Watch out for scam emails related to COVID-19 that ask for sensitive information.
Think before you click.
SCAM ALERT
Phishing Scams Related to COVID-19

One more thing to keep in mind during this period of uncertainty: The bad guys are always looking for a way in.

Cyber criminals are already exploiting the Coronavirus crisis and trying to turn it to their advantage.

Be on the look out for unsolicited emails offering information about COVID-19 in the days and weeks ahead. Some of these emails will be malicious. Like emails from hackers pitching COVID-19 health information and fake cures.

For reliable information relating to COVID-19, consult trusted sources of information such as the World Health Organization or communication emails coming from CDCR executive staff.

What you need to do:

1. **Never enter ANY username and password** into an unexpected logon page from an email request.

2. **Please report all suspicious emails** to the Information Security Office so we can block them if necessary.

3. With more CDCR staff members working remotely, please be sure to **fully shut down your computer each night** to help protect our VPN infrastructure.

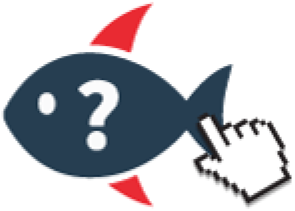
Tips to Keep in Mind

- **Think before you click.** The best thing you can do is take a minute to validate the email by looking for warning signs or red flags before you take any action on it. Red flags such as spelling mistakes, grammatical or structural errors, missing contact information or a sense of urgency to respond.

- **Examine and confirm links.** Before you click on a link, hover your mouse over it to reveal the full address. Does it go where you are expecting?

- **Don’t open attachments!** We can’t stress this enough. If you were not expecting the attachment, contact the sender to validate it. No contact info? Just delete it!

Report Phishing



If you have the “report phishing” icon on your outlook desktop application, you can simply click the button to send the email to the Information Security Office and move the suspected email into your “junk” mail folder in 1 step.

If you do not have the icon, please send a copy of the email to: phishing@cdcr.ca.gov