Be wary of scammers, some tips

August 16 2019, by Jefferson Graham, Usa Today

Credit: CC0 Public Domain

Readers, you really need to be on your toes.

On Wednesday, federal prosecutors said that hack of Capital One bank credit card applications and those 140,000 social security numbers that were accessed was just the tip of the iceberg, and that several other firms, government agencies and educational institutions were also hit.

Which just goes to show you that even when you think you're doing something that's safe—applying for a credit card application, your data is at risk.

So what to do?

Be skeptical. Very skeptical

In this case of Capital One applicants, they did the right thing. It was the bank and what it blamed as a human error in security monitoring that led them down.

But still, we need to take precautions and be extra safe.

We once had our Yahoo account hacked from a legit looking e-mail with fine print so small, that when we were asked to click a link to keep the pro level of the mail account, we did. The next day, many friends started receiving distress e-mails asking for money to get me home from a foreign land, when I was said to be penniless.

This week, another bogus e-mail arrived, this time supposedly from Instagram. It had two big giveaways that it was fake, but it took me a minute to realize.

The e-mail said it was from Instagram, and said that in order to hold onto my verified account, I needed to confirm receipt by noting my "region, phone number, and password."

Right.

Then there was the email address I was asked to write back. Not instagram.com, but instagramhelpfuls@gmail.com, such an obvious fake. If there's no company address listed, don't be a chump. Delete it

and move on.

Readers, if a company asks you to hand over phone numbers and passwords, you know something really wrong is up. Companies ask us to reset passwords, not to reveal our private information in an e-mail.

Remember that the great Hillary Clinton email scandal of 2016 happened when her campaign manager got a bogus email from a company he thought was Google asking him to update his personal information.

Be on your toes, people.

Change passwords

My friend Rhonda got hacked this week on Facebook, in one of the oldest scams in the world. Someone got hold of her personal information , and friends began to get friend requests from Rhonda, even though we were already friends.

Facebook's solution wasn't much of a help to her, just telling Rhonda to flag the account that was impersonating her so that Facebook could take it down. That didn't help stop all the bogus friend requests going out.

We urged Rhonda to change her password, because there's always a chance the hacker didn't get it. And a hacked password can get into her financial information, private messages, photos and more.

In beefing up your password, Facebook recommends longer passwords as "usually more secure" and that they shouldn't be "your email, phone number or birthday."

Most experts also tout a combination of lower and upper case letters,

numbers and symbols, ones a hacker couldn't get, like either something impossible like QQXX$^%# or a variation that only you would know like a favorite movie spelled backwards, with the addition of some symbols.