scam. Over 9 million people had their email addresses and travel data stolen while about 2,000 customers had credit card data exposed. Affected customers will be contacted by the company.

Software updates

Adobe: Adobe has released updates for Acrobat and Reader this month closing over 20 security vulnerabilities. You can download the updates here.

Microsoft: This month Microsoft has released updates for over 100 security issues in Windows programs. Sixteen of the vulnerabilities are considered critical, so users should update as soon as possible. Your device should prompt you to update automatically. You can read more about the updates here.