# Harvest Bank Newsletter

## Fall/Holiday Edition

***DEDICATED TO SCAM AWARENESS TIPS TO PROTECT YOU AND THOSE YOU CARE ABOUT***

*Excerpts from*

## "The Top Scams Affecting Senior Citizens Right Now (and how Bankers can Help)"

**By Aimee Leeper,**
*Senior Housing Crime Prevention Foundation*

"Older adults are attractive targets for financial exploitation because they tend to possess more wealth than other potential targets. [Here are a few of] the most common scams...now.

**Medicare & Health Insurance Scams**
[One of] the latest Medicare scams to pop up is where scammers are emailing, calling, and even knocking on doors, claiming to be from Medicare and offering all sorts of pandemic-related services if you "verify" your Medicare ID number. Among the offers is to send new cards they claim contain microchips.

**Covid-19 Scams**
[There is a scam centering around] a FEMA program that will pay up to $9,000 for funeral expenses if a loved one was lost to the disease. While this is a legitimate program, and citizens can reach out to FEMA to apply for these benefits, unfortunately, FEMA reports that scammers are contacting people and pretending to offer to register them for assistance. To avoid those scams:

- FEMA will not contact anyone until they call or apply for assistance
- The government won't ask for payment to get this benefit
- Nobody should give out deceased loved one's personal or financial information to anyone who has contacted them out of the blue.

**Telemarketing/phone scams**
Seniors were raised in an era that valued politeness and good manners, but this makes them more vulnerable to fraud. Hang up the phone or simply say "no" to criminals pretending to be telemarketers or representatives of a company. Three examples:

- The pigeon drop - the con artist tells the individual that he/she has found a large sum of money and is willing to split it if the person will make a "good faith payment" by withdrawing funds from his/her bank account.
- The fake accident ploy – the con artist gets the victim to wire or send money on the pretext that the person's child or another relative is in the hospital and needs the money.
- Charity scams – money is solicited for fake charities. People should avoid answering calls from unknown numbers and be aware of caller ID spoofing technology to mask their true phone number from showing.

*Continued on next page*

> **"Seniors were raised in an era that valued politeness and good manners, but this makes them more vulnerable to fraud."**

## Harvest Bank's annual Good Coin match campaign:

## "Strong Communities with YOU 2021"

From Nov 15-Dec 31, Harvest Bank will match contributions to the featured, local organizations on the bank's charitable giving site: harvestbankmn.com/give. Donations of $10-50 will be matched 1-for-1.

Good Coin is a (cloud-based) charitable giving platform, provided by FIS (a well-recognized provider of online banking solutions). At a surcharge of the standard internet processing fee - 2.9% - plus $0.30 per transaction, this is among the lowest in the industry. We invite you to check out the charities, give generously, and know that you've chosen a trustworthy way to donate!

**www.harvestbankmn.com**

### Contact Us

| | |
|---|---|
| **Kimball** | 398-3500 |
| **St. Augusta** | 251-6100 |
| **Atwater** | 974-8861 |
| **Kandiyohi** | 382-6100 |

*Continued From Previous Page*

**Internet fraud**
...scammers are also sending fake text messages alleging that there is big trouble with your internet account, a credit card, bank account or shopping order on Amazon or other popular retailers. The urgent-sounding text message may even have a real-looking logo. They want people to click on links and provide personal info.

Similar issues are popping up via ads on social media. Phony retail sites are using photos lifted from real online stores to make their fake store look legitimate. They run ads where a click directs to their fake site, where if an order is placed with payment info, the goods are never received, or are a sub-par, cheaper knock-off version, often shipped direct from overseas."

For the complete article, visit: harvestbankmn.com. Click on "community alerts, events & news".

## *Holiday Update*

In light of the pandemic spike in MN, Harvest Bank will not be holding holiday gatherings this December. Calendars and other treats will be made available nonetheless. Look for an update from your branch. We all wish you a happy, healthy, and rewarding 2022!

