(Approximately 1050 words)

Don’t ever share your password or pin #

By Jerry Heaton, Editor, Central Kentucky Computer Society

December 2018 issue, CKCS Newsletter

www.ckcs.org

newsletter (at) ckcs.org

The importance of protecting your personal information has been stressed time and again. Yet we still hear of occasions where someone has fallen for a scam which has cost them money, time and much aggravation.

I would like to think no one in our group has fallen for a scam of any type that cost them money. But I would almost bet someone I know has become a victim. I don’t know it and probably never will because victims don’t like to admit their stupidity – maybe that is a harsh word let’s just say for being such a ‘soft touch,’

Most people become victims only when they believe someone person convinces them they have a great chance to make some easy money or perhaps save them a lot of money.

I offer only a few rules which you should follow to keep from becoming a scam victim.

1. Don’t answer or linger on the phone with a caller you don’t know – even if they are from your own area code. Scammers and hackers can be anywhere in the world and still use you home area code.

2. If your phone rings once and then hangs up. DO NOT call back thinking the call was important and just got dropped. It could be their intent is to get you on the line and involve you in a lengthy conversation with the goal to keep you online as long as possible. There are area codes in the Caribbean that charge many dollars per minute which can be added to your phone bill.

3. If your phone rings and your caller ID shows someone you don’t know – don’t answer the call. If you decide to answer the call and don’t recognize the voice – hang up

Should you do decide to ignore the above suggestion, and answer a call – more rules:

1. Don’t trust anyone who calls with a great deal for you, which seems almost too good to be true – it likely is too good to be true.

2. Never ever give anyone your password – no one needs to know that but you.

3. Never ever give anyone your pin number – no one needs to know that but you.

4. Never ever give anyone your banking information – no one needs to know that but you.

All this discussion came to mind as a CKCS board of directors member Jan Landers sent me the follow scam notice to put in the newsletter this month. It credits no individual or location, nor does it identify the author. The scam though is new to me and seems plausible. Just remember, this story may be new and true, or maybe not, It begins:

Alert your family and friends. Just when you thought you'd heard it all. Beware of people bearing gifts.

The following is a recount of the incident from the victim:

Wednesday a week ago, I had a phone call from someone saying that he was from some outfit called: "Express Couriers," (The name could be any courier company). He asked if I was going to be home because there was a package for me that required a signature.

The caller said that the delivery would arrive at my home in roughly an hour. Sure enough, about an hour later, a uniformed delivery man turned up with a beautiful basket of flowers and a bottle of wine.

I was very surprised since there was no special occasion or holiday, and I certainly didn't expect anything like it. Intrigued, I inquired as to who the sender was.

The courier replied, "I don't know, I'm only delivering the package."

Apparently, a greeting card was being sent separately. (The card has never arrived!) There was also a consignment note with the gift.

He then went on to explain that because the gift contained alcohol, there was a $3.50 "delivery/verification charge," providing proof that he had actually delivered the package to an adult (of legal drinking age), and not just left it on the doorstep where it could be stolen or taken by anyone, especially a minor.

This sounded logical and I offered to pay him cash. He then said that the delivery company required payment to be by credit or debit card only, so that everything is properly accounted for, and this would help in keeping a legal record of the transaction.

He added, "Couriers don't carry cash to avoid loss or likely targets for robbery."

My husband, who by this time was standing beside me, pulled out his credit card, and the "delivery man," asked him to swipe the card on a small mobile card machine with a small screen and keypad.

Frank, my husband, was asked to enter his PIN number and a receipt was printed out. He was given a copy of the transaction.

The guy said everything was in order and wished us good day.

To our horrible surprise, between Thursday and the following Monday, $4,000 had been

charged/withdrawn from our credit/debit account at various ATM machines.

Apparently the "mobile credit card machine," which the deliveryman carried now had all the info necessary to create a "dummy" card with all our card details including the PIN number.

Upon finding out about the illegal transactions on our card, we immediately notified the bank which issued us a new card, and our credit/debit account was closed.

We also personally went to the police, where it was confirmed that it is definitely a scam because several households had been similarly hit.

WARNING: Be wary of accepting any "surprise gift or package," which you neither expected nor personally ordered, especially if it involves any kind of payment as a condition of receiving the gift or package. Also, never accept anything If you do not personally know or there is no proper identification of who the sender is.

Jan, the board member who sent me this added this comment, “Above all, the only time you should give out any personal credit/debit card information is when you yourself initiated the purchase or transaction!

No doubt you might think of another rule or two that should be added to this list to protect ourselves.