COVID-19 SCAMS

Allen Hill <ahill@uwlax.edu>

Wed 3/25/2020 11:45 AM

Students, Faculty, Staff,

The UWL Police Department received information this morning that one of our community members received a fraudulent phone call about COVID-19 testing. The fraudster knew that our community member was associated with UWL, and stated that they needed to be tested for COVID-19 right away. Our community member was threatened with being jailed if they did not agree to the testing. This unsolicited phone call was an attempt to steal money and gather sensitive personal information.

Please be aware that these scams are on the rise, and do not give out personal information on the phone or by email. The ultimate goal of these scams is to get credit card information. Currently, there isn't a cure for COVID-19 and no home test kits. If you receive a phone call regarding COVID-19 regarding testing or treatments, hang up and block the number. If you receive an email regarding COVID-19 testing or cures, delete the email and do not click on any links or attachments.

Some examples of COVID-19 scams include:

- **Treatment scams:** Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19

- **Supply scams:** Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.

- **Provider scams:** Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.

- **Charity scams:** Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.

- **Phishing scams:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information.

- **App scams:** Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.

- **Investment scams:** Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

If you think you are a victim of a scam or attempted fraud involving COVID-19, you can report it without leaving your home through several platforms. Go to:

- Contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at disaster@leo.gov
- Report it to the FBI at tips.fbi.gov
- If it's a cyber scam, submit your complaint through https://www.ic3.gov/default.aspx

Allen Hill
Chief of Police
UW-La Crosse Police Department | ahill@uwlax.edu
Non-Emergency 608.789.9000 | FAX 608.785.8909
Campus Emergency 608.789.9999 OR DIAL 911