The Northwestern District Attorney's Office came to our campuses for presentations about recognizing and avoiding scams. I wanted to pass along some tips to those of you who were unable to attend.

Phone Scams:

- Scammers can make any name and phone number appear on your caller ID. They can have it appear to be a local number and/or the name of a particular company or person.
- Scammers will try to prevent you from hanging up the phone. They try to hurry you, pressure you, play on your emotions. They sometimes present themselves as authority figures (police, Medicare, IRS, Social Security, etc.).
- Anyone who pressures you to pay or give personal information is likely a scammer. Legitimate businesses will give you time to make a decision.
- If anyone asks you to pay for anything with gift cards, it is a scam.
- Before you do anything, tell someone what is happening.
- If you receive a call from a "utility company" saying they are shutting off your service, hang up, look up the number of the company and call them to check if you are unsure.
- If you receive a call from your "bank or credit card company", and they are asking for personal information or you are unsure, hang up and look up their number to call them to check.
- If you receive a call from your "doctor's office" asking for personal information including your Medicare number, again, hang up and call your doctor's office to check.
- Texting scams include telling you that you must call a certain number, or you will be charged for something. They may say there is a problem with a delivery to your address.

Computer Scams:

- A common computer scam is when your computer tells you that you have a virus- this can include alarm sounds, flashing lights, a voice telling you not to touch any keys. They encourage you to call a certain number for help or to click on something. DO NOT call or click on anything. Tell someone. This is a scam.
- Another common computer scam is an email telling you that you need to update information for a familiar company (e.g., Netflix, Amazon) or that it is from your bank or credit card company. DO NOT CLICK ON ANYTHING OR USE THE EMAIL, PHONE NUMBER THEY PROVIDE. Go to the company website and log in to your account to check.
- Beware of any PDF attachments from someone you don't know- it can contain a virus.
- Keep your computer security up to date. Use strong password and multi-factor authentication.

Mail Scams

- Common mail scams include investment schemes, car or home warranty, IRS refunds or money owed, Lottery winning, inheritance schemes, charities.

In general, we all need to be mindful and suspicious of the email, phone, mail, and text communication we receive. Scammers are professionals- they make a lot of money and are very skilled at what they do. It is never the fault of the victim. It is also important to be aware that 72% of the money that is taken is stolen from a friend or family member.

Always tell someone if you think you may be being scammed!

Erin Curtin