The Office of
Minnesota Attorney General Keith Ellison
helping people afford their lives and live with dignity and respect • www.ag.state.mn.us

Attorney General Ellison warns Minnesotans about COVID-19 phishing attacks

March 24, 2020 (SAINT PAUL) — Minnesota Attorney General Keith Ellison today warned Minnesotans about a reported spike in phishing attacks related to COVID-19, and offered advice about how to spot, avoid, and report them.

"We're all concerned right now about our own health and the health of our loves ones and our communities. We're also concerned about affording our lives. It's disgusting to think about, but scammers are trying to take advantage of our very real concerns in order to rip us off and line their own pockets," Attorney General Ellison said. "Just like we can protect ourselves and each other by social distancing, we can protect ourselves and each other by keeping our distance from scammers. I'm putting out these tips so that everyone can recognize the signs of a phishing attacks and stay far away from them.

"It's more important every day that Minnesotans consume information about the COVID-19 pandemic *only* from trusted resources like the Minnesota Department of Health and the Centers for Disease Control and Prevention — not from scammers with "urgent" updates or "miracle" cures. They should take advice about their own health, including testing and treatment related to COVID-19, *only* from their healthcare professional or a public-health professional," Attorney General Ellison continued.

Phishing is a scam where thieves attempt to steal personal or financial account information by sending deceptive electronic messages that trick unsuspecting consumers into disclosing personal information. The bait may be an email, instant message, or pop-up window from what appears to be a trusted institution or company — for example, a government agency, financial institution, or internet service provider, among others. The consumer is encouraged to provide account information or other personal information, including financial information, and/or to click on a link that will install malware on the consumer's computer.

There has been an increase in phishing attacks in response to COVID-19. Scammers are exploiting people's heightened concern at this moment with phishing attacks that are increasingly realistic. Phishing scammers may purport to be government leaders or health officials and claim to have important information about how to reduce the spread of COVID-19. They may claim to have access to tests, vaccines, or miracle cures.

State of Minnesota IT Services has observed the following COVID-19 phishing-related scams:

- A fake COVID-19 tracking map that was distributing malware;
- COVID-19 smartphone apps distributing malware;
- Scam websites; and
- Impersonations of the Centers for Disease Control (CDC) and the World Health Organization (WHO).

These new phishing scams use updated versions of the same tricks:

- Email addresses containing look-alike domains, such as emails ending in "@cdc-gov.org" instead of the legitimate "@cdc.gov."
    - **TIP:** Check email addresses and domains carefully before opening emails.
    - **TIP:** Look for misspellings, poor grammar, or unusual or unprofessional language in the email.
    - **TIP:** Do not assume that an email is legitimate because it includes the organization's or business's logo. Scammers often use them to fool you into thinking the email is legitimate.
- Urgent requests to click on hyperlinks that direct users to malicious sites. Those links may send you a site that looks official or legitimate but is actually run by scammers.
    - **TIP:** Do not trust even legitimate-appearing hyperlinks from unknown senders.
- Sham "verifications" that ask you to provide sensitive personal information before accessing a site.
    - **TIP:** Be skeptical of requests to verify your identity with sensitive personal information — especially if a site has not asked for the information in the past.
    - **TIP:** The World Health Organization and the Centers for Disease Control and prevention will never ask you for personal informational by email.
    - **TIP:** Companies you do business with already know your account number and will never ask you to provide it to them. The Social Security Administration, Medicare, or your financial institution will never ask you for personal information by email.
- Requests to communicate with businesses or individuals outside the normal channels of communication, including unknown emails.
    - **TIP:** If you have any doubt whether a communication is legitimate, call or email those businesses or individuals directly at the publicly-listed phone number to ask if it came from them.
    - **TIP:** Do not trust the number in the suspected email, as it may send you to scammers rather than to the business or organization it claims to represent.

More trusted tips for spotting and avoiding phishing attacks are from Attorney General Ellison's website and the Federal Trade Commission.

As always, Attorney General Ellison asks Minnesotans file a complaint about any scams they come in contact with to his office. Minnesotans with specific complaints about COVID-19-related price-gouging should use the complaint form dedicated to that purpose that can be accessed on the front page of Attorney General Ellison's website.

# # #