

Josh Kaul Wisconsin Attorney General P.O. Box 7857 Madison, WI 53707-7857

NEWS FOR IMMEDIATE RELEASE

March 4, 2021

AG Kaul, DATCP Secretary-designee Romanski Warn Wisconsinites of COVID-19 Related Scams

MADISON, Wis. – Attorney General Josh Kaul and Department of Agriculture, Trade and Consumer Protection (DATCP) Secretary-designee Randy Romanski proudly join government and nonprofit organizations from across the county in celebrating the 23rd annual National Consumer Protection Week by warning Wisconsinites of COVID-19-related scams.

"Coronavirus-related scams can come in a variety of different forms, including robocalls, text messages, postings on social media sites, and more. But the aim of these fraudsters is the same: to steal consumers' money, sensitive personal information, or both," said AG Kaul. "Folks can help protect themselves against these scams by taking some simple steps, like considering whether an unsolicited contact may be a phishing attempt."

"Unfortunately, even during a pandemic, some scammers still try to obtain consumers' personal or financial information," said Secretary-designee Romanski. "Whether you have been the victim of a COVID-19 scam or you just need more information on how to protect yourself, DATCP's Bureau of Consumer Protection is here to serve as your resource."

Coronavirus Vaccine Scams:

Fraudsters are trying to capitalize on the rollout of COVID vaccines. The COVID-19 vaccine is not for sale and cannot be purchased anywhere, including online pharmacies. The vaccine is only available at federal- and state-approved locations, such as health care clinics, local health departments, community vaccination centers and pharmacies. Claims otherwise are a scam.

Page 1 of 3

Keep scammers away with these simple tips:

- Do not give out your personal or financial information. If you have any questions about a request, check with your doctor or visit the Wisconsin Department of Health Services' (DHS) website for the latest vaccine information: <u>https://www.dhs.wisconsin.gov/covid-19/vaccine.htm</u>
- Don't click on links in unsolicited emails or text messages. It could download a virus onto your computer or device. Even emails and posts that seem to be asking you to sign up for a vaccine list, promoting vaccine availability, or promoting awareness and prevention tips may contain dangerous links.
- Always talk with your doctor or another healthcare professional before you try any product claiming to treat, cure, or prevent COVID-19.
- You should not have to pay out of pocket to get the COVID-19 vaccine. The federal government and the DHS will not call, text, or email you seeking personal or financial information.
- Use reliable sources for the most current information.
 - To learn more about who is currently able to get the COVID-19 vaccine and where eligible people can get vaccinated, go to <u>https://www.dhs.wisconsin.gov/covid-19/vaccine-about.htm</u>.
 - Visit your local health departments or health insurer's website for FAQs or resources on COVID-19 vaccine distribution if you have questions about vaccine availability in your area. Individuals should be patient, but if you have questions your provider is your most reliable source of information.
 - Contact DATCP's Consumer Protection Hotline at (800) 422-7128 or <u>datcphotline@wisconsin.gov</u> if you are worried something may be a scam.

Contact Tracing Scams:

Contact tracing identifies people who have recently been in close contact with someone who has tested positive for COVID-19, which will help states more rapidly identify those who may have been exposed and quickly get them the necessary support and resources that can help protect them and their loved ones. Contact tracers authorized to work in Wisconsin will identify themselves with a first and last name, and the name of the government entity they are calling from, such as DHS or a local health department.

Scammers pretending to be contact tracers may call, text, or email also send text or email messages asking residents to click a link. These are often "phishing" scams that help a scammer gain access to a person's computer, your financial information, and/or personal information. If you receive a message like this, confirm it is legitimate by calling your healthcare provider directly. Legitimate contact tracers will not ask for money or for personal information like your Social Security, bank account, or credit card number. If a contact tracer wants to confirm your identity through a birthdate or your address, they should be able to provide that information to you.

Other COVID-19 Related Scams:

With many Wisconsinites doing more online shopping from the safety of their homes, there has been an increase in package deliveries, and greater opportunity for delivery scams. Scammers typically start with a text message or an email about delivering a package to your address. These messages include a "tracking link" that you are urged to click in order to update your delivery or payment preferences. You might also get a voicemail message with a call-back number, or a "missed delivery" tag on your door with a number to call.

While these messages often look or sound legitimate, you should never click a link or call back the number from an unexpected delivery notice. These links may open a website that prompts you to enter personal information, or it may install malware on your phone or computer that can secretly steal personal information. Consumers who receive suspicious email, text, or phone messages should go to their delivery carrier's website directly or use the retailer's tracking tools to verify the communication.

If you believe you are a victim of a scam:

If you have been targeted by a COVID-19 scam, you can report the scam to DATCP's Consumer Protection Hotline at (800) 422-7128, or email <u>datcphotline@wisconsin.gov</u>, or visit <u>www.datcp.wi.gov</u>.

For accurate, up-to-date information about COVID-19, visit: <u>https://www.dhs.wisconsin.gov/covid-19/index.htm</u>.