University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus
OFFICE OF INFORMATION SECURITY

Cybercriminals are sending COVID-19 pandemic-related phishing emails with the goal of stealing your money and personal information.

Some examples of these reported phishing emails include:

- Products that claim to prevent, treat, diagnose, or cure COVID-19
- Availability of free test kits
- Assistance with obtaining a stimulus check from the government
- Up-to-date, local statistics from impersonated public health authorities, such as the World Health Organization (WHO) and Centers for Disease Control and Prevention (CDC)
- Breaking news stories from impersonated news organizations, such as the Wall Street Journal
- Heartfelt plea for financial donors to help vaccinate children

Be on alert for these and other similar phishing emails and recognize the red flags:

- Message of fear and urgency: Legitimate messages will not instill fear or demand that you take urgent action.
- Request for personal or financial information: No public health or government agency will send you an email message (or call) asking for personal or financial information.
- Links and attachments: Cybercriminals can use links and attachments to deliver malware to your computer and gain access to sensitive work or personal information. They may also lock your computer for ransom until a payment is received.

Remember these tips if you receive a suspicious email:

- Do not provide your username, password, or any personal information requested by unsolicited email.
- Do not click links or attachments unless you are positive the content is safe.
- Ignore tactics aimed to scare you into taking urgent action, including: threats of a lawsuit, a computer full of viruses, locked accounts, or opportunities to earn or save money now.
- Legitimate companies and service providers will provide a way for you to contact them directly. If you're uncertain, you can learn more by researching them online.
- Verify the legitimacy of charities and crowdfunding sites before making donations. Do not provide donations in cash, gift cards, or money wires.

If you suspect that your university-provided computer may be compromised or if you inadvertently disclosed sensitive university information to unauthorized individuals, it is important to report it immediately.

Check out these CU websites to learn more:

- Information on how to report potential incidents: www.cu.edu/ois/report-incident
- Top 10 action to reduce risk, including keeping security in mind while working remotely: www.cu.edu/ois/top-10-action-reduce-risk

Thank you for sharing in the responsibility to keep CU's information assets secure.

University of Colorado Office of Information Security