*Seniors and College-age adults...*

# Dangers of Social Media Scams

**By Mike Burke,**

*Excerpts from Part 2, on the Shazam Blog: https://www.shazam.net/news/shazam-blog*

*Shazam is our processor for our debit cards. Contact us for a debit card with innovative features!*

"Every student heading back to school has a smartphone in their pocket, using it to communicate, socialize and kick back and relax. However, an increasing number of scammers are out there right now targeting unsuspecting students.

...Scammers target college students using popular social media networks because they're vulnerable.
It's easy for college students to let their guard down and fall victim to schemes stealing their identity or draining their bank account. Sometimes the bad guys even trick students into becoming accomplices to their fraud with the lure of easy money.

Scam artists see a big opportunity with a college student's personally identifiable information (PII). Let's look at way's cybercriminals use social media to target college students.

**Save or earn money by downloading this app scams**
Many scams on social media post false advertisements claiming the reader can win money or save money by downloading an app – albeit with a sketchy link. If students tap on the link or try to download the app, they will instead install malware to their device – exactly what the scammers were hoping for. These links are usually shortened to bit.ly, making it difficult to see outright that it's a malicious link.

Once scammers trick someone into installing malware on their phone, they work diligently to steal password information and PII.

If successful, this leads to a social media takeover, giving the trickster the ability to post ads, message the victim's friends and create spam posts.

**Card cracking scams make victims an accomplice to fraud**
College students and other young adults are the primary targets of a scam called card cracking, which is a type of account fraud. Targeted mainly through social media, the goal is for the scammer to acquire the accountholders checking account information or debit card and PIN in a money-making partnership. There are different variations of card cracking, let's look at two.

In one scenario, a scammer reaches out via social media with an online job offer or promise of financial aid that involves a money exchange. The bad guys ask for bank account information to deposit money and then make a deposit with fake, stolen or counterfeit checks. Next, they have the victim send them money or they make an immediate withdrawal from the victim's account. By the time the fake check or bogus deposit gets flagged, the money is already gone, and the accountholder is broke.

In a different version of the scam, with the lure or easy money for the student, fraudsters convince their victims to share their debit card and PIN, telling them to report the card stolen to recover the money. The fraudster cleans out the bank account, not sharing the promised portion of the money with the accomplice. Worse yet, most victims who fall for this scam don't realize they are committing a crime.

Being charged as an accomplice to a crime is a very serious offense.

**The car wrap scam, get paid to drive**
Another current hot scam on social media – get paid to drive, what could be easier than that?

The shyster offers a large sum of money to a student just to drive around with their car wrapped in an advertisement. Sounds cool and easy. When the intended target responds, the scammer sends them a counterfeit check to deposit into their account with instructions to immediately send payment to a pre-selected decal agent who will put the ads on their car.

The student is told to keep a portion of the deposit check to pay themselves.

In the end, the bogus deposit check will bounce, leaving the student to foot the bill for the money they've already sent to the decal agent who is really the scammer.

**Victim recourse**
Students who fall prey should take the following steps:

- Stop all contact with the con artist and keep copies of all communications
- Report the matter to local police department
- Report the incident to the FBI Internet Crime Complaint Center and the Federal Trade Commission.

While social media is a great way to stay in touch with friends, it's also a way for fraudsters to take advantage of college students. Through the stress of being in a whole new world, it is easy for college students to let their guard down. A good rule of thumb is to beware of easy money offers as they are rarely legal. As the saying goes, if it sounds too good to be true, it probably is."

**THIS NEWSLETTER FEATURES A PHOTO OF KIMBALL IN 2020. FUTURE NEWSLETTER EDITIONS WILL FEATURE SCENES FROM OUR OTHER COMMUNITIES. IF YOU HAVE PHOTOS OF A TOWN THAT HARVEST BANK SERVES—CONTACT ELLA MEYERSON AT HARVEST BANK-ATWATER FOR POTENTIAL INCLUSION IN A FUTURE EDITION!**