NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

CONSUMER ALERT: Extortion Emails Sent to Wisconsin Consumers

FOR IMMEDIATE RELEASE: October 25, 2024
Contact: Caleb Kulich, Public Information Officer, (608) 621-1290,
caleb.kulich@wisconsin.gov

MADISON, Wis. – The Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) is alerting the public that it has received an increased number of complaints and reports concerning extortion attempts sent by email. Consumers should know how to respond if and when they are faced with an extortion attempt.

The messages in question falsely claim that the sender has obtained private and potentially damaging video recordings, or other personal information about the target. The scammers often include some accurate information about the individual being targeted to make their claims more believable, such as the person's home address and a Google Maps photo of their residence. The tone of the messages may imply the scammer has been watching them closely, and for a long time.

The scammer will often claim the target has visited unsafe websites and explain that this is how they first obtained access to the individual's cellular phone or computer. The scammer may also claim they can remotely access the target's webcams and phone cameras to watch and record video of them at any time. Finally, the scammer threatens to share this private and embarrassing information with the target's colleagues, family, and friends unless their demands are met.

The scammers typically request payment through cryptocurrency, which can be difficult to trace by banks or government agencies and can be impossible to recover after it is sent. Consumers can expect these emails to communicate a sense of urgency, and they will likely be asked to pay up quickly or risk having the private information released very soon.

If a consumer receives a message similar to this description, they should follow these steps:

- **Do not panic.** It is unlikely the scammer truly has compromising video of them.
- **Ignore the message.** Do not call any phone number listed in the messages, click on any links, or open any attachments.
- **Never send money.** In addition to cryptocurrency, scammers commonly ask for payment to be made through gift cards, cash, or a wire transfer.
- **Change your password** if the scammer references having it. If a password is reused for multiple accounts, change it on all of them. New, unique passwords should be used for separate accounts to prevent the scammer from fraudulently accessing multiple accounts with a single password.

Report extortion attempts to DATCP, the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov, the Federal Trade Commission at www.ftc.gov, and if the message was sent to a work account, to the employer's technology department.

For more information and consumer protection resources or to file a complaint, visit DATCP's Consumer Protection webpage at ConsumerProtection.wi.gov or contact the Consumer Protection Hotline at (800) 422-7128 or DATCPHotline@wisconsin.gov.

###

Find more DATCP news in our newsroom, on Facebook, X, and Instagram.