Be on the Lookout for COVID-19 Scams

The Department of Homeland Security advises everyone to exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19. Instances of these scams are already being reported across the UA system.

By staying vigilant and following these precautions, we can avoid becoming victims:

Phone Scams
If you receive an unexpected phone call from a number you don't know and are invited to participate in a teleconference that you were not scheduled for, hang up immediately. **DO NOT press #1** as you may be inadvertently accepting charges.

Email Scams
Email messages may ask you to open an attachment or link to show you the latest statistics, health alerts, health advice, or claim to be new policies from your employer. When you click on the link or attachment, you are likely to download malicious software onto your device. **DO NOT CLICK LINKS** from sources you do not know, links you were not expecting, or that appear suspicious in any way.

Other indicators that the email is a scam:

- Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Keep in mind phishers can create links that closely resemble legitimate addresses.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email.
- Be suspicious of emails that insist you "act now". Phishing emails often try to create a sense of urgency or demand immediate action.

Fake/Malicious Websites
Malicious websites with variations on "coronavirus" in their Internet addresses are also rampant. These sites can contain malicious software that infects your computer if you visit them or they serve as online scams attempting to steal your personal information When searching for information on Coronavirus, use trusted sources such as legitimate, government websites like https://www.cisa.gov/coronavirus—for up-to-date, fact-based information about COVID-19.

How to Report Phishing

To report phishing in Google Mail:

1. Open the message.
2. Click the three stacked dots that are next to the reply arrow.
3. Click “Report phishing.”

To report phishing in Outlook 2019:

1. Select the suspicious message.
2. Go to the Home tab and select the “Junk” drop down
3. Select “Report as Phishing.”

What to do if you fall for the scam

If you have become a victim of any of these scams, notify your local service desk immediately.

Your UA service desks are ready to help! Contact us!

UAA
Technical Support Center: (907)786-4646
Toll Free: (877) 633-3888
uaa.techsupport@alaska.edu

UAF
Phone: (907) 450-8300 (x8300 on campus)
Toll-free: (800) 478-8226
helpdesk@alaska.edu

UAS
907-796-6400 (Helpdesk)
877-465-6400 (Toll Free)
uas.helpdesk@alaska.edu